

# Contents

[Exchange Online](#)

[Exchange Admin Center](#)

[Berechtigungen](#)

[Funktionsberechtigungen](#)

[Rollengruppen](#)

[Sicherheit und Compliance](#)

[Ändern von Archivrichtlinien](#)

[In-Situ-Speicher und Beweissicherungsverfahren](#)

[Erstellen oder Entfernen von In-Situ-Speichern](#)

[In-Situ-eDiscovery](#)

[Zuweisen von eDiscovery-Berechtigungen](#)

[Erstellen einer Compliance-eDiscovery-Suche](#)

[Exportieren der Suchergebnisse](#)

[Nachrichteneigenschaften und Suchoperatoren](#)

[Suchbeschränkungen](#)

[Erstellen eines Discoverypostfachs](#)

[Erstellen eines benutzerdefinierten Verwaltungsbereichs](#)

[Verkleinern eines Discoverypostfachs](#)

[Löschen und Neuerstellen des Standarddiscoverypostfachs](#)

[Verhinderung von Datenverlust](#)

[Anwendung von DLP-Regeln](#)

[Integrieren von Regeln für vertrauliche Informationen](#)

[DLP-Richtlinienvorlagen](#)

[Erstellen einer DLP-Richtlinie aus einer Vorlage](#)

[Erstellen einer benutzerdefinierten DLP-Richtlinie](#)

[Richtlinientipps](#)

[Verwalten von Richtlinientipps](#)

[Exchange-Überwachungsberichte](#)

[Exportieren von Postfachüberwachungsprotokollen](#)

- Bericht zum Postfachzugriff durch Nicht-Besitzer
- Bericht zu Beweissicherungsverfahren pro Postfach
- Durchsuchen der Rollengruppenänderungen
- Anzeigen des Administratorüberwachungsprotokolls
- Anzeigen des externen Administratorüberwachungsprotokolls
- Messaging-Datensatzverwaltung
  - Aufbewahrungstags und -richtlinien
  - Standardaufbewahrungsrichtlinie
  - Standardordner
  - Aufbewahrungszeitraum
  - Erstellen einer Aufbewahrungsrichtlinie
  - Hinzufügen oder Entfernen von Aufbewahrungstags
  - Anwenden von Aufbewahrungsrichtlinien
  - Anhalten der Aufbewahrungszeit eines Postfachs
- Journaling
  - Verwalten des Journalings
  - Konfigurieren des Journalings
- Nachrichtenflussregeln
  - Bedingungen und Ausnahmen
  - Aktionen für Nachrichtenflussregeln
  - Bewährte Methoden für die Konfiguration
  - Überprüfen von Nachrichtenanlagen
  - Aktivieren von Verschlüsselung und Entschlüsselung
  - Standardszenarien für Anlagensperre
  - Haftungsausschlüsse, Signaturen, Fußzeilen oder Kopfzeilen
  - Verfahren für Nachrichtenflussregeln
  - Verwalten von Nachrichtenflussregeln
  - Testen von Nachrichtenflussregeln
  - Verwenden von Regeln zum Umgehen unwichtiger Elemente
  - Verwenden von Regeln zum Weiterleiten von E-Mails
  - Verwenden von Regeln zum Hinzufügen von Besprechungen
  - Verwalten der Nachrichtenbestätigung

## Gängige Szenarien der Nachrichtenbestätigung

Ordner „Wiederherstellbare Elemente“ in Exchange Online

Dauerhaftes Löschen von Elementen aus dem Ordner „Wiederherstellbare Elemente“ oder Bereinigen dieses Ordners in Exchange Online

Bewährte Methoden für den Nachrichtenfluss

Testen des Nachrichtenflusses

Problembehandlung beim Nachrichtenfluss

Verwenden von Connectors zum Konfigurieren des Nachrichtenflusses

Muss ich einen Connector erstellen?

Einrichten von Connectors zum Weiterleiten von E-Mail

Einrichten von Connectors für den sicheren Nachrichtenfluss mit einem Partner

Überprüfen von Connectors

Bedingtes E-Mail-Routing

Integrieren von Office 365 mit einem E-Mail-Add-On-Dienst

Verwenden von verzeichnisbasierter Edge-Blockierung

Verwalten von akzeptierten Domänen

Aktivieren der Nachrichtenübermittlung für Unterdomänen

Remotedomänen

Verwalten von Remotedomänen

Unterstützte Zeichensätze

Nachrichtenformat und Übertragung

Konfigurieren der externen Postmasteradresse

Verwalten von Postfächern mit Office 365

Verwalten des Nachrichtenflusses mit einer Drittanbietercloud

Verwalten des Nachrichtenflusses für mehrere Speicherorte

Verwalten des Nachrichtenflusses in Office 365 und lokalen Postfächern

Einrichten eines Multifunktionsgeräts oder einer Anwendung zum Senden von E-Mails mit Office 365

Konfigurieren von IIS für Relay mit Office 365

Beheben von Problemen mit Druckern, Scannern und Branchenanwendungen, die E-Mails mithilfe von Office 365 senden

Empfänger in Exchange Online

Grenzwerte für Nachrichten und Empfänger

[Erstellen von Benutzerpostfächern](#)

[Löschen oder Wiederherstellen von Postfächern](#)

[Verwalten von Benutzerpostfächern](#)

[Hinzufügen oder Entfernen von E-Mail-Adressen](#)

[Ändern der Aufbewahrungszeit für gelöschte Elemente](#)

[Konfigurieren der E-Mail-Weiterleitung](#)

[Konfigurieren von Einschränkungen für die Nachrichtenübermittlung](#)

[Konvertieren eines Postfachs](#)

[Aktivieren oder Deaktivieren von Exchange ActiveSync](#)

[Aktivieren oder Deaktivieren von MAPI](#)

[Aktivieren oder Deaktivieren von Outlook Web App](#)

[Automatisches Speichern von gesendeten Elementen im Postfach des Delegators](#)

[Benachrichtigungen über unwichtige Elemente in Outlook](#)

[Ändern des Brandings von Benachrichtigungen über unwichtige Elemente](#)

[Aktivieren oder Deaktivieren der Wiederherstellung einzelner Elemente](#)

[Wiederherstellen von gelöschten Nachrichten](#)

[Verwenden von PowerShell zum Anzeigen von Postfachinformationen](#)

[Verwalten von Verteilergruppen](#)

[Erstellen einer Benennungsrichtlinie für Gruppen](#)

[Außerkraftsetzen der Benennungsrichtlinie für Gruppen](#)

[Verwalten dynamischer Verteilergruppen](#)

[Anzeigen der Gruppenmitglieder](#)

[Verwalten von E-Mail-aktivierten Sicherheitsgruppen](#)

[Verwalten des Gruppenzugriffs auf Office 365-Gruppen](#)

[Verwalten von E-Mail-Kontakten](#)

[Verwalten von E-Mail-Benutzern](#)

[Verwalten von Raumpostfächern](#)

[Verwalten von Gerätepostfächern](#)

[Verwalten von Berechtigungen für Empfänger](#)

[Verwalten der Facebook-Kontaktsynchronisierung](#)

[Verwalten der LinkedIn-Kontaktsynchronisierung](#)

[Konfigurieren eines moderierten Empfängers](#)

## Migrieren mehrerer E-Mail-Konten

Auswählen eines Migrationspfads

Verwenden der minimalen hybriden Lösung für eine schnelle Migration

Wissenswertes zu einer Übernahmemigration

Übernahmemigration zu Office 365

Wissenswertes zu einer mehrstufigen Migration

Durchführen einer mehrstufigen Migration

Konvertieren von Exchange 2007-Postfächern

Konvertieren von Exchange 2003-Postfächern

Migrieren von IMAP-Postfächern

Migrieren von G Suite-Postfächern

Migrieren anderer Typen von IMAP-Postfächern

IMAP-Migration im Admin Center

Verwenden des Assistenten zum Ausführen einer IMAP-Migration

Einrichten Ihrer IMAP-Serververbindung

Optimieren von IMAP-Migrationen

CSV-Dateien für IMAP-Migrationen

Vorbereiten von Gmail- oder G Suite-Konten

Migrieren Ihres Outlook.com-Kontos

Aktivieren der Prüfung in zwei Schritten für Google Apps

Migrieren von Postfächern zwischen Mandanten

Migrieren aus Lotus Notes

Hinzufügen eines SSL-Zertifikats zu Exchange 2013

Hinzufügen eines SSL-Zertifikats zu Exchange 2010

Hinzufügen eines SSL-Zertifikats zu Exchange 2007

Aktivieren von Gmail-Konten für IMAP

Bewährte Methoden für die Office 365-Migration

Zuweisen von Berechtigungen für die Migration

Verwalten von Migrationsbatches

Statusbericht zu Migrationsbenutzern

CSV-Dateien für Migration

Zusammenarbeit

Öffentliche Ordner

## Verfahren für öffentliche Ordner

Batchmigration von älteren öffentlichen Ordnern

Batchmigration der öffentlichen Ordner von Exchange 2013

Ausführen eines Rollbacks der Migration der öffentlichen Ordner von Exchange 2013

Migrieren Ihrer öffentlichen Ordner zu Office 365-Gruppen

Batchmigration von öffentlichen Exchange Online-Ordnern

Einrichten von älteren öffentlichen Hybridordnern

Einrichten von modernen öffentlichen Hybridordnern

Einrichten von öffentlichen EXO-Hybridordnern

Einrichten öffentlicher Ordner

Zugreifen auf öffentliche Ordner mit Outlook 2016 für Mac

Erstellen eines Postfachs für öffentliche Ordner

Erstellen eines öffentlichen Ordners

Wiederherstellen eines gelöschten Postfachs für öffentliche Ordner

Verwenden von öffentlichen Favoritenordnern

Aktivieren oder Deaktivieren von Mail für einen öffentlichen Ordner

Aktualisieren der Hierarchie öffentlicher Ordner

Entfernen eines öffentlichen Ordners

Anzeigen von Statistiken zu öffentlichen Ordnern

Freigegebene Postfächer

## Adressbücher

Adressbuchrichtlinien

Verfahren für Adressbuchrichtlinien

Aktivieren des Adressbuchrichtlinien-Routings

Erstellen einer Adressbuchrichtlinie

Zuweisen einer Adressbuchrichtlinie zu Benutzern

Ändern der Einstellungen einer Adressbuchrichtlinie

Entfernen einer Adressbuchrichtlinie

## Adresslisten

Verfahren für die Adressliste

Verwalten von Adresslisten

Verwenden von Empfängerfiltern zum Erstellen einer Adressliste

Entfernen einer globalen Adressliste

Konfigurieren der Eigenschaften von globalen Adresslisten

Erstellen einer globalen Adressliste

## Hierarchische Adressbücher

Aktivieren oder Deaktivieren von hierarchischen Adressbüchern

## Offlineadressbücher

Verfahren für Offlineadressbücher

Erstellen eines Offlineadressbuchs

Hinzufügen oder Entfernen einer Adressliste

Ändern des Standard-Offlineadressbuchs

Zuordnen von Empfängern

Entfernen eines Offlineadressbuchs

## Freigabe

### Organisationsbeziehungen

Erstellen einer Organisationsbeziehung

Ändern einer Organisationsbeziehung

Entfernen einer Organisationsbeziehung

### Freigaberichtlinien

Erstellen einer Freigaberichtlinie

Anwenden von Freigaberichtlinien

Ändern einer Freigaberichtlinie

## Voicemail: Unified Messaging

### Begrüßungen, Informationsansagen, Menüs und Menüansagen

Festlegen der Standardsprache für einen Wählplan

Auswählen der Sprache für eine automatische Telefonzentrale

Aktivieren der Aufzeichnung benutzerdefinierter Ansagen

### Telefonsystemintegration mit UM

Telefonieratgeber für Exchange 2013

Konfigurationshinweise für VoIP-Gateways

Konfigurationshinweise für Session Border Controller

### Verbinden des Voicemailsystems

## UM-Wählpläne

UM-Wählplan – Verfahren

Erstellen eines UM-Wählplans

Verwalten eines UM-Wählplans

Ändern des Audiocodecs

Konfigurieren der maximalen Anrufdauer

Konfigurieren der maximalen Aufzeichnungsdauer

Konfigurieren des Leerlauftimeouts für Aufzeichnungen

Konfigurieren der VoIP-Sicherheitseinstellung

Konfigurieren eines Wählplans für Benutzer mit ähnlichen Namen

Löschen eines UM-Wählplans

## UM-IP-Gateways

UM-IP-Gateway – Verfahren

Erstellen eines UM-IP-Gateways

Verwalten eines UM-IP-Gateways

Aktivieren eines UM-IP-Gateways

Deaktivieren eines UM-IP-Gateways

Konfigurieren eines vollqualifizierten Domänenamens

Konfigurieren der IP-Adresse

Konfigurieren des Überwachungsports

Löschen eines UM-IP-Gateways

## UM-Sammelanschlüsse

UM-Sammelanschluss – Verfahren

Erstellen eines UM-Sammelanschlusses

Anzeigen eines UM-Sammelanschlusses

Löschen eines UM-Sammelanschlusses

## Automatisches Beantworten und Weiterleiten von Anrufen

### DTMF-Schnittstelle

#### Automatische UM-Telefonzentrale – Verfahren

Einrichten einer automatischen UM-Telefonzentrale

Erstellen einer automatischen UM-Telefonzentrale

Hinzufügen einer Durchwahlnummer der automatischen Telefonzentrale

- Konfigurieren von Geschäftszeiten
  - Erstellen eines Feiertagszeitplans
  - Eingeben eines Firmennamens
  - Festlegen eines Unternehmensstandorts
  - Konfigurieren der Zeitzone
  - Aktivieren einer benutzerdefinierten Begrüßung während der Geschäftszeit
  - Aktivieren einer benutzerdefinierten Menüansage innerhalb der Geschäftszeiten
  - Aktivieren einer benutzerdefinierten Begrüßung außerhalb der Geschäftszeit
  - Aktivieren einer benutzerdefinierten Menüansage außerhalb der Geschäftszeiten
  - Aktivieren einer Informationsansage
  - Erstellen einer Menünavigation
  - Erstellen von Navigationsmenüs für Geschäftszeiten
  - Erstellen von Navigationsmenüs für Nicht-Geschäftszeiten
  - Verwalten einer automatischen UM-Telefonzentrale
  - Konfigurieren einer automatischen MVF-Fallback-Telefonzentrale
  - Aktivieren einer automatischen UM-Telefonzentrale
  - Deaktivieren einer automatischen UM-Telefonzentrale
  - Löschen einer automatischen UM-Telefonzentrale
  - Aktivieren oder Deaktivieren der Spracherkennung
  - Aktivieren oder Deaktivieren der Anrufweiterleitung
  - Aktivieren oder Deaktivieren des Versands von Sprachnachrichten
  - Aktivieren oder Deaktivieren der Verzeichnissuche
  - Konfigurieren von Benutzern, die kontaktiert werden können
  - Konfigurieren einer automatischen Telefonzentrale für Benutzer mit ähnlichen Namen
- Einrichten von Voicemail
- UM-Postfachrichtlinien
  - UM-Postfachrichtlinien – Verfahren
    - Erstellen einer UM-Postfachrichtlinie
    - Verwalten einer UM-Postfachrichtlinie
    - Löschen einer UM-Postfachrichtlinie

## **Voicemail für Benutzer**

### **Voicemail-aktivierter Benutzer – Verfahren**

Aktivieren eines Benutzers für Voicemail

Einschließen von Text in die E-Mail, die bei aktivierter Voicemail gesendet wird

Verwalten der Voicemaileinstellungen

Zuweisen einer UM-Postfachrichtlinie

Ändern eines UM-Wählplans

Aktivieren von Anrufen nicht UM-aktivierter Benutzer

Deaktivieren von Anrufen nicht UM-aktivierter Benutzer

Zulassen einer Sprachnachricht von Anrufern ohne Anrufer-ID

Einschließen von Text in die beim Empfang einer Sprachnachricht gesendete E-Mail

Verhindern einer Sprachnachricht von Anrufern ohne Anrufer-ID

Deaktivieren von Voicemail

Ändern einer SIP-Adresse

Ändern einer Durchwahlnummer

Hinzufügen einer SIP-Adresse

Entfernen einer SIP-Adresse

Hinzufügen einer Durchwahlnummer

Entfernen einer Durchwahlnummer

Ändern einer E.164-Nummer

Hinzufügen einer E.164-Nummer

Entfernen einer E.164-Nummer

### **Einrichten von Client-Voicemailfunktionen**

#### **Einrichten von Outlook Voice Access**

Outlook Voice Access-Befehle

Navigieren von Menüs mit Outlook Voice Access

Wiedergabe über Telefon

#### **Outlook Voice Access – Verfahren**

Aktivieren oder Deaktivieren von Outlook Voice Access

Konfigurieren einer Outlook Voice Access-Nummer

Deaktivieren ausgewählter Funktionen

Festlegen von Postfachfunktionen für Benutzer

Festlegen von Postfachfunktionen für einen Benutzer

Aktivieren oder Deaktivieren der automatischen Spracherkennung

Aktivieren einer Informationsansage

Aktivieren einer benutzerdefinierten Begrüßung

Aktivieren oder Deaktivieren der Wiedergabe über Telefon

Aktivieren oder Deaktivieren des Versands von Sprachnachrichten

Aktivieren oder Deaktivieren der Anrufweiterleitung

Konfigurieren der Gruppe von Benutzern, die von Outlook Voice Access-Benutzern kontaktiert werden können

Konfigurieren der primären Suchmethode

Konfigurieren der sekundären Suchmethode

Konfigurieren der Anzahl von Anmeldefehlern

Konfigurieren der Anzahl von Eingabefehlern

Konfigurieren der Beschränkung der persönlichen Begrüßungstexte

Schützen von Voicemail

Geschützte Voicemail – Verfahren

Konfigurieren geschützter Voicemail von authentifizierten Anrufern

Konfigurieren geschützter Voicemail von nicht authentifizierten Anrufern

Aktivieren oder Deaktivieren der Multimediamiedergabe

Festlegen des Anzeigetexts für Clients ohne Unterstützung der Windows-Rechteverwaltung

Ermöglichen der Anrufweiterleitung für Voicemailbenutzer

Weiterleiten von Anrufen – Verfahren

Mailboxansageregeln

Mailboxansageregeln in der gleichen Postfachrichtlinie

Erstellen einer Mailboxansageregel

Anzeigen und Verwalten einer Mailboxansageregel

Aktivieren oder Deaktivieren einer Mailboxansageregel für einen Benutzer

Entfernen einer Mailboxansageregel für einen Benutzer

Zulassen der Anzeige von Voicemailtranskriptionen für Benutzer

Ratgeber für Voicemailvorschau

Voicemailvorschau – Verfahren

Konfigurieren von Voicemailvorschau-Partnerdiensten

Aktivieren der Voicemailvorschau

Deaktivieren der Voicemailvorschau

MWI in Exchange Online

Zulassen von MWI-Verfahren

Zulassen von MWI an einem UM-IP-Gateway

Verhindern von MWI an einem UM-IP-Gateway

Aktivieren von MWI für Benutzer

Deaktivieren von MWI für Benutzer

Aktivieren von Benachrichtigungen über verpasste Anrufe

Deaktivieren von Benachrichtigungen über verpasste Anrufe

Autorisieren von Benutzern für Anrufe

Kurzwahlnummern, Rufnummernpräfixe und Nummernformate

Autorisieren von Benutzern für Anrufe – Verfahren

Aktivieren ausgehender Anrufe für UM-IP-Gateways

Deaktivieren ausgehender Anrufe für UM-IP-Gateways

Konfigurieren von Kurzwahlnummern

Erstellen von Wählregeln

Autorisieren von Anrufen mit Wählregeln

Einrichten von eingehenden Faxen

Faxratgeber für Exchange UM

Faxfunktion – Verfahren

Festlegen des Partnerfaxserver-URI zum Ermöglichen des Faxbetriebs

Einschließen von Text in die beim Empfang einer Faxnachricht gesendete E-Mail

Zulassen des Empfangs von Faxnachrichten für Benutzer mit demselben

Wählplan

Unterbinden des Empfangs von Faxnachrichten für Benutzer mit demselben  
Wählplan

Aktivieren der Faxfunktion für eine Gruppe von Benutzern

Deaktivieren der Faxfunktion für eine Gruppe von Benutzern

Aktivieren eines Benutzers für den Faxempfang

Unterbinden des Faxempfangs für einen Benutzer

Festlegen von Outlook Voice Access-PIN-Sicherheit

PIN-Sicherheit – Verfahren

Festlegen von PIN-Richtlinien

Zurücksetzen einer Voicemail-PIN

Abrufen von PIN-Informationen für Voicemail

Einschließen von Text in die beim Zurücksetzen einer PIN gesendete E-Mail

Festlegen der minimalen PIN-Länge

Festlegen der PIN-Gültigkeitsdauer

Festlegen der Anzahl von vorherigen PINs für die Wiederverwendung

Deaktivieren gängiger PIN-Muster

Aktivieren gängiger PIN-Muster

Festlegen der Anzahl von Anmeldefehlern vor dem Zurücksetzen der PIN

Festlegen der Anzahl von Anmeldefehlern vor dem Sperren

Ausführen von Voicemail-Anrufberichten

UM-Berichte – Verfahren

Überprüfen der Voicemailanrufe für eine Organisation

Überprüfen der Voicemailanrufe für einen Benutzer

Audioqualität von VoIP-Anrufen in der Organisation

Audioqualität von VoIP-Anrufen für einen Benutzer

Interpretieren der Daten von Voicemailanrufen

UM- und Voicemailterminologie

Clients und Mobilgeräte in Exchange Online

Exchange ActiveSync

Postfachrichtlinien für mobile Geräte

POP3 und IMAP4

Aktivieren oder Deaktivieren des POP3- oder IMAP4-Zugriffs

POP3- oder IMAP4-Einstellungen

Outlook für iOS und Android

FAQ zu Outlook für iOS und Android

Einrichten mit der modernen Authentifizierung

Verwalten von Outlook für iOS und Android

Absichern von Outlook für IOS und Android

Bereitstellen von App-Konfigurationseinstellungen

Outlook für IOS und Android in der Government Cloud

## Mobiler Zugriff

Konfigurieren der E-Mail auf dem Mobiltelefon

Remotezurücksetzung auf dem Mobiltelefon

## Outlook im Web

Outlook Web App-Postfachrichtlinien

Verfahren für Outlook Web App-Postfachrichtlinien

Erstellen einer Outlook Web App-Postfachrichtlinie

Anwenden oder Entfernen einer Outlook Web App-Postfachrichtlinie

Entfernen einer Outlook Web App-Postfachrichtlinie

Konfigurieren der Eigenschaften von Outlook Web App-Postfachrichtlinien

OWA für Geräte – Kontakte synchronisieren

Öffentliche Anlagenverarbeitung

Vermehrung des von Posteingangsregeln verwendeten Speicherplatzes

## E-Mail-Info

Konfigurieren der Größe einer großen Benutzergruppe

Konfigurieren einer benutzerdefinierten E-Mail-Info

E-Mail-Infos über Organisationsbeziehungen

Verwalten von E-Mail-Infos für Organisationsbeziehungen

## Add-Ins für Outlook

Tests der Remoteverbindungsuntersuchung

## Clientzugriffsregeln

Verfahren für Clientzugriffsregeln

Deaktivieren der Standardauthentifizierung in Exchange Online

Deaktivieren oder Aktivieren der modernen Authentifizierung in Exchange Online

## Überwachen

Verwenden von Berichten zum E-Mail-Schutz

Anpassen und Planen von Berichten zum E-Mail-Schutz

Wo befindet sich in Office 365 Übermittlungsberichte?

## Verfolgen einer E-Mail

Ausführen einer Nachrichtenablaufverfolgung und Anzeigen der Ergebnisse

Häufig gestellte Fragen zur Nachrichtenablaufverfolgung

## Sichern von E-Mails

## Beheben von Outlook-Verbindungsproblemen in Office 365 und Exchange Online

Beheben von Problemen mit Outlook und Office 365

Diagnoseprotokollierung im Support- und Wiederherstellungs-Assistenten

Suchen und Beheben von Problemen mit der E-Mail-Zustellung als Administrator von Office 365 für Unternehmen

Dienstupgrade von Exchange Online und Exchange Online Protection

Informationen zur Exchange-Dokumentation

Barrierefreiheit

Barrierefreiheit in der Exchange-Verwaltungskonsole

Erste Schritte mit der Sprachausgabe

Tastenkombinationen im Admin Center

Verwenden einer Sprachausgabe zum Hinzufügen eines Gerätewebfachs im Exchange Admin Center

Verwenden einer Sprachausgabe zum Hinzufügen eines E-Mail-Kontakts im Exchange Admin Center

Verwenden einer Sprachausgabe zum Hinzufügen eines Raumpostfachs im Exchange Admin Center

Verwenden einer Sprachausgabe zum Hinzufügen eines freigegebenen Postfachs in Exchange Admin Center 2016

Verwenden einer Sprachausgabe zum Hinzufügen von Mitgliedern zu einer Verteilergruppe im Exchange Admin Center

Verwenden einer Sprachausgabe zum Archivieren von Postfachelementen im Exchange Admin Center

Verwenden einer Sprachausgabe zum Konfigurieren der Zusammenarbeit im Exchange Admin Center

Verwenden einer Sprachausgabe zum Erstellen einer Verteilergruppe im Exchange Admin Center

Verwenden einer Sprachausgabe zum Konfigurieren von Transportregeln im Exchange Admin Center

Verwenden einer Sprachausgabe zum Definieren von Regeln zum Ver- oder Entschlüsseln von E-Mail-Nachrichten im Exchange Admin Center 2016

Verwenden einer Sprachausgabe zum Bearbeiten des Anzeigenamens eines Postfachs im Exchange Admin Center

Verwenden einer Sprachausgabe zum Exportieren und Überprüfen von Überwachungsprotokollen im Exchange Admin Center

Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im

## Exchange Admin Center

Verwenden einer Sprachausgabe zum Verwalten des Schutzes vor Schadsoftware im Exchange Admin Center

Verwenden einer Sprachausgabe zum Verwalten des Antispamschutzes

Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center

Verwenden einer Sprachausgabe zum Ausführen eines Überwachungsberichts im Exchange Admin Center

Verwenden einer Sprachausgabe zum Verfolgen einer E-Mail-Nachricht im Exchange Admin Center

Verwenden einer Sprachausgabe zum Arbeiten mit mobilen Clients im Exchange Admin Center

Exchange Online ist Teil der Office 365-Suite von Produkten.

## **Endbenutzer - finden Sie unter Office-Hilfe und Schulung**

### **Zuweisen von Administratorberechtigungen**

### **Erfahren Sie mehr über die Exchange-Verwaltungskonsole**

## **Verwalten von Exchange Online**

Als Administrator für Ihren Office 365-Mandanten sind Sie für die Verwaltung des Exchange Online-Diensts Ihrer Organisation im Exchange-Verwaltungskonsole verantwortlich. So können Sie auf das EAC zugreifen:

1. [Melden Sie sich](#) bei Office 365 mit Ihrem Geschäfts-, Schul-, oder Unikonto an, und wählen Sie dann die Kachel **Admin**.
2. Wählen Sie in der Office 365-Verwaltungskonsole **Admin zentriert / Exchange**.

Eine Einführung in finden Sie unter [Exchange Admin center in Exchange Online](#)

## **Hilfe für Office 365-Administratoren**

Wir arbeiten derzeit an der Zusammenführung der Inhalte der [Office-Hilfe und Schulungswebsite](#). Siehe hierzu:

- [Office 365 Business - Administratorhilfe](#): Erste Schritte mit Office 365 Admin Center, Zurücksetzen von Kennwörtern und mehr.
- [E-Mail in Office 365 Business - Administratorhilfe](#): Einrichten von E-Mail, Problembehebung und Importieren von E-Mails.

# Exchange Admin Center in Exchange Online

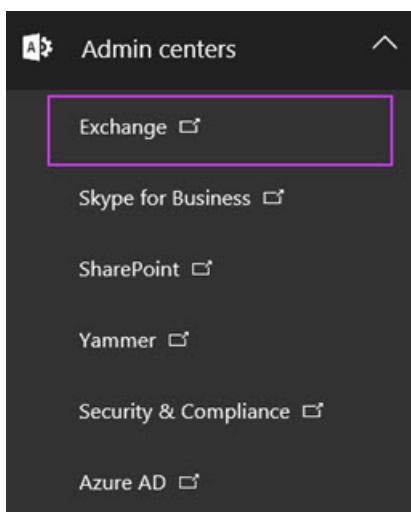
18.12.2018 • 8 minutes to read

Verwenden Sie die Exchange-Verwaltungskonsole zum Verwalten von e-Mail-Einstellungen für Ihre Organisation.

## Wechseln zum Exchange Admin Center

Sie benötigen [Administratorberechtigungen für Office 365](#) für die Exchange-Verwaltungskonsole.

1. Melden Sie sich bei Office 365 mit Ihrem Geschäfts-, Schul-, oder Unikonto an, und wählen Sie dann die Kachel **Admin**.
2. Wählen Sie im Office 365 Admin Center die Optionen **Admin > Exchange**.



## Exchange Admin Center-features

Nachfolgend finden Sie im Exchange Administrationscenter aussieht.

The screenshot illustrates the Exchange admin center's mailbox management interface. The left sidebar lists various administrative categories. The main area displays a list of mailboxes, and a details pane on the right provides detailed information for a selected mailbox.

**Feature pane**

**Tabs**: mailboxes, groups, resources, contacts, shared, migration

**Toolbar**: edit, search, more

**List view**

**Details pane**

DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
Administrator	User	Administrator@tailspintoys.com
Amy E. Alberts	User	amy@tailspintoys.com
Antonio Alwan	User	antonio@tailspintoys.com
Gigdem Akin	User	Gigdem@tailspintoys.com
<b>Dimple Arya</b>	<b>User</b>	<b>Dimple@tailspintoys.com</b>
James Alvord	User	james@tailspintoys.com
Jay Hamlin	User	Jay@tailspintoys.com
Kim Akers	User	Kim@tailspintoys.com
Kweku Ako-Adjei	User	kweku@tailspintoys.com
Michael Allen	User	michael@tailspintoys.com
Pilar Ackerman	User	Pilar@tailspintoys.com

1 selected of 8 total

## Featurebereich

Hier sind die Funktionen, die sich in der linken Navigationsleiste befinden.

BEREICH	AKTION
<b>Dashboard</b>	Eine Übersicht des Admin Centers.
<b>Empfänger</b>	Anzeigen und Verwalten von Postfächern, Gruppen, Ressourcenpostfächern, Kontakten, freigegebenen Postfächern sowie Postfachmigrationen.
<b>Berechtigungen</b>	Verwalten von Administrator- und Benutzerrollen sowie Outlook Web App-Richtlinien.
<b>Verwaltung der Richtlinientreue</b>	Verwalten der In-Situ-eDiscovery, In-Situ-Speicher, Überwachung, Verhinderung von Datenverlust, Aufbewahrungsrichtlinien, Aufbewahrungstags und Journalregeln.
<b>Organization (Organisation)</b>	Verwalten von organisationsfreigabe und apps für Outlook
<b>Schutz</b>	Verwalten der Schadsoftwarefilter, Verbindungsfilter, Inhaltsfilter, ausgehender Spammnachrichten und Quarantäne für Ihre Organisation.
<b>Nachrichtenfluss</b>	Verwalten von Regeln, Nachrichtenverfolgung, akzeptierten Domänen, Remotedomänen und Connectors.

BEREICH	AKTION
<b>Mobil</b>	Verwalten von mobilen Geräten, über die Sie Verbindungen mit Ihrer Organisation zulassen. Sie können den Zugriff auf und die Richtlinien für mobile Geräte verwalten.
<b>Öffentliche Ordner</b>	Verwalten öffentlicher Ordner und öffentlicher Ordnerpostfächer.
<b>Unified Messaging</b>	Verwalten von UM-Wählplänen und UM-IP-Gateways.

## Registerkarten

Die Registerkarten sind Ihre zweite Ebene der Navigation. Alle Featurebereiche enthalten verschiedene Registerkarten, die jeweils ein vollständiges Feature repräsentieren.

## Symbolleiste

Wenn Sie die meisten Registerkarten klicken, sehen Sie eine Symbolleiste. Die Symbolleiste enthält Symbole, die eine bestimmte Aktion ausführen. In der folgenden Tabelle sind die am häufigsten verwendeten Symbole und ihre Aktionen beschrieben. Zum Anzeigen der Aktion ein Symbol zugeordnet ist, zeigen Sie einfach auf das Symbol.

SYMBOL	NAME	ACTION
	Hinzufügen, Neu	Erstellen eines neuen Objekts. Bei einigen dieser Symbole gibt es einen dazugehörigen nach unten zeigenden Pfeil, auf den Sie klicken können, um weitere Objekte anzuzeigen, die Sie erstellen können. Beispielsweise in <b>Empfänger &gt; Gruppen</b> , durch Klicken auf den Pfeil nach unten <b>Verteilergruppe, Sicherheitsgruppe und dynamische Verteilergruppe</b> als zusätzliche Optionen angezeigt.
	Bearbeiten	Bearbeiten eines Objekts.
	Löschen	Löschen eines Objekts. Über dieses Symbol können Sie ein Objekt löschen. Bei einigen Löschsymbolen gibt es einen nach unten zeigenden Pfeil, auf den Sie zum Einblenden weiterer Optionen klicken können.
	Suche	Öffnen eines Suchfelds, in das Sie den Suchbegriff für ein zu suchendes Objekt eingeben können.
	n/v	Upgrade einer Verteilergruppe auf eine Office 365-Gruppe. Dieses Symbol kann nur für eine Verteilergruppe verwendet werden.
	Aktualisieren	Aktualisieren der Listenansicht.

SYMBOL	NAME	ACTION
	Weitere Optionen	Anzeigen weiterer Aktionen, die Sie für die Objekte dieser Registerkarte ausführen können. Beispielsweise in <b>Empfänger</b> > <b>Postfächer</b> durch Klicken auf dieses Symbol zeigt die folgenden Optionen: <b>Spalten hinzufügen/entfernen</b> , <b>Gelöschte Postfächer</b> , <b>Exportieren von Daten in eine CSV-Datei</b> und <b>Erweiterte Suche</b> .
	Pfeil nach oben und Pfeil nach unten	Verschieben Sie die Priorität eines Objekts nach oben oder unten. Beispielsweise in <b>E-Mail-Fluss</b> > <b>Regeln</b> klicken Sie auf den Pfeil nach oben, um die Priorität einer Regel auszulösen. Sie können diese Pfeile auch verwenden, um die Hierarchie Öffentlicher Ordner zu navigieren.
	Kopieren	Kopieren eines Objekts, damit Sie es ändern können, ohne das ursprüngliche Objekt zu ändern. Wählen Sie beispielsweise in <b>Berechtigungen</b> > <b>Administratorrollen</b> in der Listenansicht eine Rolle aus, und klicken Sie auf dieses Symbol. Nun können Sie eine neue Rollengruppe erstellen, die auf einer vorhandenen Rollengruppe basiert.
	Entfernen	Entfernen eines Elements aus einer Liste. Im Dialogfeld <b>Berechtigungen für Öffentliche Ordner</b> können Sie beispielsweise Benutzer aus der Liste der Benutzer entfernen, die auf den öffentlichen Ordner zugreifen dürfen, indem Sie den Benutzer auswählen und auf dieses Symbol klicken.

## Listenansicht

Wenn Sie eine Registerkarte auswählen, wird Sie in den meisten Fällen eine Listenansicht angezeigt. Die Listenansicht im Exchange Administrationscenter ist darauf ausgelegt, um Einschränkungen, die vorhanden waren in Exchange-Systemsteuerung zu entfernen.

In Exchange Online ist der sichtbare Grenzwert von in der Listenansicht für Exchange Admin Center ungefähr 10.000 Objekte. Darüber hinaus ist Paging enthalten, damit Sie auf die Ergebnisse navigieren können. In der Listenansicht **Empfänger** können Sie auch Seitengröße konfigurieren und die Daten in eine CSV-Datei exportieren.

## Detailbereich

Wenn Sie in der Listenansicht ein Element auswählen, werden Informationen zu diesem Objekt im Detailbereich angezeigt.

Klicken Sie zum \\*\\*Bearbeiten mehrerer Elemente\\*\\* bei gedrückter STRG-TASTE auf die für die

Massenbearbeitung gewünschten Objekte, und wählen Sie anschließend im Detailbereich die Optionen aus. ###  
Konsolen-Kachel, Ich-Kachel und Hilfe

Die Kachel Ressourcencenter können Sie eine Administrationscenter zu ändern. Der eigene Kachel können Sie der Exchange-Verwaltungskonsole abmelden und als anderer Benutzer anmelden. Von der Hilfe ? Dropdown-Menü, können Sie die folgenden Aktionen ausführen:

- **Hilfe:** Klicken Sie auf ? zum Anzeigen der online-Hilfe-Inhalten.
- **Blase Hilfe zu deaktivieren:** unterstützen der Blase zeigt kontextbezogene Hilfe für Felder beim Erstellen oder bearbeiten und -Objekts. Sie können die Hilfe Blase Hilfe deaktivieren oder auf aktivieren, wenn sie deaktiviert wurde.

## Unterstützte Browser

Lesen Sie die folgenden Artikel:

- [Systemanforderungen für Office 365](#): Listen unterstützte Browser für Office 365 und Exchange-Verwaltungskonsole.
- [Unterstützte Browser für Outlook Web App](#).

## Verwandte Artikel

Verwenden Sie die Exchange-Server? Finden Sie unter [Exchange Admin center in Exchange Server](#).

Verwenden Sie Exchange Online Protection (EOP)? Weitere Informationen dazu finden Sie unter [Exchange admin center in Exchange Online Protection](#).

# Berechtigungen in Exchange Online

18.12.2018 • 31 minutes to read

Exchange Online inOffice 365 umfasst diverse vordefinierte Berechtigungen, die auf dem RBAC-Berechtigungsmodell (Role Based Access Control, rollenbasierte Zugriffssteuerung) basieren und zur problemlosen Zuweisung von Berechtigungen zu Administratoren und Benutzern umgehend verwendet werden können. Mithilfe der Berechtigungsfunktionen in Exchange Online können Sie die Einrichtungs- und Bereitstellungsschritte einer neuen Organisation schnell ausführen.

RBAC ist auch das Modell der Berechtigungen, das in Microsoft Exchange Server verwendet wird. Die meisten der Links in diesem Thema finden Sie Themen, die Exchange-Server zu verweisen. Die Konzepte in diesen Themen gelten auch für Exchange Online.

Informationen zu Berechtigungen in Office 365 finden Sie unter [Berechtigungen in Office 365](#).

## NOTE

Verschiedene Funktionen und Konzepte der rollenbasierten Zugriffssteuerung werden in diesem Thema nicht behandelt, da es sich um erweiterte Funktionen handelt. Wenn Sie Ihre Anforderungen mit den in diesem Thema erläuterten Funktionen nicht erfüllen können und Ihr Berechtigungsmodell zusätzlich anpassen möchten, finden Sie unter [Understanding Role Based Access Control](#) weitere Informationen.

## Rollenbasierte Berechtigungen

In Exchange Online basieren die Berechtigungen, mit denen Administratoren und Benutzern erteilen auf Verwaltungsrollen. Eine Verwaltungsrolle definiert die Gruppe von Aufgaben, die ein Administrator oder Benutzer ausführen können. Beispielsweise eine Verwaltungsrolle aufgerufen `Mail Recipients` definiert die Aufgaben, die einer Person auf einem Satz von Postfächern, Kontakten und Verteilergruppen ausführen können. Wenn ein Administrator oder Benutzer eine Verwaltungsrolle zugeordnet wird, erhält die Person die Berechtigungen von der Verwaltungsrolle bereitgestellt.

Administratorrollen und Endbenutzerrollen sind die beiden Arten von Verwaltungsrollen. Es folgt eine Kurzbeschreibung der einzelnen Typen:

- **Administratorrollen:** Diese Rollen enthalten Berechtigungen, mit denen Administratoren oder spezialisierten Benutzern mithilfe von Rollengruppen, die Bestandteil der Exchange Online-Organisation, beispielsweise Empfänger, Verwaltung der Richtlinientreue oder Unified Messaging verwalten zugewiesen werden können .
- **Endbenutzerrollen:** dieser Rollen, die mit rollenzuweisungsrichtlinien zugewiesen sind, können Benutzer ihre eigenen Postfächer und Verteilerlisten Gruppen verwalten, die sie besitzen. Endbenutzerrollen beginnen mit dem Präfix `My` .

Verwaltungsrollen erteilen Berechtigungen zum Ausführen von Aufgaben für Administratoren und Benutzern von Cmdlets zur Verfügung stellen für Personen, die die Rollen zugewiesen sind. Da die Exchange-Verwaltungskonsole (EAC) und Exchange Online PowerShell-Cmdlets zum Verwalten von Exchange Online verwenden, erhält das Gewähren des Zugriffs auf ein Cmdlet die Administrator oder Benutzer die Berechtigung zum Ausführen der Aufgabe in jeder der Exchange Online Verwaltungsschnittstellen.

Exchange Online umfasst ca. 45 Rollen, die Sie zum Erteilen von Berechtigungen verwenden können. Eine Liste der Rollen finden Sie unter [Built-in Management Roles](#).

#### **NOTE**

Einige Verwaltungsrollen stehen möglicherweise nur für lokale Exchange Server-Installationen bereit und sind in Exchange Online nicht verfügbar.

## Rollengruppen und Rollenzuweisungsrichtlinien

Über Verwaltungsrollen werden Berechtigungen zum Ausführen von Aufgaben in Exchange Online erteilt. Sie brauchen jedoch eine einfache Möglichkeit, um diese Rollen Administratoren und Benutzern zuzuweisen. Exchange Online bietet zu diesem Zweck die folgenden Methoden:

- **Rollengruppen:** Rollengruppen können Sie Administratoren und spezialisierten Benutzern Berechtigungen gewähren.
- **Rollenzuweisungsrichtlinien:** rollenzuweisungsrichtlinien können Sie zum Erteilen von Berechtigungen für Endbenutzer zum Ändern der Einstellung auf ihren eigenen Postfächern oder Verteilergruppen Gruppen, die sie besitzen.

Die nachstehenden Abschnitten enthalten weitere Informationen zu Rollengruppen und Rollenzuweisungsrichtlinien.

### **Rollengruppen**

Jeder Administrator, der Exchange Online verwaltet werden, muss mindestens einer oder mehreren Rollen zugewiesen werden. Administratoren möglicherweise mehr als eine Rolle, weil mit diesen Auftrag Funktionen erzielt werden können, die mehrere Bereiche in Exchange Online umfassen. Ein Administrator kann beispielsweise Empfänger und Unified Messaging-Funktionen in Exchange Online-Organisation verwalten. In diesem Fall dem Administrator möglicherweise zugewiesen werden sowohl die **Mail Recipients** und **Unified Messaging** Rollen.

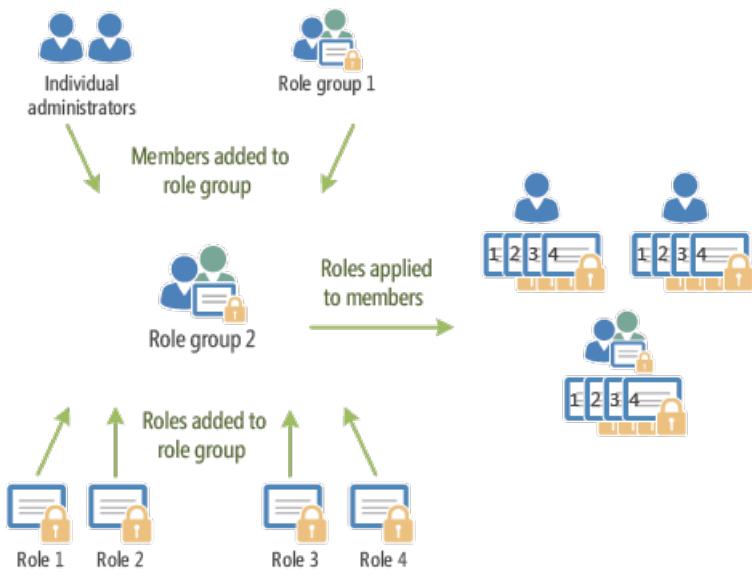
Um die Zuweisung mehrerer Rollen zu einem Administrator zu vereinfachen, umfasst Exchange Online Rollengruppen. Beim Zuweisen einer Rolle zu einer Rollengruppe werden die Berechtigungen der Rolle allen Mitgliedern der Rollengruppe erteilt. So können Sie mehreren Rollengruppenmitgliedern gleichzeitig eine Vielzahl von Rollen zuweisen. Rollengruppen gelten typischerweise für umfassendere Verwaltungsbereiche, z. B. die Empfängerverwaltung. Sie werden ausschließlich mit Administratorrollen und nicht mit Endbenutzerrollen verwendet. Rollengruppenmitglieder können Exchange Online-Benutzer und andere Rollengruppen sein.

#### **NOTE**

Eine Rolle kann einem Benutzer direkt und ohne Verwendung einer Rollengruppe zugewiesen werden. Diese Methode zur Rollenzuweisung ist jedoch ein erweitertes Verfahren, das in diesem Thema nicht behandelt wird. Es wird empfohlen, zur Verwaltung von Berechtigungen Rollengruppen einzusetzen.

Die folgende Abbildung zeigt die Beziehung zwischen Benutzern, Rollengruppen und Rollen.

### **Rollen, Rollengruppen und Rollengruppenmitglieder**



Exchange Online umfasst eine Vielzahl von integrierten Rollengruppen, die jeweils Berechtigungen zum Verwalten bestimmter Bereiche in Exchange Online bieten. Bei einigen Rollengruppen gibt es möglicherweise Überschneidungen. In der folgenden Tabelle sind die einzelnen Rollengruppen sowie eine Beschreibung ihrer Verwendung aufgeführt.

### Integrierte Rollengruppen

ROLLENGRUPPE	BESCHREIBUNG
Unternehmensadministratoren ( <b>TenantAdmins_{eindeutiger Wert}</b> )	Die Rollengruppe "Unternehmensadministratoren" ist eine spezielle Rollengruppe, die die Rolle "Globale Administratoren" für Office 365 und die Exchange Online-Rollengruppe "Organisationsverwaltungsrolle" zusammenführt. Der Rollengruppe "Unternehmensadministratoren" sind keine Rollen zugewiesen. Sie gehört jedoch der Rollengruppe "Organisationsverwaltung" an und erbt die von dieser Rollengruppe bereitgestellte Berechtigung. Diese Rollengruppe kann nicht in Exchange Online verwaltet werden. Sie können dieser Rollengruppe Mitglieder hinzufügen, indem Sie Benutzer zur Office 365-Rolle der globalen Administratoren hinzufügen.
Discoveryverwaltung	Administratoren oder Benutzer, die Mitglied der Rollengruppe Discoveryverwaltung sind, können Postfächer in der Exchange Online-Organisation nach Daten durchsuchen, die mit bestimmten Kriterien übereinstimmen. Zudem können diese Mitglieder eine rechtliche Aufbewahrungspflicht für Postfächer konfigurieren.
Helpdesk	Die Helpdesk-Rollengruppe ermöglicht ihren Mitgliedern standardmäßig das Anzeigen und Ändern der Microsoft Outlook Web App-Optionen aller Benutzer in der Organisation. Zu diesen Optionen gehört mitunter das Ändern des Anzeigennamens, der Adresse und der Telefonnummer des Benutzers. Optionen, die in den Outlook Web App-Optionen nicht verfügbar sind, beispielsweise die Änderung der Postfachgröße oder die Konfiguration der Postfachdatenbank, in der sich ein Postfach befindet, gehören nicht dazu.

ROLLENGRUPPE	BESCHREIBUNG
Help Desk-Administratoren ( <b>HelpdeskAdmins_&lt;eindeutiger Wert&gt;</b> )	Der Rollengruppe "Help Desk-Administratoren" sind keine Rollen zugewiesen. Sie gehört jedoch der Rollengruppe "Organisationsverwaltung" (nur Leserechte) an und erbt die von dieser Rollengruppe bereitgestellten Berechtigungen. Diese Rollengruppe kann nicht in Exchange Online verwaltet werden. Sie können dieser Rollengruppe Mitglieder hinzufügen, indem Sie Benutzer zur Kennwort-Administratorrolle für Office 365 hinzufügen.
Organisationsverwaltung	Administratoren, die Mitglieder der Rollengruppe "Organisationsverwaltung" sind, haben Administratorzugriff für die gesamte Exchange Online-Organisation und ausführen, beinahe jede Aufgabe für jede Exchange Online-Objekt, mit einigen Ausnahmen, wie die <b>Discovery Management</b> Rolle. > [!IMPORTANT]> Da die Rollengruppe Organisationsverwaltung sehr viele Berechtigungen umfasst, sollten nur Benutzer, die Administratoraufgaben auf Organisationsebene mit potenziellen Auswirkungen auf die gesamte Exchange Online-Organisation ausführen, Mitglieder dieser Rollengruppe sein.
Empfängerverwaltung	Administratoren, die Mitglied der Rollengruppe Empfängerverwaltung sind, haben Administratorzugriff zum Erstellen oder Ändern von Exchange Online-Empfängern innerhalb der Exchange Online-Organisation.
Datensatzverwaltung	Benutzer, die Mitglieder der Rollengruppe Datensatzverwaltung sind, können Funktionen zur Einhaltung von Vorschriften konfigurieren, z. B. Aufbewahrungsrichtlinientags, Nachrichtenklassifikationen und Transportregeln.
UM-Verwaltung	Administratoren, die Mitglied der UM-Verwaltungsrollengruppe sind, können in der Exchange Online-Organisation Einstellungen wie die UM-Eigenschaften für Postfächer, UM-Telefonansagen und die Konfiguration automatischer UM-Telefonzentralen verwalten.
Schreibgeschützte Organisationsverwaltung	Administratoren, die Mitglied der Rollengruppe Organisationsverwaltung - nur Leserechte sind, können die Eigenschaften aller Objekte in der Exchange Online-Organisation anzeigen.

Wenn Sie eine kleine Organisation, die nur wenige Administratoren verfügt arbeiten, müssen Sie möglicherweise die Rollengruppe "Organisationsverwaltung" nur Administratoren hinzugefügt, und müssen Sie möglicherweise noch nie anderen Rollengruppen verwenden. Wenn Sie in einer größeren Organisation arbeiten, müssen Sie Administratoren, die bestimmte Aufgaben Verwalten von Exchange Online, wie Empfänger oder organisationsweiten Unified Messaging-Konfiguration. In diesen Fällen können Sie die UM-verwaltungsrollengruppe ein Administrator sein, um die Rollengruppe "Recipient Management" und ein anderer Administrator hinzufügen. Administratoren können Sie ihre spezifische Bereiche innerhalb des ExchangeOnline verwalten, aber sie keine Berechtigungen zum Verwalten von Bereichen, die nicht für zuständig sind.

Wenn die integrierten Rollengruppen in Exchange Online nicht für die Aufgabenbereiche Ihrer Administratoren geeignet sind, können Sie Rollengruppen erstellen und Rollen zu diesen Gruppen hinzufügen. Weitere Informationen finden Sie weiter unten in diesem Thema im Abschnitt **Arbeiten mit Rollengruppen**.

## Rollenzuweisungsrichtlinien

Exchange Online bietet Richtlinien zur Rollenzuweisung, mit denen Sie steuern können, welche Einstellungen Benutzer für eigene Postfächer und Verteilergruppen konfigurieren können. Diese Einstellungen umfassen den Anzeigenamen, Kontaktinformationen, Voicemaileinstellungen und die Mitgliedschaft in Verteilergruppen.

Um für die verschiedenen Typen von Benutzern innerhalb der Organisation unterschiedliche Berechtigungsebenen zu implementieren, kann eine Exchange Online-Organisation über mehrere Rollenzuweisungsrichtlinien verfügen. Einige Benutzer können abhängig von der ihrem Postfach zugeordneten Rollenzuweisungsrichtlinie z. B. zum Ändern ihrer Adresse oder Erstellen von Verteilergruppen berechtigt sein, während andere Benutzer diese Aufgaben nicht ausführen dürfen. Rollenzuweisungsrichtlinien werden direkt zu Postfächern hinzugefügt, und jedem Postfach kann nur jeweils eine Rollenzuweisungsrichtlinie zugeordnet sein.

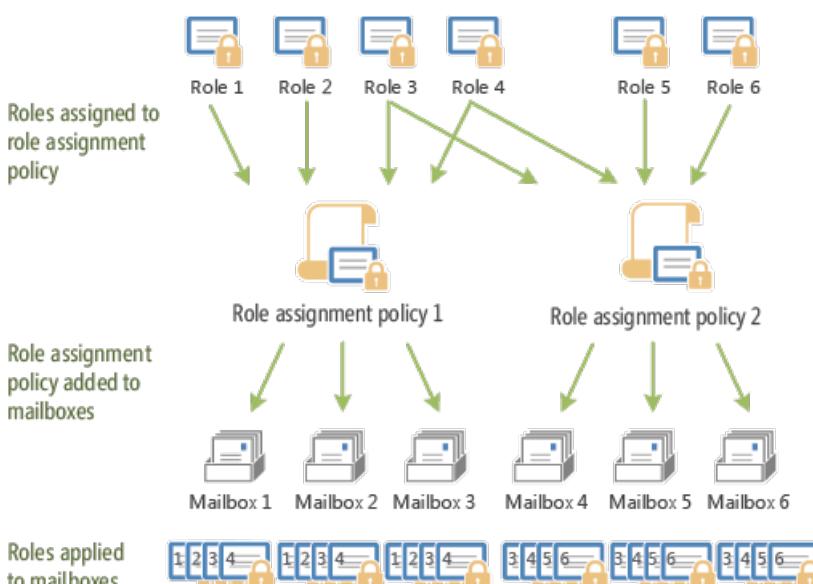
Eine Rollenzuweisungsrichtlinie in Ihrer Organisation ist als Standardrichtlinie gekennzeichnet. Die Standardrichtlinie für die Rollenzuweisung wird neuen Postfächern zugeordnet, denen bei der Erstellung nicht explizit eine Rollenzuweisungsrichtlinie zugeordnet wird. Die Standardrichtlinie für die Rollenzuweisung sollte die Berechtigungen umfassen, die dem Großteil Ihrer Postfächer erteilt werden sollen.

Berechtigungen werden endbenutzerrollen mit rollenzuweisungsrichtlinien hinzugefügt. Endbenutzerrollen beginnen mit `My` und gewähren von Berechtigungen für Benutzer nur ihre Postfächer oder Verteilergruppen Gruppen verwalten, deren Besitzer Sie sind. Sie können nicht zum Verwalten von allen anderen Postfächern verwendet werden. Rollenzuweisungsrichtlinien können nur endbenutzerrollen zugewiesen werden.

Beim Zuweisen einer Endbenutzerrolle zu einer Rollenzuweisungsrichtlinie erhalten alle Postfächer, die dieser Rollenzuweisungsrichtlinie zugeordnet sind, die über die Rolle erteilten Berechtigungen. So können Sie Berechtigungen zu einer Gruppe von Benutzern hinzufügen oder von dieser Gruppe entfernen, ohne einzelne Postfächer konfigurieren zu müssen. Die Abbildung unten zeigt Folgendes:

- Endbenutzerrollen werden Rollenzuweisungsrichtlinien zugewiesen. Rollenzuweisungsrichtlinien können dieselben Endbenutzerrollen gemeinsam verwenden.
- Rollenzuweisungsrichtlinien werden Postfächern zugeordnet. Jedem Postfach kann nur eine Rollenzuweisungsrichtlinie zugeordnet werden.
- Nachdem einem Postfach eine Rollenzuweisungsrichtlinie zugeordnet wurde, werden die Endbenutzerrollen auf das Postfach angewendet. Die über die Rollen erteilten Berechtigungen werden dem Benutzer des Postfachs zugewiesen.

## Rollen, Rollenzuweisungsrichtlinien und Postfächer



Die Rollenzuweisungsrichtlinie "Standardrichtlinie für Rollenzuweisung" ist in Exchange Online enthalten. Wie

der Name schon sagt, handelt es sich um die Standardrichtlinie für Rollenzuweisung. Informationen zum Ändern der mit dieser Rollenzuweisungsrichtlinie bereitgestellten Berechtigungen oder zum Erstellen von Rollenzuweisungsrichtlinien finden Sie unter [Arbeiten mit Rollenzuweisungsrichtlinien](#) weiter unten in diesem Thema.

## Office 365-Berechtigungen in Exchange Online

Wenn Sie einen Benutzer in Office 365 erstellen, können Sie angeben, ob diesem verschiedenen Administratorrollen zugewiesen werden sollen, wie zum Beispiel Globaler Administrator, Service-Administrator, Kennwort-Administrator. Einige, jedoch nicht alle Office 365-Rollen gewähren dem Benutzer Administratorberechtigungen in Exchange Online.

### NOTE

Der Benutzer, der zur Erstellung Ihres Office 365-Mandanten verwendet wurde, wird der Globalen Administratorrolle für Office 365 zugewiesen.

In der nachstehenden Tabelle sind die Office 365-Rollen und die dazugehörigen Exchange Online-Rollengruppen aufgeführt.

OFFICE 365-ROLLE	EXCHANGE ONLINE-ROLLENGRUPPE
Globaler Administrator	Organisationsverwaltung <b>Hinweis:</b> der globalen Administratorrolle und der Rollengruppe "Organisationsverwaltung" zusammen mit einer spezielle Unternehmensadministrator Rollengruppe gebunden sind. Die Unternehmensadministrator Rollengruppe wird intern von Exchange Online verwaltet und kann nicht direkt geändert werden.
Abrechnungsadministrator	Keine entsprechende Exchange Online-Rollengruppe.
Kennwort-Administrator	Help Desk-Administrator.
Service-Administrator	Keine entsprechende Exchange Online-Rollengruppe.
Benutzerverwaltungsadministrator	Keine entsprechende Exchange Online-Rollengruppe.

Eine Beschreibung der Exchange Online-Rollengruppen finden Sie in der Tabelle "Integrierte Rollengruppen" in [Rollengruppen](#).

Wenn Sie einen Benutzer zu den Rollen "Globaler Administrator" oder "Kennwort-Administrator" für Office 365 hinzufügen, erhält der Benutzer die von der entsprechenden Exchange Online-Rollengruppe gewährten Rechte. Für andere Office 365-Rollen existiert keine entsprechende Exchange Online-Rollengruppe und gewähren keine administrativen Berechtigungen in Exchange Online. Weitere Informationen zum Zuweisen von Office 365-Rollen zu Benutzern finden Sie unter [Zuweisen von Adminrollen](#).

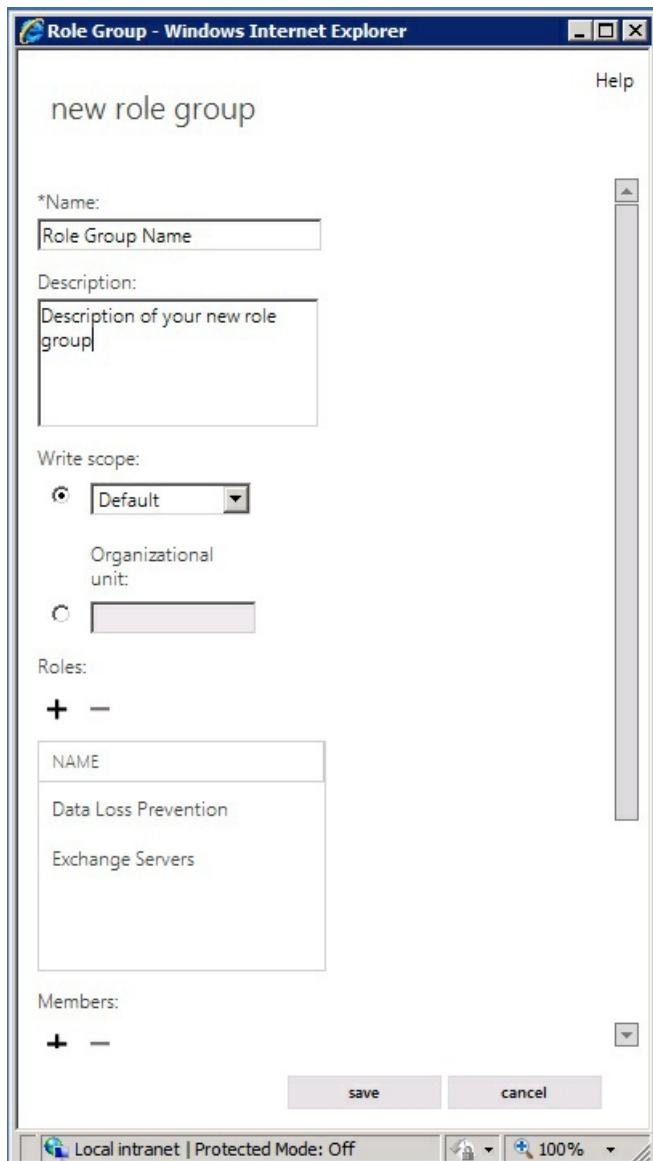
Benutzern können administrative Rechte in Exchange Online gewährt werden, ohne dass diese Office 365-Rollen zugewiesen werden. Hierzu wird der Benutzer als Mitglied einer Exchange Online-Rollengruppe hinzugefügt. Wird ein Benutzer direkt zu einer Exchange Online-Rollengruppe hinzugefügt, erhält dieser die von dieser Rolle in Exchange Online gewährten Berechtigungen. Er erhält jedoch keine Berechtigungen für andere Office 365-Komponenten. Er verfügt ausschließlich in Exchange Online über administrative Berechtigungen. Benutzer können allen in der Tabelle "Integrierte Rollengruppen" in [Rollengruppen](#) aufgeführten Rollengruppen hinzugefügt werden, mit Ausnahme der Rollengruppen "Unternehmensadministrator" und "Help Desk-Administrator". Weitere Informationen zum direkten Hinzufügen von Benutzern zu einer Exchange Online-

Rollengruppe finden Sie unter [Arbeiten mit Rollengruppen](#).

## Arbeiten mit Rollengruppen

Am besten verwenden Sie zum Verwalten der Berechtigungen mithilfe von Rollengruppen in Exchange Online die Exchange-Verwaltungskonsole. Wenn Sie zum Verwalten von Rollengruppen die Exchange-Verwaltungskonsole verwenden, können Sie mit ein paar Mausklicks Rollen und Mitglieder hinzufügen und entfernen, Rollengruppen erstellen oder Rollengruppen kopieren. Um diese Aufgaben auszuführen, bietet die Exchange-Verwaltungskonsole einfache Dialogfelder wie das in der folgenden Abbildung gezeigte Dialogfeld **Neue Rollengruppe**.

### Dialogfeld "Neue Rollengruppe" in der Exchange-Verwaltungskonsole



Exchange Online enthält mehrere Rollengruppen, die Berechtigungen in spezielle Verwaltungsbereiche einteilen. Wenn diese vorhandenen Rollengruppen die Berechtigungen bieten, die Ihre Administratoren zum Verwalten der Exchange Online-Organisation benötigen, müssen Sie die Administratoren lediglich als Mitglieder der entsprechenden Rollengruppen hinzufügen. Nachdem Sie Administratoren zu einer Rollengruppe hinzugefügt haben, können diese die Funktionen im Zusammenhang mit dieser Rollengruppe verwalten. Um Mitglieder einer Rollengruppe hinzuzufügen oder aus dieser zu entfernen, öffnen Sie die Rollengruppe in der Exchange-Verwaltungskonsole, und fügen Sie der Mitgliedschaftsliste Mitglieder hinzu bzw. entfernen Sie Mitglieder daraus. Eine Liste der integrierten Rollengruppen finden Sie in der Tabelle "Integrierte Rollengruppen" in [Rollengruppen](#).

#### **IMPORTANT**

Wenn ein Administrator Mitglied mehrerer Rollengruppen ist, erteilt Exchange Online dem Administrator die Berechtigungen aller Rollengruppen, in denen er Mitglied ist.

Wenn keine der in Exchange Online enthaltenen Rollengruppen die erforderlichen Berechtigungen bietet, können Sie über die Exchange-Verwaltungskonsole eine Rollengruppe erstellen und dieser die Rollen mit den erforderlichen Berechtigungen hinzufügen. Für eine neue Rollengruppe führen Sie die folgenden Aufgaben aus:

1. Auswählen eines Namens für die Rollengruppe.
2. Auswählen der Rollen, die zur Rollengruppe hinzugefügt werden sollen.
3. Hinzufügen von Mitgliedern zur Rollengruppe.
4. Speichern der Rollengruppe.

Nach dem Erstellen der Rollengruppe wird diese wie alle anderen Rollengruppen verwaltet.

Wenn eine vorhandene Rollengruppe einige, jedoch nicht alle erforderlichen Berechtigungen bietet, können Sie die Rollengruppe kopieren und anschließend Änderungen vornehmen, um eine neue Rollengruppe zu erstellen. Sie können eine vorhandene Rollengruppe kopieren und ändern, ohne dass sich dies auf die ursprüngliche Rollengruppe auswirkt. Wenn Sie die Rollengruppe kopieren, können Sie einen neuen Namen und eine Beschreibung angeben, Rollen zur neuen Rollengruppe hinzufügen oder aus dieser entfernen und neue Mitglieder hinzufügen. Beim Erstellen oder Kopieren einer Rollengruppe verwenden Sie erneut das in der Abbildung oben gezeigte Dialogfeld.

Vorhandene Rollengruppen können ebenfalls geändert werden. Über ein Dialogfeld in der Exchange-Verwaltungskonsole, das dem oben gezeigten Dialogfeld ähnelt, können Sie Rollen vorhandenen Rollengruppen hinzufügen bzw. aus diesen Gruppen entfernen und gleichzeitig Mitglieder hinzufügen oder entfernen. Durch das Hinzufügen und Entfernen von Rollen zu bzw. aus Rollengruppen aktivieren und deaktivieren Sie Verwaltungsfunktionen für Mitglieder dieser Rollengruppe.

#### **NOTE**

Wenngleich Sie ändern können, welche Rollen integrierten Rollengruppen zugewiesen sind, sollten Sie die integrierten Rollengruppen stattdessen kopieren, die Kopie der Rollengruppe ändern und anschließend Mitglieder zur Kopie der Rollengruppe hinzufügen. > Die Rollengruppen "Unternehmensadministrator" und "Help Desk-Administrator" können nicht kopiert oder geändert werden.

## [Rollenbasierte Berechtigungen](#)

## Arbeiten mit Rollenzuweisungsrichtlinien

Am besten verwenden Sie die Exchange-Verwaltungskonsole, um die Berechtigungen zu verwalten, die Sie Endbenutzern zum Verwalten ihrer eigenen Postfächer in Exchange Online zuweisen. Wenn Sie zum Verwalten von Endbenutzerberechtigungen die Exchange-Verwaltungskonsole verwenden, können Sie mit ein paar Mausklicks Rollen hinzufügen und entfernen oder Rollenzuweisungsrichtlinien erstellen. Um diese Aufgaben auszuführen, bietet die Exchange-Verwaltungskonsole einfache Dialogfelder wie das in der folgenden Abbildung gezeigte Dialogfeld **Rollenzuweisungsrichtlinie**.

### **Dialogfeld "Rollenzuweisungsrichtlinie" in der Exchange-Verwaltungskonsole**

**Role Assignment Policy - Windows Internet Explorer**

## role assignment policy

\*Name:  
New Role Assignment policy

Description:  
Description for your new role assignment policy

Contact information:

MyContactInformation  
 This role enables individual users to modify their contact information, including address and phone numbers.

MyAddressInformation  
 This role enables individual users to view and modify their street address and work telephone and fax numbers. This is a custom role created from the "MyContactInformation" parent role.

MyMobileInformation  
 This role enables individual users to view and modify their mobile telephone and pager numbers. This is a custom role created from the "MyContactInformation" parent role.

MyPersonalInformation  
 This role enables individual users to view and modify their Web site address and home telephone number. This is a custom

**save** **cancel**

Local intranet | Protected Mode: Off 100%

Exchange Online umfasst eine Standard-Rollenzuweisungsrichtlinie. Benutzer, deren Postfächer dieser Rollenzuweisungsrichtlinie zugeordnet sind, können folgende Aufgaben ausführen:

- Beitreten zu oder Verlassen von Verteilergruppen, die Mitgliedern das Verwalten der eigenen Mitgliedschaft gestatten.
- Anzeigen und Ändern grundlegender Postfacheinstellungen ihrer eigenen Postfächer. Dazu zählen z. B. Einstellungen für Posteingangsregeln, Rechtschreibprüfung, Junk-E-Mail und Microsoft ActiveSync-Geräte.
- Ändern ihrer Kontaktinformationen, z. B. geschäftliche Adresse und Telefonnummer, Mobiltelefonnummer und Pagernummer.
- Erstellen, Ändern oder Anzeigen von Einstellungen für Textnachrichten.
- Anzeigen oder Ändern von Voicemaileinstellungen.
- Anzeigen und Ändern ihrer Marketplace-Apps.
- Erstellen von Teampostfächern und Verbinden dieser Postfächer mit Microsoft SharePoint-Listen.
- Erstellen, Ändern oder Anzeigen von Abonnementeinstellungen für E-Mails, wie z. B. Nachrichtenformat und Protokollstandards.

Um der Standardrichtlinie für Rollenzuweisung oder einer anderen Rollenzuweisungsrichtlinie Berechtigungen

hinzuzufügen oder Berechtigungen aus diesen zu entfernen, können Sie die Exchange-Verwaltungskonsole verwenden. Diese Aufgaben werden in einem Dialogfeld ausgeführt, das dem oben gezeigten ähnelt. Wenn Sie die Rollenzuweisungsrichtlinie in der Exchange-Verwaltungskonsole öffnen, aktivieren Sie die Kontrollkästchen neben den Rollen, die der Richtlinie zugewiesen werden sollen, bzw. deaktivieren Sie die Kontrollkästchen neben den Rollen, die entfernt werden sollen. Die an der Rollenzuweisungsrichtlinie vorgenommenen Änderungen werden auf alle Postfächer angewendet, die der Richtlinie zugeordnet sind.

Wenn Sie den verschiedenen Typen von Benutzern in Ihrer Organisation unterschiedliche Endbenutzerberechtigungen zuweisen möchten, können Sie Rollenzuweisungsrichtlinien erstellen. Beim Erstellen einer Rollenzuweisungsrichtlinie wird ein Dialogfeld angezeigt, das dem oben gezeigten ähnelt. Sie können einen neuen Namen für die Rollenzuweisungsrichtlinie angeben und anschließend die Rollen auswählen, die der Rollenzuweisungsrichtlinie zugewiesen werden sollen. Nach dem Erstellen einer Rollenzuweisungsrichtlinie können Sie die Richtlinie über die Exchange-Verwaltungskonsole Postfächern zuordnen.

Wenn Sie ändern, welche rollenzuweisungsrichtlinie die Standardeinstellung ist möchten, müssen Sie Exchange Online PowerShell verwenden. Wenn Sie die standardmäßigen rollenzuweisungsrichtlinie ändern, ist alle Postfächer, die erstellt werden die neuen Rolle Standardzuweisungsrichtlinie zugeordnet, wenn eine nicht explizit angegeben wurde. Die vorhandenen Postfächern zugeordnete rollenzuweisungsrichtlinie ändern nicht, wenn Sie eine neue Rolle Standardzuweisungsrichtlinie auswählen.

#### NOTE

Wenn Sie ein Kontrollkästchen für eine Rolle mit untergeordneten Rollen aktivieren, werden auch die Kontrollkästchen der untergeordneten Rollen aktiviert. Wenn Sie das Kontrollkästchen für eine Rolle mit untergeordneten Rollen deaktivieren, werden auch die Kontrollkästchen der untergeordneten Rollen deaktiviert.

## Dokumentation zu Berechtigungen

Die folgende Tabelle enthält Links zu Themen mit Informationen zu Berechtigungen und deren Verwaltung in Exchange Online.

THEMA	BESCHREIBUNG
<a href="#">Understanding Role Based Access Control</a>	Informieren Sie sich über die einzelnen RBAC-Komponenten, und erfahren Sie, wie Sie erweiterte Berechtigungsmodelle erstellen können, wenn Rollengruppen und Verwaltungsrollen nicht ausreichen.
<a href="#">Manage Role Groups</a>	Konfigurieren Sie mithilfe von Rollengruppen Berechtigungen für Exchange Online-Administratoren und spezielle Benutzer.
<a href="#">Manage Role Group Members</a>	Fügen Sie Rollengruppen Mitglieder hinzu, und entfernen Sie Mitglieder aus Rollengruppen. Durch das Hinzufügen und Entfernen von Mitgliedern in Rollengruppen, legen Sie die Personen fest, die Exchange OnlineFeatures verwalten können.
<a href="#">Manage Role Assignment Policies</a>	Konfigurieren Sie mit Rollenzuweisungsrichtlinien die Features, auf die Endbenutzer in ihren Postfächern Zugriff haben, und ändern Sie die Angabe, welche Rollenzuweisungsrichtlinie die Standardzuweisungsrichtlinie ist.
<a href="#">Change the Assignment Policy on a Mailbox</a>	Konfigurieren Sie die Rollenzuweisungsrichtlinie, die auf mindestens ein Postfach angewendet wird.

THEMA	BESCHREIBUNG
<a href="#">View Effective Permissions</a>	Zeigen Sie die Benutzer an, die über Berechtigungen zum Verwalten von Exchange Online-Features verfügen.
<a href="#">Featureberechtigungen in Exchange Online</a>	Erfahren Sie mehr über die zum Verwalten von Exchange Online-Features und -Diensten erforderlichen Berechtigungen.

# Featureberechtigungen in Exchange Online

18.12.2018 • 4 minutes to read

Die zum Ausführen von Konfigurationsaufgaben zur Verwaltung von Microsoft Exchange Online erforderlichen Berechtigungen richten sich nach dem verwendeten Verfahren bzw. nach dem Cmdlet, das Sie ausführen möchten.

Informationen zu Exchange Online Protection-Berechtigungen (EOP) finden Sie unter [Feature Permissions in EOP](#).

Führen Sie folgende Aktionen aus, um herauszufinden, welche Berechtigungen Sie zum Ausführen des Verfahrens bzw. des Cmdlets benötigen:

1. Suchen Sie in der Tabelle unten nach der Funktion, die dem Verfahren oder dem Cmdlet, das Sie ausführen möchten, am ehesten entspricht.
2. Betrachten Sie als Nächstes die für die Funktion erforderlichen Berechtigungen. Ihnen muss eine dieser Rollengruppen, eine entsprechende benutzerdefinierte Rollengruppe oder eine entsprechende Verwaltungsrolle zugewiesen sein. Sie können auch auf eine Rollengruppe klicken, um die zugehörigen Verwaltungsrollen anzuzeigen. Wenn für eine Funktion mehr als eine Rollengruppe aufgelistet wird, muss Ihnen lediglich eine der Rollengruppen zugewiesen sein, um diese Funktion nutzen zu können. Weitere Informationen zu Rollengruppen und Verwaltungsrollen finden Sie unter [Grundlegendes zur rollenbasierten Zugriffssteuerung](#).
3. Führen Sie jetzt das Cmdlet **Get-ManagementRoleAssignment** aus, um in den Ihnen zugewiesenen Rollengruppen oder Verwaltungsrollen nachzusehen, ob Sie über die zum Verwalten der Funktion erforderlichen Berechtigungen verfügen.

## NOTE

Ihnen muss die Verwaltungsrolle "Rollenverwaltung" zugewiesen sein, um das Cmdlet **Get-ManagementRoleAssignment** ausführen zu können. Wenn Sie nicht über die Berechtigungen zum Ausführen des Cmdlets **Get-ManagementRoleAssignment** verfügen, wenden Sie sich den Exchange-Administrator, um die Ihnen zugewiesenen Rollengruppen oder Verwaltungsgruppen zu erfahren.

Wenn Sie die Möglichkeit zum Verwalten einer Funktion an einen anderen Benutzer delegieren möchten, finden Sie weitere Informationen unter [Delegate a Management Role](#).

## Exchange Online-Berechtigungen

Sie können zur Verwaltung Ihrer Exchange Online-Organisation und -Empfänger die in der folgenden Tabelle aufgeführten Features verwenden. Benutzer, denen die Verwaltungsrollengruppe mit Leserechten zugewiesen ist, können die Konfiguration der Funktionen in der folgenden Tabelle anzeigen. Weitere Informationen finden Sie unter Organisationsverwaltung - nur Leserechte **View Only Organization Management**.

FUNKTION	ERFORDERLICHE BERECHTIGUNGEN
Antischadsoftware	<a href="#">Organisationsverwaltung</a> <a href="#">Hygiene Management</a>

FUNKTION	ERFORDERLICHE BERECHTIGUNGEN	
Antispam	Organisationsverwaltung Hygiene Management	
Verhinderung von Datenverlust	Organization Management Compliance Management	
Office 365-Connectors	Organization Management	
Journalarchivierung	Organization Management Recipient Management	
Verknüpfter Benutzer	Organization Management Recipient Management	
Nachrichtenübermittlung	Organization Management	
Postfacheinstellungen	Organisationsverwaltung Empfängerverwaltung	
Microsoft Office 365- Nachrichtenverschlüsselung (OME)	Organization Management Compliance Management Records Management	
Nachrichtenablaufverfolgung	Organization Management Compliance Management Help Desk	
Organisationskonfiguration	Organization Management	
Outlook auf The Web- Postfachrichtlinien	Organisationsverwaltung [Empfängerverwaltung	( <a href="http://technet.microsoft.com/library/669d602e-68e3-41f9-a455-b942d212d130.aspx">http://technet.microsoft.com/library/669d602e-68e3-41f9-a455-b942d212d130.aspx</a> )
Berechtigungen für POP3 und IMAP4	Organization Management	
Quarantäne	Organization Management Hygiene Management	
Abonnements	Organization Management Empfängerverwaltung <b>Hinweis:</b> ein Benutzer kann in ihres eigenen Postfachs Abonnements erstellen. Ein Administrator keine Abonnements im Postfach eines anderen Benutzers erstellen, aber sie können ändern oder Löschen von Abonnements im Postfach eines anderen Benutzers.	
Aufsicht	Organization Management	

FUNKTION	ERFORDERLICHE BERECHTIGUNGEN
Berichte anzeigen	<p><a href="#">Organization Management</a> - Benutzer haben Zugriff auf Postfachberichte und E-Mail-Schutzberichte.</p> <p><a href="#">View-Only Organization Management</a> - Benutzer haben Zugriff auf Postfachberichte.</p> <p><a href="#">View-Only Recipients</a> - Benutzer haben Zugriff auf E-Mail-Schutzberichte.</p> <p><a href="#">Compliance Management</a> - Benutzer haben Zugriff auf E-Mail-Schutzberichte und DLP-Berichte (Data Loss Prevention, Schutz vor Datenverlust), sofern ihr Abonnement über DLP-Funktionen verfügt.</p>

# Verwalten von Rollengruppen

18.12.2018 • 28 minutes to read

Eine Rollengruppe ist eine spezielle universelle Sicherheitsgruppe (USG), die in das Berechtigungsmodell Rolle basierend Access Control (RBAC) in Exchange Online verwendet wurde. Verwaltungsrollengruppen vereinfachen die Zuweisung und Verwaltung von Berechtigungen für Benutzer in Exchange Online. Die Mitglieder der Rollengruppe den gleichen Satz von Rollen zugewiesen sind, und Sie hinzufügen und Entfernen von Berechtigungen von Benutzern durch Hinzufügen oder Entfernen aus der Rollengruppe. Weitere Informationen zu Rollengruppen in Exchange Online finden Sie unter [Berechtigungen in Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 bis 10 Minuten
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). Klicken Sie zum Öffnen von Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Verfahren in diesem Thema benötigen Sie die Rolle Management RBAC-Rolle in Exchange Online. In der Regel erhalten Sie diese Berechtigung, über die Mitgliedschaft in der Rollengruppe "Organisationsverwaltung" (Office 365 globalen Administratorrolle).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter: [Exchange Online](#) oder [Exchange Online Protection](#).

## Anzeigen von Rollengruppen

### Verwenden der Exchange-Verwaltungskonsole zum Anzeigen von Rollengruppen

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Administratorrollen**. Hier werden alle Rollengruppen in Ihrer Organisation aufgelistet.
2. Wählen Sie aus einer Rollengruppe. Im Detailbereich werden der **Name, Beschreibung, Rollen zugewiesene, Mitglieder, verwaltet von** und der Rollengruppe **Bereich zu schreiben**. Sie können diese Informationen auch anzeigen, indem Sie auf **Bearbeiten** klicken.

### Verwenden von Exchange Online PowerShell Rollengruppen anzeigen

Wenn eine Rollengruppe anzeigen möchten, verwenden Sie die folgende Syntax:

```
Get-RoleGroup [-Identity "<Role Group Name>"] [-Filter <Filter>]
```

In diesem Beispiel wird eine Übersichtsliste aller Rollengruppen zurückgegeben.

```
Get-RoleGroup
```

In diesem Beispiel werden detaillierte Informationen für die Rollengruppe mit dem Namen Empfängeradministratoren zurückgegeben.

```
Get-RoleGroup -Identity "Recipient Administrators" | Format-List
```

Dieses Beispiel gibt alle Rollengruppen, in dem der Benutzer aufzunehmen Mitglied ist. Sie müssen den Wert DistinguishedName (DN) für aufzunehmen, verwenden Sie feststellen können, indem Sie den Befehl ausführen:

```
Get-User -Identity Julia | Format-List DistinguishedName .
```

```
Get-RoleGroup -Filter {Members -eq 'CN=Julia,OU=contoso.onmicrosoft.com,OU=Microsoft Exchange Hosted Organizations,DC=NAMPR001,DC=PROD,DC=OUTLOOK,DC=COM'}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-RoleGroup](#).

## Erstellen von Rollengruppen

Wenn Sie eine neue Rollengruppe erstellen, müssen Sie alle Einstellungen konfigurieren selbst (während der Erstellung der Gruppe oder nach). Um mit der Konfiguration von einer vorhandenen Rollengruppe zu starten und zu ändern, finden Sie unter [vorhandenen Rollengruppen kopieren](#).

### Verwenden der Exchange-Verwaltungskonsole zum Erstellen von Rollengruppen

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Administratorrollen** und klicken Sie dann auf **Hinzufügen**.

2. Konfigurieren Sie im Fenster **neue Rollengruppe** die folgenden Einstellungen:

- **Name:** Geben Sie einen eindeutigen Namen für die Rollengruppe.
- **Beschreibung:** Geben Sie eine optionale Beschreibung für die Rollengruppe.
- **Bereich schreiben:** der Standardwert ist **Standard**, aber Sie können auch auswählen, eine benutzerdefinierte empfängerschreibbereich, die Sie bereits erstellt haben.
- **Rollen:** Klicken Sie auf **Add** zum Auswählen der Rollen, die im Fenster neue Rollengruppe zugewiesen werden, die angezeigt werden soll.
- **Member:** Klicken Sie auf **Add** Auswählen der Elemente, die im Fenster neue Rollengruppe hinzuzufügen, die angezeigt werden soll. Sie können Benutzer, universellen Sicherheitsgruppen (USGs) oder anderen Rolle gruppiert (Sicherheitsprinzipale) auswählen.

Wenn Sie fertig sind, klicken Sie auf **Speichern**, um die Rollengruppe zu erstellen.

### Verwenden von Exchange Online PowerShell zum Erstellen einer Rolle

Um eine neue Rollengruppe erstellen möchten, verwenden Sie die folgende Syntax:

```
New-RoleGroup -Name "Unique Name" -Description "Descriptive text" -Roles <"Role1","Role2"...> -ManagedBy <Managers> -Members <Members> -CustomRecipientWriteScope "<Existing Write Scope Name>"
```

- Der **Rollen**-Parameter gibt die Verwaltungsrollen Rollengruppe zuweisen, indem Sie mit der folgenden Syntax `"Role1","Role1",..."RoleN"`. Sie können die verfügbaren Rollen sehen, mit dem Cmdlet **Get-ManagementRole**.
- Der Parameter **Members** gibt die Mitglieder der Rollengruppe mithilfe der folgenden Syntax an: `"Member1","Member2",..."MemberN"`. Sie können angeben, dass Benutzer, universellen Sicherheitsgruppen (USGs) oder anderen Rollen (Sicherheitsprinzipale) gruppiert.

- Der Parameter *ManagedBy* gibt die Stellvertretungen eingerichtet, die ändern können, und die Rollengruppe entfernen, indem Sie mit der folgenden Syntax: `"Delegate1","Delegate2",..."DelegateN"`. Beachten Sie, dass diese Einstellung nicht in der Exchange-Verwaltungskonsole verfügbar ist.
- Der Parameter *CustomRecipientWriteScope* gibt an, der vorhandenen benutzerdefinierten empfängerschreibbereich der Rollengruppe zuweisen. Sie können den verfügbaren benutzerdefinierten Empfänger Bereiche zu schreiben, mit dem Cmdlet **Get-ManagementScope** sehen.

In diesem Beispiel wird eine neuen Rollengruppe mit dem Namen "Begrenzte Recipient Management" mit den folgenden Einstellungen erstellt:

- Die E-Mail-Empfänger und e-Mail-aktivierten Öffentlichen Ordner Rollen werden die Rollengruppe zugewiesen.
- Die Benutzer Kim und Martin werden als Mitglieder hinzugefügt. Da keine benutzerdefinierte empfängerschreibbereich angegeben wurde, kann Kim und Martin alle Empfänger in der Organisation verwalten.

```
New-RoleGroup -Name "Limited Recipient Management" -Roles "Mail Recipients","Mail Enabled Public Folders" -Members "Kim","Martin"
```

Dies ist das gleiche Beispiel mit einer benutzerdefinierten empfängerschreibbereich, d. Kim h. und Martin kann nur Verwalten von Empfängern, die in den Bereich Seattle Empfänger (Empfänger, die die **Stadt** -Eigenschaft auf den Wert Seattle festgelegt werden) enthalten sind.

```
New-RoleGroup -Name "Limited Recipient Management" -Roles "Mail Recipients","Mail Enabled Public Folders" -Members "Kim","Martin" -CustomRecipientWriteScope "Seattle Recipients"
```

Für ausführliche Informationen zu Syntax und Parameter, [New-RoleGroup](#).

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Zum bestätigen, dass Sie erfolgreich eine Rollengruppe erstellt haben, führen Sie einen der folgenden Schritte aus:

- Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen** > **Administratorrollen**, wählen Sie aus der neuen Rollengruppe erstellt wird, und überprüfen Sie die Einstellungen im Bereich Details, oder klicken Sie auf **Bearbeiten** um die Einstellungen zu überprüfen.
- Ersetzen Sie in Exchange Online PowerShell <Gruppe Rollenname> mit dem Namen der Rollengruppe und führen den folgenden Befehl, um die Einstellungen zu überprüfen:

```
Get-RoleGroup -Identity "<Role Group Name>" | Format-List
```

## Kopieren Sie die vorhandenen Rollengruppen

Ist eine vorhandene Rollengruppe schließen im Hinblick auf die Berechtigungen und Einstellungen, die Sie Benutzern zuweisen möchten, können Sie die vorhandene Rollengruppe kopieren und die Kopie entsprechend Ihren Anforderungen zu ändern.

#### **Kopieren einer Rollengruppe mithilfe der Exchange-Verwaltungskonsole**

**Hinweis:** Sie können nicht mit der Exchange-Verwaltungskonsole um eine Rollengruppe zu kopieren, wenn Sie Exchange Online PowerShell so konfigurieren Sie mehrere Bereiche oder exklusiver Bereiche auf die Rollengruppe verwendet haben. Zum Kopieren von Rollengruppen, die diese Einstellungen haben, müssen Sie Exchange Online PowerShell verwenden.

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Administratorrollen**.
2. Wählen Sie aus der Rollengruppe, die Sie verwenden möchten, kopieren, und klicken Sie dann auf **Kopie**
3. Konfigurieren Sie im Fenster **neue Rollengruppe** die folgenden Einstellungen:
  - **Name:** der Standardwert ist "Kopie von \_ <Rollengruppe Name>\_" aber Sie können einen eindeutigen Namen für die Rollengruppe eingeben.
  - **Beschreibung:** die vorhandene Beschreibung ist vorhanden, jedoch können Sie ihn ändern.
  - **Bereich schreiben:** der vorhandene Write Bereich aktiviert ist, aber Sie können wählen Sie **Standard** oder einer anderen benutzerdefinierten empfängerschreibbereich, die Sie bereits erstellt haben.
  - **Rollen:** Klicken Sie auf **Add**  oder **Entfernen von**  so ändern Sie die Rollen, die der Rollengruppe zugewiesen sind.
  - **Member:** Klicken Sie auf **Add**  oder **Entfernen von**  die Gruppenmitgliedschaft zu ändern.

Wenn Sie fertig sind, klicken Sie auf **Speichern**, um die Rollengruppe zu erstellen.

### **Verwenden von Exchange Online PowerShell, eine Rollengruppe kopieren**

1. Speichern Sie die Rollengruppe, die Sie kopieren wollen, mithilfe der folgenden Syntax in einer Variablen:

```
$RoleGroup = Get-RoleGroup "<Existing Role Group Name>"
```

2. Erstellen der neuen Rollengruppe mit der folgenden Syntax an:

```
New-RoleGroup -Name "<Unique Name>" -Roles $RoleGroup.Roles [-Members <Members>] [-ManagedBy <Managers>] [-CustomRecipientWriteScope "<Existing Custom Recipient Write Scope Name>"]
```

- Der Parameter *Members* gibt die Mitglieder der Rollengruppe mithilfe der folgenden Syntax an:  "Member1", "Member2", ..., "MemberN". Sie können angeben, dass Benutzer, universellen Sicherheitsgruppen (USGs) oder anderen Rollen (Sicherheitsprinzipale) gruppiert.
- Der Parameter *ManagedBy* gibt die Stellvertretungen eingerichtet, die ändern können, und die Rollengruppe entfernen, indem Sie mit der folgenden Syntax:  "Delegate1", "Delegate2", ..., "DelegateN". Beachten Sie, dass diese Einstellung nicht in der Exchange-Verwaltungskonsole verfügbar ist.
- Der Parameter *CustomRecipientWriteScope* gibt an, der vorhandenen benutzerdefinierten empfängerschreibbereich der Rollengruppe zuweisen. Sie können den verfügbaren benutzerdefinierten Empfänger Bereiche zu schreiben, mit dem Cmdlet **Get-ManagementScope** sehen.

Dieses Beispiel kopiert die Rollengruppe "Organisationsverwaltung" in der neuen Rollengruppe mit dem Namen "Begrenzte Organization Management". Mitglieder der Rolle Isabelle, Carter und Lukas sind und die die Rolle Gruppe delegiert werden Jenny und Katie.

```
$RoleGroup = Get-RoleGroup "Organization Management"
New-RoleGroup "Limited Organization Management" -Roles $RoleGroup.Roles -Members "Isabelle", "Carter", "Lukas" - ManagedBy "Jenny", "Katie"
```

Dieses Beispiel kopiert die Rollengruppe "Organisationsverwaltung" in der neuen Rollengruppe

Organisationsverwaltung Vancouver mit der Vancouver Benutzer benutzerdefinierte Empfänger empfängerschreibbereich aufgerufen.

```
$RoleGroup = Get-RoleGroup "Organization Management"  
New-RoleGroup "Vancouver Organization Management" -Roles $RoleGroup.Roles -CustomRecipientWriteScope  
"Vancouver Users"
```

Für ausführliche Informationen zu Syntax und Parameter, [New-RoleGroup](#).

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie erfolgreich eine Rollengruppe kopiert haben, führen Sie einen der folgenden Schritte aus:

- Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Administratorrollen**, wählen Sie aus der neuen Rollengruppe erstellt wird, und überprüfen Sie die Einstellungen im Bereich Details, oder klicken Sie auf **Bearbeiten** um die Einstellungen zu überprüfen.
- Ersetzen Sie in Exchange Online PowerShell <Gruppe Rollenname> mit dem Namen der Rollengruppe und führen den folgenden Befehl, um die Einstellungen zu überprüfen:

```
Get-RoleGroup -Identity "<Role Group Name>" | Format-List
```

## Ändern von Rollengruppen

#### Verwenden der Exchange-Verwaltungskonsole zum Ändern von Rollengruppen

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Administratorrollen**, wählen Sie aus der Rollengruppe, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

Die gleichen Optionen sind verfügbar, wenn Sie Rollengruppen wie beim Ändern Sie [Rollengruppen erstellen] ([Use the EAC to create role groups](#)). Sie können:

- Ändern Sie Name und Beschreibung.
- Ändern Sie den Bereich schreiben (Wenn Sie benutzerdefinierte Empfänger Write Bereiche erstellt haben).
- Hinzufügen und Entfernen von Verwaltungsrollen (erstellen oder Entfernen von rollenzuweisungen).
- Hinzufügen und Entfernen von Mitgliedern.

#### Hinweise:

- Sie können nicht der Exchange-Verwaltungskonsole verwenden, um den Bereich schreiben, Rollen und Mitglieder einer Rollengruppe, wenn Sie Exchange Online PowerShell verwendet haben, konfigurieren Sie mehrere Bereiche oder exklusiver Bereiche auf die Rollengruppe ändern. Um die Einstellungen dieser Rolle Gruppen zu ändern, müssen Sie Exchange Online PowerShell verwenden.
- Einige Rollengruppen (beispielsweise die Rollengruppe "Organisationsverwaltung") beschränken Sie die Rollen, die Sie aus Gruppe entfernen können.
- Sie können hinzufügen oder Entfernen von Delegaten zu einer Rollengruppe in der Exchange-Verwaltungskonsole. Sie können nur Exchange Online PowerShell verwenden.

#### Verwenden von Exchange Online PowerShell Rollengruppen Rollen hinzu (rollenzuweisungen erstellen)

Um Rollen Rollengruppen in Exchange Online PowerShell hinzuzufügen, erstellen Sie *verwaltungsrollenzuweisungen* mithilfe der folgenden Syntax an:

```
New-ManagementRoleAssignment [-Name "<Unique Name>"] -SecurityGroup "<Role Group Name>" -Role "<Role Name>" [-RecipientRelativeWriteScope <MyGAL | MyDistributionGroups | Organization | Self>] [-CustomRecipientWriteScope "<Role Scope Name>"]
```

- Der Name der Rolle Aufgabe wird automatisch erstellt, wenn Sie eine nicht angeben.
- Wenn Sie keine Parameters *RecipientRelativeWriteScope* den impliziten Lese-Bereich verwenden, und implizite Write-Bereich der Rolle für die Rollenzuweisung angewendet wird.
- Ein vordefinierter Bereich Ihrer geschäftlichen Anforderungen erfüllt, können Sie des Parameters *RecipientRelativeWriteScope* verwenden, um den Bereich für die Rollenzuweisung anzuwenden.
- Verwenden Sie den Parameter *CustomRecipientWriteScope*, zum Anwenden von benutzerdefinierten empfängerschreibbereich.

In diesem Beispiel wird die Verwaltungsrolle Transportregeln der Rollengruppe "Seattle Compliance" zugewiesen.

```
New-ManagementRoleAssignment -SecurityGroup "Seattle Compliance" -Role "Transport Rules"
```

In diesem Beispiel wird die Rolle Nachrichtenverfolgung der Rollengruppe "Enterprise Support" zugewiesen und der vordefinierte Bereich Organisation angewendet.

```
New-ManagementRoleAssignment -SecurityGroup "Enterprise Support" -Role "Message Tracking" -RecipientRelativeWriteScope Organization
```

In diesem Beispiel wird die Rolle Nachrichtenverfolgung der Rollengruppe "Seattle Recipient Admins" zugewiesen und der Bereich "Seattle Recipients" angewendet.

```
New-ManagementRoleAssignment -SecurityGroup "Seattle Recipient Admins" -Role "Message Tracking" -CustomRecipientWriteScope "Seattle Recipients"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-ManagementRoleAssignment](#).

### Mithilfe von Exchange Online PowerShell Rollen aus Rollengruppen entfernen (remove rollenzuweisungen)

Um die Rollen aus Rollengruppen in Exchange Online PowerShell entfernen möchten, entfernen Sie *verwaltungsrollenzuweisungen* mithilfe der folgenden Syntax an:

```
Get-ManagementRoleAssignment -RoleAssignee "<Role Group Name>" -Role "<Role Name>" -Delegating <$true | $false> | Remove-ManagementRoleAssignment
```

- Um die *regulären* Rollenzuweisungen entfernen, die Benutzern Berechtigungen erteilen möchten, verwenden Sie den Wert `$false` für den Parameter *Delegieren*.
- Zum Entfernen von Rollenzuweisungen *Delegieren*, mit denen die Rolle an andere Personen zugewiesen werden können, verwenden Sie den Wert `$true` für den Parameter *Delegieren*.

Dieses Beispiel entfernt die Rolle Verteilergruppen aus der Rollengruppe "Seattle Recipient Administrators".

```
Get-ManagementRoleAssignment -RoleAssignee "Seattle Recipient Administrators" -Role "Distribution Groups" -Delegating $false | Remove-ManagementRoleAssignment
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Remove-ManagementRoleAssignment](#).

### Verwenden Sie Exchange Online PowerShell, um den Bereich der Rollenzuweisungen in Rollengruppen ändern

Des Bereichs Schreiben einer rollenzuweisung in einer Rollengruppe definiert die Objekte, die die Mitglieder der Rollengruppe ausgeführt werden können (beispielsweise alle Benutzer oder nur die Benutzer, deren Eigenschaft "Stadt" den Wert Vancouver hat). Sie können den Schreibzugriff Geltungsbereich die Rollen, die einer Rollengruppe zu ändern:

- Der implizite Bereich aus den Rollen selbst. Dies bedeutet, dass Sie nicht eine beliebige benutzerdefinierte Bereiche angeben, wenn Sie die Rollengruppe erstellt, oder Sie den Wert der alle rollenzuweisungen in einer vorhandenen Rollengruppe auf den Wert legen `$null`.
- Im selben benutzerdefinierten Bereich für alle rollenzuweisungen.
- Andere benutzerdefinierte Bereiche für jede einzelne rollenzuweisung.

Um den Bereich auf allen rollenzuweisungen auf einer Rollengruppe gleichzeitig festlegen möchten, verwenden Sie die folgende Syntax:

```
Get-ManagementRoleAssignment -RoleAssignee "<Role Group Name>" | Set-ManagementRoleAssignment [-CustomRecipientWriteScope "<Recipient Write Scope Name>"] [-RecipientRelativeScopeWriteScope <MyDistributionGroups | Organization | Self>] [-ExclusiveRecipientWriteScope "<Exclusive Recipient Write Scope name>"]
```

In diesem Beispiel wird der Empfängerbereich für alle rollenzuweisungen auf die Rollengruppe "Sales Recipient Management" in direkten Vertriebsmitarbeiter geändert.

```
Get-ManagementRoleAssignment -RoleAssignee "Sales Recipient Management" | Set-ManagementRoleAssignment -CustomRecipientWriteScope "Direct Sales Employees"
```

Führen Sie die folgenden Schritte aus, um den Bereich für eine einzelne Rolle Zuordnung zwischen einer Rollengruppe und eine Verwaltungsrolle zu ändern:

- Ersetzen Sie <Gruppe Rollenname> mit dem Namen der Rollengruppe und führen den folgenden Befehl, um die Namen der alle rollenzuweisungen der Rollengruppe zu suchen:

```
Get-ManagementRoleAssignment -RoleAssignee "<Role Group Name>" | Format-List Name
```

- Ermitteln Sie den Namen der Rollenzuweisung, die Sie ändern möchten. Verwenden Sie den Namen der Rollenzuweisung im nächsten Schritt.
- Um den Bereich für die einzelnen rollenzuweisung festzulegen, verwenden Sie die folgende Syntax:

```
Set-ManagementRoleAssignment -Identity "<Role Assignment Name>" [-CustomRecipientWriteScope "<Recipient Write Scope Name>"] [-RecipientRelativeScopeWriteScope <MyDistributionGroups | Organization | Self>] [-ExclusiveRecipientWriteScope "<Exclusive Recipient Write Scope name>"]
```

In diesem Beispiel wird der Empfängerbereich für die rollenzuweisung mit dem Namen Mail Recipients\_Sales Recipient Management auf die alle Vertriebsmitarbeiter geändert.

```
...
Set-ManagementRoleAssignment "Mail Recipients_Sales Recipient Management" -CustomRecipientWriteScope "All Sales Employees"
...
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-ManagementRoleAssignment](#).

## Verwenden von Exchange Online PowerShell Ändern der Liste der Stellvertretungen in Rollengruppen

Rolle Gruppe Delegaten definieren, wer berechtigt ist, ändern und Löschen der Rollengruppe. Sie können keine Rolle Gruppe Stellvertretungen in der Exchange-Verwaltungskonsole verwalten.

Verwenden Sie die folgende Syntax, um die Liste der Stellvertretungen in einer Rollengruppe zu ändern:

```
Set-RoleGroup -Identity "<Role Group Name>" -ManagedBy <Delegates>
```

- *Ersetzen* die vorhandene Liste der Stellvertretungen mit den Werten, die Sie angeben möchten, verwenden Sie folgende Syntax: `"Delegate1", "Delegate2", ... "DelegateN"`.
- *Wählen Sie einzelne ändern* der vorhandenen Liste der Stellvertretungen, verwenden Sie die folgende Syntax: `@{Add="Delegate1", "Delegate2" ...; Remove="Delegate3", "Delegate4" ...}`.

In diesem Beispiel werden alle aktuelle Delegaten der Rollengruppe Help Desk durch die angegebenen Benutzer ersetzt.

```
Set-RoleGroup -Identity "Help Desk" -ManagedBy "Gabriela Laureano", "Hyun-Ae Rim", "Jacob Berger"
```

Dieses Beispiel fügt Daigoro Akai und Valeria Barrio aus der Liste der Stellvertretungen auf die Rollengruppe "Help Desk" entfernt.

```
Set-RoleGroup -Identity "Help Desk" -ManagedBy @{Add="Daigoro Akai"; Remove="Valeria Barrios"}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-RoleGroup](#).

## Verwenden von Exchange Online PowerShell ändern Sie die Liste der Elemente in Rollengruppen

- Die Cmdlets **Add-RoleGroupMember** und **Remove-RoleGroupMember** hinzufügen oder entfernen einzelne Mitglieder zu einem Zeitpunkt. Das Cmdlet **Update-RoleGroupMember** kann ersetzen oder ändern die vorhandene Liste der Elemente.
- Die Mitglieder einer Rollengruppe können Benutzer, universellen Sicherheitsgruppen (USGs) oder anderen Rolle gruppiert (Sicherheitsprinzipale) sein.

Verwenden Sie die folgende Syntax, um die Mitglieder einer Rollengruppe zu ändern:

```
Update-RoleGroupMember -Identity "<Role Group Name>" -Members <Members> [-BypassSecurityGroupManagerCheck]
```

- *So Ersetzen* Sie die vorhandene Liste der Elemente mit den Werten, die Sie angeben möchten, verwenden Sie folgende Syntax: `"Member1", "Member2", ... "MemberN"`.
- *Wählen Sie einzelne ändern* der vorhandenen Liste der Elemente, verwenden Sie die folgende Syntax: `@{Add="Member1", "Member2" ...; Remove="Member3", "Member4" ...}`.

In diesem Beispiel werden alle aktuellen Mitglieder der Rollengruppe "Help Desk" durch die angegebenen Benutzer ersetzt.

```
Update-RoleGroupMember -Identity "Help Desk" -Members "Gabriela Laureano", "Hyun-Ae Rim", "Jacob Berger"
```

Dieses Beispiel fügt Daigoro Akai und Valeria Barrio aus der Liste der Elemente auf der Rollengruppe "Help Desk" entfernt.

```
Update-RoleGroupMember -Identity "Help Desk" -Members @{Add="Daigoro Akai"; Remove="Valeria Barrios"}
```

Informationen zur Syntax und Parametern finden Sie unter [Update-RoleGroupMember](#).

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie eine Rollengruppe erfolgreich geändert haben, führen Sie die folgenden Schritte aus:

- Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Administratorrollen**, wählen Sie aus der neuen Rollengruppe erstellt wird, und überprüfen Sie die Einstellungen im Bereich Details, oder klicken Sie auf **Bearbeiten**  um die Einstellungen zu überprüfen.
- Ersetzen Sie in Exchange Online PowerShell <Gruppe Rollenname> mit dem Namen der Rollengruppe und führen den folgenden Befehl, um die Einstellungen zu überprüfen:

```
Get-RoleGroup -Identity "<Role Group Name>" | Format-List
```

- Ersetzen Sie in Exchange Online PowerShell <Gruppe Rollenname> mit dem Namen der Rollengruppe und führen den folgenden Befehl, um die Einstellungen zu überprüfen:

```
Get-ManagementRoleAssignment -RoleAssignee "<Role Group Name>" | Format-Table *WriteScope
```

## Entfernen von Rollengruppen

Sie können keine integrierten Rollengruppen entfernen, aber Sie können benutzerdefinierte Rollengruppen, die Sie erstellt haben entfernen.

### Hinweise:

- Wenn Sie eine Rollengruppe entfernen, werden die verwaltungsrollenzuweisungen zwischen der Rollengruppe und Verwaltungsrollen gelöscht. Alle Verwaltungsrollen, die der Rollengruppe zugewiesen sind, werden nicht gelöscht.
- Wenn ein Benutzer auf die Rollengruppe für den Zugriff auf ein Feature abhängig ist, wird der Benutzer keinen Zugriff mehr haben Sie dem Feature nach dem Löschen der Rollengruppe.

### Entfernen einer Rollengruppe mithilfe der Exchange-Verwaltungskonsole

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Administratorrollen**.
2. Wählen Sie aus der Rollengruppe zu entfernen, und klicken Sie dann auf **Löschen** .
3. Klicken Sie auf **Ja** im Bestätigungsfenster zur.

### Verwenden von Exchange Online PowerShell, eine Rollengruppe entfernen

Wenn eine benutzerdefinierte Rollengruppe entfernen möchten, verwenden Sie die folgende Syntax:

```
Remove-RoleGroup -Identity "<Role Group Name>" [-BypassSecurityGroupManagerCheck]
```

In diesem Beispiel wird die Rollengruppe "Training Administrators" entfernt.

```
Remove-RoleGroup -Identity "Training Administrators"
```

Dieses Beispiel entfernt die Rollengruppe "Vancouver Recipient Administrators". Da der Benutzer den Befehl in der **ManagedBy**-Eigenschaft der Rollengruppe definiert ist, ist die Option *BypassSecurityGroupManagerCheck* in

den Befehl erforderlich. Der Benutzer, der den Befehl ausführt, wird die Rolle Verwaltungsrolle zugewiesen, die Benutzer das Kontrollkästchen Sicherheit Gruppe Manager umgehen können.

```
Remove-RoleGroup - Identity "Vancouver Recipient Administrators" -BypassSecurityGroupManagerCheck
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Remove-RoleGroup](#).

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie eine Rollengruppe entfernt haben, führen Sie einen der folgenden Schritte aus:

- Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Administratorrollen** und stellen Sie sicher, dass die Rollengruppe nicht mehr aufgeführt wird.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl überprüfen, ob die Rollengruppe nicht mehr aufgeführt wird:

```
Get-RoleGroup
```

# Sicherheit und Richtlinientreue für Exchange Online

18.12.2018 • 7 minutes to read

E-Mails sind für Information-Worker in Organisationen aller Größen ein zuverlässiges und allgegenwärtiges Kommunikationsmedium. Nachrichtenspeicher und Postfächer sind heute Repositorys mit wertvollen Daten. Organisationen müssen Messagingrichtlinien formulieren, die die regelkonforme Verwendung ihrer Nachrichtensysteme vorschreiben, den Benutzern Anleitungen zur Umsetzung der Richtlinien zur Verfügung stellen und ggf. Details zu den Kommunikationsarten bereitstellen, die nicht zulässig sind.

Organisationen müssen auch Richtlinien zum Lebenszyklus von E-Mails erstellen, Nachrichten so lange aufzubewahren, wie es aus geschäftlichen oder rechtlichen Gründen notwendig ist, E-Mail-Datensätze zu Beweissicherungs- und Untersuchungszwecken aufzubewahren und darauf vorbereitet sein, jegliche E-Mail-Datensätze zu finden und bereitzustellen, die zur Erfüllung von eDiscovery-Anforderungen benötigt werden.

Vertrauliche Informationen wie geistiges Eigentum, Betriebsgeheimnisse, Geschäftspläne sowie personenbezogene Informationen (Personally Identifiable Information, PII), die von Ihrer Organisation erfasst oder verarbeitet werden, müssen vor Lecks geschützt werden.

## Sicherheit und Richtlinientreue in Exchange Online

Die folgende Tabelle bietet einen Überblick über die Funktionen für Sicherheit und Richtlinientreue in Microsoft Exchange Online und enthält Links zu Themen, in denen Sie weitere Informationen zu diesen Funktionen und ihrer Verwaltung finden.

FUNKTION	BESCHREIBUNG
<a href="#">Archivieren von Postfächern in Exchange Online</a>	Archivpostfächer (ein sogenanntes In-Situ-Archiv) unterstützen Personen in Ihrer Office 365-Organisation dabei, die Steuerung über Messagingdaten zu übernehmen, indem zusätzlicher E-Mail-Speicher bereitgestellt wird. Mit Outlook oder Outlook Web App können Personen Nachrichten in ihren Archivpostfächern anzeigen und Nachrichten zwischen ihren primären und Archivpostfächern verschieben und kopieren.
<a href="#">In-Situ-Speicher und Beweissicherungsverfahren</a>	Mithilfe des In-Situ-Speichers und des Beweissicherungsverfahrens können Sie Postfachinhalte zur Einhaltung der Richtlinientreue und für eDiscovery beibehalten oder archivieren.
<a href="#">In-Place eDiscovery</a>	Compliance-eDiscovery bietet autorisierten Compliance Officers in Ihrer Organisation die Möglichkeit, Postfachdaten in Ihrer gesamten Exchange-Organisation zu durchsuchen, Suchergebnisse in der Vorschau anzuzeigen, diese in ein Discovery-Postfach zu kopieren oder sie in eine PST-Datei zu exportieren.

FUNKTION	BESCHREIBUNG
Inaktive Postfächer in Exchange Online	Sie können den Inhalt der gelöschte Postfächer mithilfe von inaktiver Postfächer auf unbestimmte Zeit beibehalten. Sie können zum Erstellen eines inaktiven Postfachs platzieren an In-Place Hold oder eine Aufbewahrung für eventuelle Rechtsstreitigkeiten für das Postfach und dann das entsprechende Office 365-Benutzerkonto gelöscht. Zusätzlich zum Postfach Inhalt beibehalten, können Administratoren oder Compliance Officer In-Place eDiscovery in Exchange Online oder Content-Suche in der Office 365-Sicherheit und Compliance Center Sie um den Inhalt eines inaktiven Postfachs zu durchsuchen.
Verhinderung von Datenverlust (DLP)	Mit DLP-Richtlinien (Data Loss Prevention, Verhinderung von Datenverlust) können Sie vertrauliche Informationen identifizieren und überwachen, z. B. Personalausweis- oder Kreditkartennummern oder Standardformulare, die in Ihrem Unternehmen verwendet werden. Sie können DLP-Richtlinien festlegen, um Benutzer darüber zu informieren, dass sie vertrauliche Informationen senden, oder um die Übertragung vertraulicher Informationen zu blockieren.
Exchange-Überwachungsberichte	Mit den Überwachungsfunktionen in Exchange Online können Sie Änderungen nachverfolgen, die von Microsoft und den Administratoren Ihrer Organisation an Ihrer Exchange Online-Konfiguration vorgenommen wurden. Außerdem können Sie den Postfachzugriff durch Personen, bei denen es sich nicht um den Postfachbesitzer handelt, überwachen. In Exchange Online werden überwachte Aktionen aufgezeichnet und können in einem Onlinebericht angezeigt oder in eine Datei exportiert werden.
Verwaltung von Nachrichtendatensätzen (MRM)	Messaging-datensatzverwaltung (MRM) hilft bei Ihrer Organisation, die zur Erfüllung von geschäftlichen und behördlichen Vorschriften und zur Reduzierung der rechtlichen Risiken im Zusammenhang mit e-Mail-e-Mail-Lebenszyklus verwalten. In Exchange Online können Sie Compliance-Archiv oder Aufbewahrung für eventuelle Rechtsstreitigkeiten verwenden, e-Mail und die <a href="#">Aufbewahrungstags</a> und <a href="#">Aufbewahrungsrichtlinien</a> zum Archivieren und Löschen von e-Mail beibehalten.
Verwaltung von Informationsrechten in Exchange Online	Informationen, die Verwaltung von Informationsrechten (IRM) hilft Sie und Ihre Benutzer steuern Sie, wer zugreifen kann, weiterleiten, drucken oder kopieren vertrauliche Daten in einer e-Mail. IRM kann Ihre lokale Active Directory-Rechteverwaltungsdienste (AD RMS) Server verwenden.
Office 365-Nachrichtenverschlüsselung	Office 365 Message Encryption ermöglichen das Senden verschlüsselter Nachrichten an Personen innerhalb und außerhalb Ihrer Organisation, unabhängig von der Ziel-e-Mail-Dienst – gibt an, ob es sich um Outlook.com, Yahoo, Google Mail oder einem anderen Dienst ist. Ausgewählte Empfänger können verschlüsselte Antworten senden. Office 365 Message Encryption kombiniert e-Mail-Verschlüsselung und Rights Management-Funktionen. Rights Management-Funktionen werden von Azure Information Protection bereitgestellt.

FUNKTION	BESCHREIBUNG
<a href="#">S/MIME for Message Signing and Encryption</a>	Secure/Multipurpose Internet Mail Extensions (S/MIME) ermöglicht es e-Mail-Benutzer zum Schutz von vertraulichen Informationen durch das Senden signierte und verschlüsselte e-Mail innerhalb ihrer Organisation. Als Administrator können Sie S/MIME-basierte Sicherheit für Ihre Organisation aktivieren, wenn Sie Postfächer in Exchange Server oder Exchange Online haben.
<a href="#">Journale in Exchange Online</a>	Mithilfe der Aufzeichnung eingehender und ausgehender E-Mail-Kommunikation in Journalen können rechtliche, regulatorische und organisatorische Auflagen eingehalten werden. In Exchange Online können Sie Journalregeln erstellen, um Journalberichte an Ihr lokales Postfach oder Archivierungssystem oder an einen externen Archivierungsdienst zu übermitteln.
<a href="#">Nachrichtenflussregeln (Transportregeln) in Exchange Online</a>	Mithilfe von E-Mail-Flussregeln, die auch als Transportregeln bezeichnet werden, können Sie von Benutzern gesendete oder erhaltene Nachrichten untersuchen und Maßnahmen ergreifen, wie beispielsweise Nachrichten blockieren oder als unzustellbar erklären, Nachrichten zur Überprüfung durch einen Vorgesetzten oder Administrator zurückstellen oder eine Kopie an einen anderen Empfänger zustellen, wenn die Nachricht bestimmte Bedingungen erfüllt.

# Ändern von Archivrichtlinien

18.12.2018 • 8 minutes to read

Archivrichtlinien können Sie in Exchange Online um Postfachelemente automatisch in persönlichen (lokalen) oder cloudbasierten Archive zu verschieben. Archivrichtlinien sind aufbewahrungstags, mit denen die Aufbewahrungsaktion **in Archiv verschieben**.

Exchange-Setup erstellt eine Aufbewahrungsrichtlinie **MRM-Standardrichtlinie** aufgerufen. Diese Richtlinie hat eine Richtlinie Standardtag (DPT) zugewiesen, die Elemente nach zwei Jahren in das Archivpostfach verschoben. Die Richtlinie enthält außerdem eine Anzahl von persönlichen Tags, die Benutzer automatisch auf Ordner oder zu Postfachelemente anwenden können, verschieben oder Löschen von Nachrichten. Wenn ein Postfach besitzt eine Aufbewahrungsrichtlinie zugewiesen wird, wenn es Archiv aktiviert ist, wird die **MRM-Standardrichtlinie** automatisch von Exchange zugewiesen. Sie können auch Ihre eigenen Archive und Richtlinien erstellen und anwenden auf Postfachbenutzer. Weitere Informationen finden Sie unter [aufbewahrungstags und Aufbewahrungsrichtlinien](#).

Sie können in Ihren geschäftlichen Anforderungen erfüllen die Standardrichtlinie enthalten aufbewahrungstags ändern. Beispielsweise können Sie die Archivierung DPT zum Verschieben von Elementen in das Archiv nach drei Jahren anstelle von zwei ändern. Sie können auch zusätzliche Persönliche Tags erstellen und entweder in einer Aufbewahrungsrichtlinie die **MRM-Standardrichtlinie**, einschließlich hinzufügen oder Benutzern ermöglichen, persönliche Tags auf ihre Postfächer über Outlook Web App-Optionen hinzufügen.

Weitere Verwaltungsaufgaben im Zusammenhang mit Archiven finden Sie unter [Aktivieren oder deaktivieren Sie ein Archivpostfach im Exchange Online](#).

## NOTE

In einer Exchange-Hybridbereitstellung können Sie ein cloudbasiertes Archivpostfach für ein lokales primäres Postfach aktivieren. Beim Zuweisen einer Archivrichtlinie zu einem lokalen Postfach werden die Elemente zum cloudbasierten Archiv verschoben. Wenn ein Element in das Archivpostfach verschoben wird, wird im lokalen Postfach keine Kopie davon beibehalten. Wenn das lokale Postfach ausgesetzt wird, werden Elemente anhand einer Archivrichtlinie weiterhin in das cloudbasierte Archivpostfach verschoben, in dem sie so lange aufbewahrt werden, wie dies durch die In-Situ-Speicherung festgelegt wurde.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Messaging-Datensatzverwaltung" im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Ändern der Standardarchivrichtlinie mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie zu **Verwaltung der Richtlinientreue > Aufbewahrungstags**.
2. Wählen Sie in der Listenansicht das Tag **Standard 2 Jahre, in Archiv verschieben**, und klicken Sie dann auf **Bearbeiten**.

## TIP

Klicken Sie auf die Spalte **TYP**, um die Aufbewahrungstags nach Typ zu sortieren. Die Standardarchivrichtlinie wird mit dem Typ **Standard** und der Aufbewahrungsaktion **Archiv** angezeigt. Alternativ können Sie auf **NAME** klicken, um die Aufbewahrungstags nach Name zu sortieren.

3. Bearbeiten Sie in **Aufbewahrungstag** gegebenenfalls die folgenden Einstellungen, und klicken Sie auf **Speichern**:

- **Name:** Verwenden Sie dieses Feld am oberen Rand der Seite zum Anzeigen oder Ändern der Name des Tags.
- **Tagtyp Aufbewahrung:** Dieses schreibgeschützte Feld zeigt den Typ des Tags an.
- **Aufbewahrungsaktion:** Dieses Feld für archivrichtlinien nicht ändern.
- **Beibehaltungszeitraum:** Wählen Sie eine der folgenden Optionen aus:
- **Never:** Klicken Sie auf diese Schaltfläche, um das Tag zu deaktivieren. Wenn die DPT deaktiviert ist, wird das Tag nicht mehr auf das Postfach angewendet.

## IMPORTANT

Elemente, auf die ein deaktiviertes Aufbewahrungstag angewendet wird, werden nicht vom Postfach-Assistenten verarbeitet. Wenn Sie verhindern möchten, dass ein Tag auf Elemente angewendet wird, sollten Sie das Tag nicht löschen, sondern deaktivieren. Beim Löschen eines Tags wird die Tagkonfiguration aus Active Directory gelöscht, und der Postfach-Assistent verarbeitet alle Nachrichten, um das gelöschte Tag zu entfernen.

## NOTE

Wenn ein Benutzer ein Tag auf ein Element anwendet und davon ausgeht, dass das Element nie verschoben wird, kann das spätere Aktivieren des Tags zum Verschieben von Elementen führen, die der Benutzer im primären Postfach aufzubewahren wollte.

- **Wenn das Element das folgende Alter (in Tagen) erreicht:** Klicken Sie auf diese Schaltfläche, um anzugeben, dass Elemente verschoben werden, um nach einem bestimmten Zeitraum zu archivieren. Diese Einstellung ist standardmäßig so konfiguriert, um Elemente in das Archiv nach zwei Jahren (730 Tage) zu verschieben. Geben Sie zum Ändern dieser Einstellung in das entsprechende Textfeld die Anzahl der Tage in der Aufbewahrungszeitraum. Der Wertebereich liegt zwischen 1 und 24,855 Tagen.
- **Kommentar:** in diesem Feld können Sie einen Kommentar eingeben, die für Outlook und Outlook Web App-Benutzer angezeigt werden.

## Verwenden von Exchange Online PowerShell, archivrichtlinien ändern

In diesem Beispiel wird die `Default 2 year move to archive` Tag nach 1.095 Tage (in 3 Jahren) Elemente zu

verschieben.

```
Set-RetentionPolicyTag "Default 2 year move to archive" -Name "Default 3 year move to archive" -  
AgeLimitForRetention 1095
```

Dieses Beispiel deaktiviert die `Default 2 year move to archive` Tag.

```
Set-RetentionPolicyTag "Default 2 year move to archive" -RetentionEnabled $false
```

In diesem Beispiel werden alle Archiv-DPTs und persönlichen Tags abgerufen und deaktiviert.

```
Get-RetentionPolicyTag | ? {$_._RetentionAction -eq "MoveToArchive"} | Set-RetentionPolicyTag -RetentionEnabled  
$false
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-RetentionPolicyTag](#) und [Get-RetentionPolicyTag](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Verwenden Sie das Cmdlet [Get-RetentionPolicyTag](#), um die Einstellungen des Aufbewahrungstags abzurufen.

Dieser Befehl ruft die Eigenschaften des ab dem `Default 2 year move to archive` aufbewahrungstag und Pipes Formatieren der Ausgabe an das Cmdlet **Format-List**, um alle Eigenschaften in einer Liste anzuzeigen.

```
Get-RetentionPolicyTag "Default 2 year move to archive" | Format-List
```

# In-Situ-Speicher und Beweissicherungsverfahren

18.12.2018 • 30 minutes to read

## NOTE

Wir haben den 1 Juli 2017 Stichtag zum Erstellen von neuen Compliance-Archive in Exchange Online (in Office 365 und Exchange Online-Plänen) verschoben. Aber weiter unten in diesem Jahr oder frühe nächste Jahr, nicht möglich, neue Compliance-Archive in Exchange Online erstellen. Als Alternative zu Compliance-Archive verwenden können Sie [eDiscovery-Fälle](#) oder [Office 365-Aufbewahrungsrichtlinien](#) in die Office 365-Sicherheit und Compliance Center verwenden. Nachdem wir neue Compliance-Archive außer Betrieb nehmen, Sie vermutlich noch vorhandene Compliance-Archive ändern, und Erstellen von neuen Compliance-Archive in einer Exchange-hybridbereitstellung wird weiterhin unterstützt. Und Sie vermutlich noch Postfächer auf Aufbewahrung für eventuelle Rechtsstreitigkeiten zu platzieren.

Wenn Rechtsstreitigkeiten zu erwarten sind, sind Organisationen dazu verpflichtet, die für den Fall relevanten elektronisch gespeicherten Informationen einschließlich E-Mail aufzubewahren. Diese Erwartung ist häufig vorhanden, bevor die Details des Falls bekannt werden, und die Menge der aufzubewahrenden Daten ist häufig groß. Organisationen müssen möglicherweise alle E-Mails zu einem bestimmten Thema oder alle E-Mails für bestimmte Personen aufzubewahren. Abhängig von den eDiscovery-Verfahren der jeweiligen Organisation können folgende Maßnahmen zur Aufbewahrung von E-Mails angewendet werden:

- Endbenutzer werden gebeten, E-Mails aufzubewahren und keine Nachrichten zu löschen. Allerdings können Benutzer E-Mails dennoch bewusst oder versehentlich löschen.
- Automatische Löschanalysen wie Messaging-Datensatzverwaltung (Messaging Records Management, MRM) können angehalten werden. Dies kann dazu führen, dass große Mengen an E-Mails das Benutzerpostfach füllen und so die Produktivität des Benutzers beeinträchtigen. Durch das Anhalten des automatischen Löschanalysen kann außerdem nicht verhindert werden, dass die Benutzer E-Mails manuell löschen.
- Einige Organisationen kopieren oder verschieben E-Mails in ein Archiv, um sicherzustellen, dass sie nicht gelöscht, verändert oder manipuliert werden. Dies führt zu einem Kostenanstieg aufgrund des manuellen Aufwands, der zum Kopieren oder Verschieben von Nachrichten in ein Archiv erforderlich ist, oder aufgrund der zum Sammeln und Speichern von E-Mails außerhalb von Exchange verwendeten Drittanbietersoftware.

Fehler bei der Aufbewahrung von E-Mails können für eine Organisation rechtliche und finanzielle Folgen haben, beispielsweise die Prüfung der Aufbewahrungs- und Offenlegungsverfahren für Datensätze in der Organisation, nachteilige Gerichtsurteile, Strafmaßnahmen oder Bußgelder.

Sie können den In-Situ-Speicher oder das Beweissicherungsverfahren verwenden, um folgende Ziele zu erreichen:

- Platzieren von Benutzerpostfächern in Archiven und Beibehalten von Postfachelementen in unveränderbarer Form
- Beibehalten von Postfachelementen, die von Benutzern oder automatischen Löschanalysen wie z. B. MRM gelöscht werden
- Verwenden abfragebasierter Compliance-Archive zum Suchen nach und Aufbewahren von Elementen anhand bestimmter Kriterien
- Beibehalten von Elementen auf unbestimmte Zeit oder über einen bestimmten Zeitraum

- Platzieren von Benutzerpostfächern in verschiedenen Archiven für verschiedene Fälle oder Untersuchungen
- Das Halten für den Benutzer transparent halten, ohne MRM anhalten zu müssen
- Ermöglichen der In-Situ-eDiscovery-Suche nach Elementen, die der Aufbewahrungspflicht unterliegen

## Compliance-Archiv-Szenarien

Das Konzept der rechtlichen Aufbewahrungspflicht werden in früheren Versionen von Exchange halten Sie alle Postfachdaten für einen Benutzer auf unbestimmte Zeit oder bis Wenn Sperre entfernt wurde. In Exchange Online enthält die Compliance-Archiv ein neues Modell, das Sie die folgenden Parameter angeben können:

- **Was halten:** Sie können angeben, welche Elemente enthalten, die mithilfe von Abfrageparametern wie Schlüsselwörtern, Absender und Empfänger, starten und Enddatum und auch angeben, wie die Nachrichtentypen e-Mail-Nachrichten oder Kalenderelemente, die Sie in die Warteschleife stellen möchten.
- **Halten Sie, wie lange:** Sie können eine Dauer für Elemente in der Warteschleife angeben.

Mit diesem neuen Modell ermöglichen Compliance-Archive es Ihnen, detaillierte Aufbewahrungsrichtlinien zu erstellen, um Postfachelemente in den folgenden Szenarien beizubehalten:

- **Dauerhafte Aufbewahrung:** Halten Sie die unbestimmte Szenario ähnelt der Aufbewahrung für eventuelle Rechtsstreitigkeiten. Es wurde für die direkte Verwendung Postfachelemente beibehalten, sodass Sie eDiscovery-Anforderungen erfüllen können. Während des Berichtszeitraums Rechtsstreitigkeiten oder einer Untersuchung werden nie Elemente gelöscht. Die Dauer ist nicht im Voraus bekannt, sodass kein Enddatum konfiguriert ist. Speichern alle e-Mail-Elemente auf unbestimmte Zeit, keine Abfrageparameter angeben oder Dauer Zeit beim Erstellen einer In-Place Hold.
- **Abfragebasierte Aufbewahrung:** Wenn Ihrer Organisation Elementen basierend auf angegebenen Abfrageparametern erhalten bleiben, können Sie ein abfragebasiertes Compliance-Archiv. Sie können Abfrageparametern wie Schlüsselwörtern, Start- und Enddaten, Absender und Empfänger-Adressen und Nachrichtentypen angeben. Nachdem Sie ein abfragebasiertes Compliance-Archiv erstellt haben, werden alle vorhandenen und zukünftigen Postfachelemente (einschließlich zu einem späteren Zeitpunkt empfangene Nachrichten), die die Abfrageparameter entsprechen beibehalten.

### IMPORTANT

Elemente, die als nicht durchsuchbare, gekennzeichnet sind in der Regel aufgrund eines Fehlers beim Indizieren einer Anlage, auch bleiben, da nicht bestimmt werden kann, ob sie Abfrageparametern übereinstimmen. Weitere Informationen zu teilweise indizierte Elemente finden Sie unter [teilweise indizierte Elemente in Inhaltssuche in Office 365](#).

- **Zeitbasierte Aufbewahrung:** sowohl Compliance-Archiv und Aufbewahrung für eventuelle Rechtsstreitigkeiten können Sie eine Dauer von Zeit für das Speichern Elemente angegeben. Ein Element Postfach empfangen oder erstellt wird, wird die Dauer ab dem Datum berechnet.

Wenn Ihre Organisation erfordert, dass alle Postfachelemente für einen bestimmten Zeitraum beibehalten werden, können beispielsweise 7 Jahre Sie eine zeitbasierte Aufbewahrung erstellen, damit die Elemente in der Warteschleife für einen bestimmten Zeitraum aufbewahrt werden. Angenommen Sie, ein Postfach, wird eine zeitbasierten Compliance-Archiv platziert und verfügt über eine Aufbewahrungszeit 365 Tage festgelegt. Wenn ein Element in dem Postfach gelöscht wird, nachdem es 300 Tage ab dem Datum empfangen wurde, ist es frei, die für einen zusätzlichen 65 Tage vor wird dauerhaft gelöscht. Sie können eine zeitbasierten Compliance-Archiv in Verbindung mit einer Aufbewahrungsrichtlinie um sicherzustellen, dass Elemente für die angegebene Dauer beibehalten und

nach Ablauf dieses Zeitraums dauerhaft entfernt werden.

Sie können In-Situ-Speicher dazu verwenden, Benutzerpostfächer in mehreren Speichern zu platzieren. Wenn ein Benutzer in mehreren In-Situ-Speichern platziert wird, werden die Suchabfragen von einem abfragebasierten Archiv kombiniert (mit **OR** -Operatoren). In diesem Fall beträgt die maximale Anzahl von Stichwörtern in allen abfragebasierten Archiven für ein Postfach 500. Bei mehr als 500 Stichwörtern werden sämtliche Inhalte des Postfachs archiviert (nicht bloß die Inhalte, die mit den Suchkriterien übereinstimmen). Alle Inhalte werden archiviert, bis die Gesamtzahl von Stichwörtern auf 500 oder weniger verringert wird.

## In-Situ-Speicher und Beweissicherungsverfahren

Aufbewahrung für eventuelle Rechtsstreitigkeiten verwendet die **LitigationHoldEnabled** -Eigenschaft eines Postfachs Inhalt von Postfächern in der Warteschleife platziert. Compliance-Archiv differenzierte sieht halten Sie Funktionalität auf Grundlage von Abfrageparametern und die Möglichkeit, mehrere platzieren enthält, die Aufbewahrung für eventuelle Rechtsstreitigkeiten nur alle Elemente in einen Haltestatus versetzen können. Sie können auch angeben, dass Dauer Elemente enthalten soll, wenn ein Postfach in der Aufbewahrung für eventuelle Rechtsstreitigkeiten eingefügt wird. Ein Element Postfach empfangen oder erstellt wird, wird die Dauer ab dem Datum berechnet. Wenn eine Dauer nicht festgelegt ist, werden die Elemente aufrechterhalten, auf unbestimmte Zeit oder, bis die Sperre entfernt wurde.

Wenn ein Postfach auf einen oder mehrere Compliance-Archive und Aufbewahrung für eventuelle Rechtsstreitigkeiten (ohne Dauer) gleichzeitig eingefügt wird, werden alle Elemente aufrechterhalten auf unbestimmte Zeit oder bis Haltestatus entfernt werden. Wenn Sie die Aufbewahrung für eventuelle Rechtsstreitigkeiten entfernen und der Benutzer wird weiterhin auf eine oder mehrere In-Place-Haltebereiche platziert, werden für den Zeitraum in die Warteschleife Einstellungen angegebenen Elementen anhand der In-Place Hold Kriterien aufrechterhalten.

### NOTE

Wenn Sie ein Postfach auf Compliance-Archiv oder Aufbewahrung für eventuelle Rechtsstreitigkeiten einleiten, wird der Haltestatus auf sowohl die primäre als auch das Archivpostfach platziert. Wenn Sie eine lokale Hauptpostfach in der Warteschleife in einer Exchange-hybridbereitstellung setzen, wird das Cloud-basierten Archivpostfach (sofern aktiviert) auch in die Warteschleife gestellt.

Weitere Informationen finden Sie unter:

- [Aktivieren des Beweissicherungsverfahrens für ein Postfach](#)
- [Platzieren aller Postfächer im Archiv](#)

## Platzieren eines Postfachs in einem Compliance-Archiv

Autorisierte Benutzer, die der Rollengruppe " [Discoveryverwaltung](#) rollenbasierten Zugriffssteuerung (RBAC)" hinzugefügt oder die gesetzliche Aufbewahrungsfrist und Postfachsuche Verwaltungsrollen zugewiesen wurden, können Postfachbenutzer Compliance-Archiv platzieren. Sie können die Aufgabe, führen Datensatzverwalter oder Compliance Officer Anwälte in Ihrer Organisation rechtliche Abteilung beim Zuweisen der geringsten Berechtigungen delegieren. Weitere Informationen zum Zuweisen der Rollengruppe "Discoveryverwaltung" finden Sie unter [Zuweisen von eDiscovery-Berechtigungen in Exchange](#).

Der **Compliance - eDiscovery und -Archiv** -Assistent in der Exchange-Verwaltungskonsole (EAC) oder den **New-MailboxSearch** und verwandte in Exchange Online PowerShell-Cmdlets können Sie um ein Postfach auf Compliance-Archiv zu platzieren. Weitere Informationen zum Platzieren eines Postfachs In-Place Hold finden Sie unter [Create or Remove an In-Place Hold](#).

Viele Organisationen erfordern, dass Benutzer darüber informiert werden, wenn sie in der Warteschleife

platziert sind. Darüber hinaus wird ein Postfach in der Warteschleife, alle Aufbewahrungsrichtlinien für den Postfachbenutzer müssen nicht angehalten werden. Da Nachrichten weiterhin wie erwartet gelöscht werden, werden Benutzer nicht feststellen sie auf enthalten sind. Wenn Ihre Organisation erfordert, dass Benutzer in der Warteschleife darüber informiert werden, können Sie eine Benachrichtigung an das des Postfachbenutzers **Aufbewahrung Comment** -Eigenschaft hinzufügen und verwenden die **RetentionUrl** -Eigenschaft zur Verknüpfung mit einer Webseite Weitere Informationen. Outlook 2010 und höher zeigt die Benachrichtigung und die URL in der backstage-Bereich. Sie müssen Exchange Online PowerShell hinzufügen und verwalten diese Eigenschaften für ein Postfach verwenden.

## Platzieren von öffentlichen Ordner im Archiv

In Exchange Online können Sie Öffentliche Ordner in der Warteschleife mithilfe einer In-Place Hold platzieren. Verwenden die Aufbewahrung für eventuelle Rechtsstreitigkeiten für Öffentliche Ordner wird nicht unterstützt. Wenn Sie eine In-Place Hold erstellen, ist die einzige Option zu einen Haltestatus für alle öffentlichen Ordner in Ihrer Organisation zu platzieren. Das Ergebnis ist, dass alle Postfächer für Öffentliche Ordner ein Compliance-Archivs platziert wird.

Wenn Sie Öffentliche Ordner auf Compliance-Archiv platzieren, werden darüber hinaus auch e-Mail-Nachrichten im Zusammenhang mit der Öffentliche Ordner-Hierarchie Synchronisierungsprozess beibehalten. Dadurch kann Tausende von Hierarchie Synchronisierung weiterführende e-Mail Elemente beibehalten wird. Diese Nachrichten können das Speichercontingent für den Ordner "wiederherstellbare Elemente" auf Postfächer für Öffentliche Ordner gefüllt. Um dies zu verhindern, können Sie ein abfragebasiertes Compliance-Archiv erstellen und fügen Sie die folgenden `property:value` Paar zur Suchabfrage:

```
NOT(subject:HierarchySync*)
```

Das Ergebnis ist, dass alle Nachrichten (im Zusammenhang mit der Synchronisierung der Hierarchie der öffentlichen Ordner), die den Ausdruck "HierarchySync" in der Betreffzeile aufweisen, nicht im Archiv platziert werden.

## Archive und der Ordner "Wiederherstellbare Elemente"

Compliance-Archiv und Aufbewahrung für eventuelle Rechtsstreitigkeiten wird zum Aufbewahren von Elementen des Ordners wiederherstellbare Elemente verwendet. Ordner "wiederherstellbare Elemente" ersetzt die Funktion informell bekannt als die Dumpster in früheren Versionen von Exchange. Ordner "wiederherstellbare Elemente" wird von der Standardansicht von Outlook, Outlook Web App und anderen e-Mail-Clients ausgeblendet. Weitere Informationen zum Ordner "wiederherstellbare Elemente" finden Sie unter [Ordner "wiederherstellbare Elemente"](#).

Wenn ein Benutzer eine Nachricht von einem anderen Ordner als dem Ordner Gelöschte Elemente löscht, wird standardmäßig die Nachricht in den Ordner Gelöschte Objekte verschoben. Dies wird als eine Verschiebung bezeichnet. Wenn ein Benutzer einen weichen ein Element löscht (erreicht durch Drücken der UMSCHALTASTE und DELETE) oder ein Element aus dem Ordner Gelöschte Objekte löscht, wird die Nachricht in den Ordner wiederherstellbare Elemente, wodurch verschwindet aus Sicht des Benutzers verschoben.

Elemente im Ordner "wiederherstellbare Elemente" werden beibehalten, für die Aufbewahrungszeit für das Postfach des Benutzers konfiguriert sind. Standardmäßig ist die Aufbewahrungszeit für gelöschte 14 Tage für Exchange Online-Postfächer. Sie können auch ein Speichercontingent für "wiederherstellbare Elemente" konfigurieren. Dies wird eine potenzielle DOS-Angriff (DoS) aufgrund des Ordners "wiederherstellbare Elemente" Wachstum die Organisation verhindert. Wenn ein Postfach für Compliance-Archiv oder Aufbewahrung für eventuelle Rechtsstreitigkeiten erteilt nicht zur Verfügung, werden Elemente dauerhaft aus dem Ordner "wiederherstellbare Elemente" First-in, zuerst gelöscht, Basis Wenn das wiederherstellbare

Elemente Warnung Kontingent überschritten wird oder wenn das Element wurde in den Ordner für die Dauer länger befand als der Aufbewahrungszeitraum für gelöschte Elemente.

Der Ordner "Wiederherstellbare Elemente" enthält folgende Unterordner zum Speichern gelöschter Elemente an verschiedenen Standorten und zum Erleichtern von In-Situ-Speichern und Beweissicherungsverfahren:

- **Löschvorgänge** - Elemente aus dem Ordner Gelöschte Objekte entfernt oder aus anderen Ordnern vorläufig gelöschten in den Unterordner Löschvorgänge verschoben werden und für den Benutzer sichtbar sind, wenn Sie das Feature gelöschte Elemente wiederherstellen in Outlook und Outlook Web App verwenden. Standardmäßig befinden sich Elemente in diesem Ordner, bis die Aufbewahrungszeit für das Postfach konfiguriert abläuft.
- **Löscht ein** - Wenn ein Benutzer ein Element aus dem Ordner wiederherstellbare Elemente löscht (mithilfe der gelöschte Elemente wiederherstellen Tool in Outlook und Outlook Web App, das Element in den Ordner Benutzerkontenverwaltung verschoben wird. Elemente, die die Aufbewahrungszeit konfiguriert für das Postfach übersteigen werden auch in den Ordner Benutzerkontenverwaltung verschoben. Elemente in diesem Ordner nicht für Benutzer sichtbar sind, wenn sie die Verwendung des gelöschte Elemente wiederherstellen. Wenn Assistenten für verwaltete Ordner das Postfach verarbeitet, werden die Elemente im Ordner Benutzerkontenverwaltung aus dem Postfach gelöscht. Wenn Sie den Postfachbenutzer beweissicherungsverfahrens einleiten, Löschen nicht Assistenten für verwaltete Ordner Elemente in diesem Ordner.
- **DiscoveryHold** - Wenn ein Benutzer ein Compliance-Archiv platziert wird gelöschte Elemente werden in diesem Ordner verschoben. Wenn Assistenten für verwaltete Ordner das Postfach verarbeitet, überprüft es Nachrichten in diesem Ordner. Elemente, die mit der In-Place Hold Abfrage übereinstimmen werden beibehalten, bis die Hold-Periode in der Abfrage angegeben. Wenn keine Hold-Periode angegeben wird, werden Elemente aufrechterhalten auf unbestimmte Zeit oder bis der Benutzer aus dem Archiv entfernt wird.
- **Versionen** – Wenn ein Benutzer platziert auf Compliance-Archiv oder Aufbewahrung für eventuelle Rechtsstreitigkeiten Postfach, das vom Benutzer oder von einem Prozess Elemente von Manipulation oder Änderung geschützt werden müssen. Dies geschieht mit einem Prozess Kopie bei Schreibvorgang. Wenn ein Benutzer oder eine bestimmte Prozess ändert die Eigenschaften eines postfachelements wird eine Kopie des ursprünglichen Elements im Versionsordner gespeichert, bevor der Commit für die Änderung erfolgt ist. Der Vorgang ist für nachfolgende Änderungen wiederholt. Elemente im Ordner "Versionen" erfasst werden auch indiziert und in eDiscovery-suchen zurückgegeben. Nachdem Sie die Sperre entfernt wurde, werden vom Assistenten für verwaltete Ordner Kopien im Ordner "Versionen" entfernt.

### Eigenschaften, die eine Kopie bei Schreibvorgang auslösen

ELEMENTTYP	EIGENSCHAFTEN, DIE EINE KOPIE BEI SCHREIBVORGANG AUSLÖSEN
Nachrichten (IPM.Note*) Beiträge (IPM.Post*)	Betreff Body Anlagen Absender/Empfänger Sende-/Empfangsdatum
Andere Elemente als Nachrichten und Beiträge	Jede Änderung an einer sichtbaren Eigenschaft mit folgenden Ausnahmen: Speicherort des Elements (wenn ein Element zwischen Ordnern verschoben wird) Statusänderung des Elements (gelesen oder ungelesen) Änderungen an dem einem Element zugewiesenen Aufbewahrungstag

ELEMENTTYP	EIGENSCHAFTEN, DIE EINE KOPIE BEI SCHREIBVORGANG AUSLÖSEN
Elemente im Standardordner Entwürfe	Keine (Elemente im Ordner "Entwürfe" sind von der Kopie bei Schreibvorgang ausgenommen)

### IMPORTANT

Die Kopie-bei-Schreibvorgang-Funktion ist für Kalenderelemente im Postfach des Organisators deaktiviert, wenn Besprechungsantworten von Teilnehmern empfangen werden und die Nachverfolgungsinformationen für die Besprechung aktualisiert werden. Für Kalenderelemente und Elemente mit Erinnerungseinstellungen ist die Kopie-bei-Schreibvorgang-Funktion für die Eigenschaften „ReminderTime“ und „ReminderSignalTime“ deaktiviert. Änderungen an diesen Eigenschaften werden nicht von der Kopie-bei-Schreibvorgang-Funktion erfasst. Änderungen an RSS-Feeds werden nicht von der Kopie-bei-Schreibvorgang-Funktion erfasst.

Auch wenn die Ordner "DiscoveryHold", "Purges" und "Versions" für die Benutzer nicht zu sehen sind, werden alle Elemente im Ordner "Wiederherstellbare Elemente" von der Exchange-Suche indiziert und können über die Compliance-eDiscovery gefunden werden. Nachdem der In-Situ-Speicher oder das Beweissicherungsverfahren für das Postfach eines Benutzers beendet wurde, werden Elemente in den Ordner "Purges" und "Versions" durch den Assistenten für verwaltete Ordner gelöscht.

## Archive und Postfachkontingente

Elemente im Ordner "wiederherstellbare Elemente" sind nicht in Richtung des Benutzers Postfachkontingent berechnet. In Exchange Online hat "wiederherstellbare Elemente" eigene Kontingente. Für Exchange werden die Standardwerte für die Postfacheigenschaften *RecoverableItemsWarningQuota* und *RecoverableItemsQuota* jeweils auf 20 und 30 GB festgelegt. In Exchange Online wird das Kontingent für "wiederherstellbare Elemente" (in der primären Postfach des Benutzers) auf 100 GB automatisch erhöht, wenn Sie ein Postfach Beweissicherungsverfahren oder Compliance-Archiv platzieren. Wenn das Speicherkontingent für den Ordner "wiederherstellbare Elemente" in das primäre Postfach eines Postfachs in der Warteschleife ist erreicht bald den Grenzwert erreicht, können Sie die folgenden Schritte ausführen:

- **Aktivieren Sie das Archivpostfach und Aktivieren von erweiterbares Archivierung** – können Sie einen unbegrenzten Speicherplatz für "wiederherstellbare Elemente" einfach durch das Archivpostfach aktivieren und dann das automatisch erweitert, Archivierung Feature in Exchange Online. Dies führt 110 GB für den Ordner "wiederherstellbare Elemente" in das primäre Postfach und eine unbegrenzte Zeitspanne Speicherplatz für den Ordner wiederherstellbare Elemente im Archiv des Benutzers. Finden Sie unter wie: [Aktivieren von archivpostfächern in die Office 365-Sicherheit und Compliance Center](#) und [unbegrenzte Archivierung in Office 365 zu aktivieren](#).

### Hinweise:

- Nachdem Sie das Archiv für ein Postfach aktiviert haben, die fast für "wiederherstellbare Elemente" das Speicherkontingent überschritten ist, Sie möglicherweise ausführen möchten, der Assistent für verwaltete Ordner manuell Auslösen der Assistent, um das Postfach verarbeitet werden, damit abgelaufene Elemente verschoben werden, um die Ordner wiederherstellbare Elemente im Archivpostfach. Anweisungen finden Sie unter Schritt 4 in [Kontingent für Postfächer auf halten wiederherstellbaren Elementen erhöhen](#).
- Beachten Sie, dass weitere Elemente im Postfach des Benutzers in das neue Archivpostfach verschoben werden können. Sie sollten in Betracht ziehen, dem Benutzer mitzuteilen, das dies passieren kann, nachdem Sie das Archivpostfach aktiviert haben.
- **Erstellen eine benutzerdefinierten Aufbewahrungsrichtlinie für Postfächer auf halten** -

zusätzlich zu aktivieren das Archivpostfach und erweiterbares Archivierung für Postfächer Beweissicherungsverfahren oder Compliance-Archiv, sollten Sie außerdem erstellen Sie eine benutzerdefinierte Richtlinie an MRM Retention in Exchange Online für Postfächer auf halten. Dies wenden wir Sie eine Aufbewahrungsrichtlinie auf Postfächer in der Warteschleife, die von der MRM-Standardrichtlinie abweicht, die auf Postfächer angewendet wird, die nicht in der Warteschleife sind. Auf diese Weise können Sie um aufbewahrungstags anzuwenden, die speziell für Postfächer in der Warteschleife entwickelt wurden. Dazu gehört das Erstellen eines neuen aufbewahrungstags für "wiederherstellbare Elemente".

Weitere Informationen finden Sie unter [Erhöhen der wiederherstellbare Elemente Kontingent für Postfächer auf halten.](#)

## Aufbewahrung und E-Mail-Weiterleitung

Benutzer können Outlook und Outlook Web App zum Einrichten von e-Mail-Weiterleitung für ihr Postfach verwenden. E-Mail-Weiterleitung ermöglicht Benutzern das Konfigurieren ihres Postfachs auf forward-e-Mail-Nachrichten, die an ihr Postfach auf anderes Postfach befindet sich in oder außerhalb ihrer Organisation gesendet werden. E-Mail-Weiterleitung kann konfiguriert werden, sodass alle Nachrichten, die an das ursprüngliche Postfach gesendet ist nicht mit dem Postfach kopiert und wird nur an die Weiterleitungsadresse gesendet.

Wenn e-Mail-Weiterleitung für ein Postfach eingerichtet ist, und Nachrichten werden nicht in das ursprüngliche Postfach kopiert, was geschieht, wenn das Postfach in der Warteschleife ist? Die Warteschleife Einstellungen für das Postfach werden bei der Übermittlung überprüft. Wenn die Nachricht die Warteschleife Kriterien für das Postfach entspricht, wird eine Kopie der Nachricht in den Ordner wiederherstellbare Elemente gespeichert. Dies bedeutet, dass Sie eDiscovery-Tools verwenden können, suchen Sie das ursprüngliche Postfach um Nachrichten zu suchen, die an ein anderes Postfach weitergeleitet wurden.

## Löschen eines aufzubewahrenden Postfachs

Beim Löschen der entsprechende Office 365-Konto für ein Postfach, das Beweissicherungsverfahren oder Compliance-Archiv, das Postfach befindet, wird in eines inaktiven Postfachs, der vom Typ des vorläufig gelöschten Postfachs ist konvertiert. Inaktive Postfächer werden verwendet, um den Inhalt des Postfachs eines Benutzers beizubehalten, nachdem die Organisation verlassen. Elemente in eines inaktiven Postfachs bleiben für die Dauer des Haltestatus, die für das Postfach platziert wurde, bevor sie als inaktiv festgelegt wurde. Dies ermöglicht Administratoren, Compliance Officer oder Datensatzverwalter zur Verwendung des Inhaltssuche-Tools in der Office 365-Sicherheit und Compliance Center und Durchsuchen Sie den Inhalt eines inaktiven Postfachs zugreifen. Inaktive Postfächer e-Mail nicht empfangen werden und sind nicht in anderen Listen oder freigegebenen Adressbuch Ihrer Organisation angezeigt. Weitere Informationen finden Sie unter [Übersicht über inaktiver Postfächer in Office 365](#).

# Erstellen oder Entfernen eines Compliance-Archivs

18.12.2018 • 14 minutes to read

## NOTE

Wir haben den 1 Juli 2017 Stichtag zum Erstellen von neuen Compliance-Archive in Exchange Online (in Office 365 und Exchange Online-Plänen) verschoben. Aber weiter unten in diesem Jahr oder frühe nächste Jahr, nicht möglich, neue Compliance-Archive in Exchange Online erstellen. Als Alternative zu Compliance-Archive verwenden können Sie [eDiscovery-Fälle](#) oder [Aufbewahrungsrichtlinien](#) in die Office 365-Sicherheit und Compliance Center verwenden. Nachdem wir neue Compliance-Archive außer Betrieb nehmen, Sie vermutlich noch vorhandene Compliance-Archive ändern, und Erstellen von neuen Compliance-Archive im Exchange Server und Exchange Hybrid-Bereitstellungen werden weiterhin unterstützt. Und Sie vermutlich noch Postfächer auf Aufbewahrung für eventuelle Rechtsstreitigkeiten zu platzieren.

Eine In-Place Hold behält alle Inhalt von Postfächern, einschließlich der gelöschten Objekte und der ursprünglichen Versionen geänderter Objekte. Eine solche Postfachelemente werden in einer [Compliance - eDiscovery](#)-Suche zurückgegeben. Wenn Sie eine In-Place Hold auf dem Postfach eines Benutzers auf platzieren, sind den Inhalt in der entsprechenden Archivpostfach (falls aktiviert) auch in die Warteschleife gestellt und in einer eDiscovery-Suche zurückgegeben.

## Was sollten Sie wissen, bevor Sie beginnen?

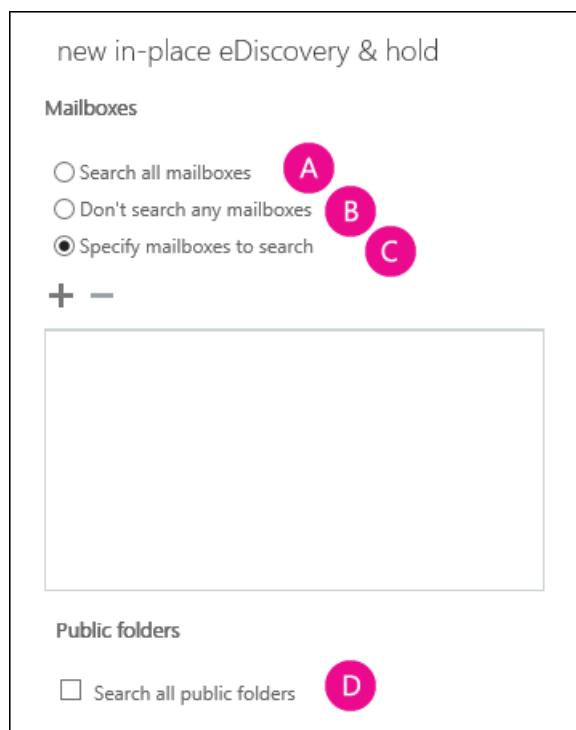
- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Compliance-Archiv" im Thema [Messaging Policy and Compliance Permissions](#).
- Um ein Exchange Online-Postfach auf Compliance-Archiv zu platzieren, müssen sie eine Lizenz Exchange Online (Plan 2) zugewiesen werden. Wenn ein Postfach mit einer Exchange Online (Plan 1)-Lizenz zugewiesen ist, müssten Sie weisen Sie ihr eine separate Lizenz der Exchange Online-Archivierung auf platziert halten.
- Je nach Ihrer Active Directory-Topologie und Replikationswartzeit kann es bis zu einer Stunde dauern, bis ein Compliance-Archiv fertig gestellt ist.
- Wenn Sie eine In-Place Hold auf dem Postfach eines Benutzers, platzieren wird Inhalt im Archivpostfach des Benutzers wie bereits erklärt auch in der Warteschleife platziert. Wenn Sie eine In-Place Hold in einem lokalen primären Postfach in einer Exchange-hybridbereitstellung setzen, wird das Cloud-basierten Archivpostfach (sofern aktiviert) auch in der Warteschleife platziert.
- Wenn ein Benutzer in mehreren In-Situ-Speichern platziert wird, werden die Suchabfragen von einem abfragebasierten Archiv kombiniert (mit **OR** -Operatoren). In diesem Fall beträgt die maximale Anzahl von Stichwörtern in allen abfragebasierten Archiven für ein Postfach 500. Bei mehr als 500 Stichwörtern werden sämtliche Inhalte des Postfachs archiviert (nicht bloß die Inhalte, die mit den Suchkriterien übereinstimmen). Alle Inhalte werden archiviert, bis die Gesamtzahl von Stichwörtern auf 500 oder weniger verringert wird.
- In Exchange Online wird das Kontingent für "wiederherstellbare Elemente" auf 100 GB automatisch erhöht, wenn Sie eine Compliance-Archiv für ein Postfach platzieren. Die Standardgröße des Ordners "wiederherstellbare Elemente" beträgt 30 GB.
- In Exchange Online können Sie eine Compliance-Archiv auf Office 365 Gruppen platzieren. Wenn Sie eine

Office 365-Gruppe in der Warteschleife einleiten, wird das Gruppenpostfach in der Warteschleife platziert; die Postfächer der Mitglieder der Gruppe werden nicht in die Warteschleife gestellt. Informationen zu Office 365-Gruppen finden Sie unter [Informationen zu Office 365-Gruppen](#).

## Erstellen eines Compliance-Archivs

### Erstellen eines In-Situ-Speichers über das EAC

1. Navigieren Sie zu **Verwaltung der Richtlinientreue > Compliance - eDiscovery und -Archiv.**
2. Klicken Sie auf **neue** 
3. Geben Sie im Abschnitt **Compliance-eDiscovery und Compliance-Archiv** auf der Seite **Name und Beschreibung** einen Namen für die Suche und optional eine Beschreibung ein, und klicken Sie dann auf **Weiter**.
4. Wählen Sie auf der Seite **Postfächer und Öffentliche Ordner** die Inhaltsspeicherorte aus, die Sie im Archiv platzieren möchten, und klicken Sie dann auf **Weiter**.



5. **Suchen Sie alle Postfächer:** Sie können nicht mit dieser Option zum Erstellen einer In-Place Hold. Sie können mit dieser Option für Compliance-eDiscovery-suchen, aber zum Erstellen einer Compliance-Archivs müssen Sie auswählen, die bestimmte Postfächer, die Sie in die Warteschleife stellen möchten.
6. **Keine Postfächer suchen:** Wählen Sie diese Option aus, wenn Sie eine In-Place Hold ausschließlich für Öffentliche Ordner erstellen.
7. **Angeben von Postfächern zu suchen:** Wählen Sie diese Option aus, und klicken Sie dann auf **Hinzufügen**  , wählen Sie die Postfächer oder Verteilergruppen, die Sie in die Warteschleife stellen möchten. In Exchange Online können Sie auch die Office 365-Gruppen in der Warteschleife platziert auswählen.
8. **Alle öffentlichen Ordner suchen:** In Exchange Online, Sie können wählen Sie dieses Kontrollkästchen, um alle öffentlichen Ordner in Ihrer Organisation in der Warteschleife platziert. Wie bereits erklärt um eine In-Place Hold nur für Öffentliche Ordner zu erstellen, werden Sie sicher, dass Sie die Option **nicht suchen, alle Postfächer** auswählen.
9. Klicken Sie auf der Seite **Suchabfrage** führen Sie die folgenden Felder, und klicken Sie dann auf **Weiter**.

- **Alle Inhalte der Benutzerpostfächer enthalten:** Klicken Sie auf diese Schaltfläche, um alle Inhalte in ausgewählten Postfächern in der Warteschleife platziert.
- **Filter basierend auf Kriterien:** Klicken Sie auf diese Schaltfläche, um Suchkriterien, einschließlich von Schlüsselwörtern, Start- und Enddaten, Absender und Empfänger-Adressen und Nachrichtentypen. Beim Erstellen einer abfragebasierter Archive, nur die Elemente, die den Kriterien erhalten bleiben, Suchkriterien entsprechen.

#### TIP

Wenn Sie Öffentliche Ordner auf Compliance-Archiv platzieren, werden auch e-Mail-Nachrichten im Zusammenhang mit der Öffentliche Ordner-Hierarchie Synchronisierungsprozess beibehalten. Dadurch kann Tausende von Hierarchie Synchronisierung weiterführende e-Mail Elemente beibehalten wird. Diese Nachrichten können das Speicherkontingent für den Ordner "wiederherstellbare Elemente" auf Postfächer für Öffentliche Ordner gefüllt. Um dies zu verhindern, können Sie ein abfragebasiertes Compliance-Archiv erstellen und fügen Sie die folgenden `property:value` Paar zur Suchabfrage: > `NOT(subject:HierarchySync*)` > das Ergebnis ist, die jede Nachricht (bezieht sich auf die Synchronisierung von Öffentliche Ordner-Hierarchie), die den Ausdruck enthält "HierarchySync" in der Betreffzeile wird nicht in der Warteschleife platziert.

6. Aktivieren Sie auf der Seite **Einstellungen für Compliance-Archive** das Kontrollkästchen **Inhalt, der mit der Suchanfrage übereinstimmt, in ausgewählten Postfächern aufbewahren**, und wählen Sie eine der folgenden Optionen:

- **In einer Warteschleife verbleibt:** Klicken Sie auf diese Schaltfläche, um auf eine aufzubewahren von der Suche zurückgegebenen Elementen zu platzieren. Elemente in der Warteschleife bleiben, bis Sie des Postfachs aus der Suche entfernen oder entfernen die Suche erhalten.
- **Geben Sie Anzahl der Tage speichern Elemente relativ zu ihrer Empfangsdatum:** Klicken Sie auf diese Schaltfläche, um Elemente für einen bestimmten Zeitraum zu halten. Beispielsweise können Sie diese Option, wenn Ihre Organisation erfordert, dass alle Nachrichten mindestens sieben Jahre lang aufbewahrt werden. Sie können eine zeitbasierten Compliance-Archiv zusammen mit einer Aufbewahrungsrichtlinie stellen Sie sicher, dass Elemente in sieben Jahren gelöscht werden. Weitere Informationen zu Aufbewahrungsrichtlinien Richtlinien finden Sie unter [Aufbewahrungstags](#) und [Aufbewahrungsrichtlinien](#).

#### Verwenden von Exchange Online PowerShell zum Erstellen einer Compliance-Archivs

Bei diesem Beispiel wird das Compliance-Archiv "Hold-CaseId012" erstellt und das Postfach "joe@contoso.com" im Archiv platziert.

#### IMPORTANT

Wenn Sie zusätzliche Suchparameter für eine In-Place Hold nicht angeben, halten alle Elemente in der angegebenen Quelle, die Postfächer platziert werden. Wenn Sie den `ItemHoldPeriod`-Parameter nicht angeben, werden Elemente in der Warteschleife platziert auf unbestimmte Zeit oder das Postfach ist entweder aus dem Haltebereich entfernt oder der Haltebereich gelöscht.

```
New-MailboxSearch "Hold-CaseId012"-SourceMailboxes "joe@contoso.com" -InPlaceHoldEnabled $true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-MailboxSearch](#).

#### Woher wissen Sie, ob dieser Vorgang erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um die erfolgreiche Erstellung eines Compliance-Archivs zu überprüfen:

- Überprüfen Sie in der Exchange-Verwaltungskonsole, ob das Compliance-Archiv in der Listenansicht der Registerkarte **Compliance-eDiscovery und -Archiv** aufgeführt wird.
- Rufen Sie mit dem Cmdlet **Get-MailboxSearch** die Postfachsuche ab, und überprüfen Sie die Suchparameter. Ein Beispiel für das Abrufen einer Postfachsuche finden Sie in den Beispielen unter [Get-MailboxSearch](#).

[Zurück zum Seitenanfang](#)

## Entfernen eines Compliance-Archivs

### IMPORTANT

In Exchange Server können ein In-Place Hold und In-Place eDiscovery Postfachsuchvorgänge verwendet werden. Sie können keine angehaltene postfachsuche entfernen, die für die Compliance-Archiv verwendet wird. Sie müssen die In-Place Hold zuerst deaktivieren, durch Deaktivieren des Kontrollkästchens **die Suchabfrage im ausgewählten Postfächer auf übereinstimmende Place Inhalt enthalten** auf der Seite **Einstellungen In-Place Hold** oder durch Festlegen des Parameters *InPlaceHoldEnabled* auf `$false` in Exchange Online PowerShell. Sie können auch ein Postfach mithilfe der in der Suche angegebenen mit dem Parameter *SourceMailboxes* entfernen.

### Entfernen eines In-Situ-Speichers über das EAC

1. Navigieren Sie zu **Verwaltung der Richtlinientreue > Compliance - eDiscovery und -Archiv**.
2. Wählen Sie in der Listenansicht die Compliance-Archivs zu entfernen, und klicken Sie dann auf **Bearbeiten**.
3. Deaktivieren Sie in den Eigenschaften von **Compliance-eDiscovery und -Archiv** auf der Seite **Compliance-Archiv** das Kontrollkästchen **Inhalt, der mit der Suchanfrage übereinstimmt, in ausgewählten Postfächern aufzubewahren**, und klicken Sie dann auf **Speichern**.
4. Aktivieren Sie das Compliance-Archiv wieder aus der Liste, und klicken Sie dann auf **Löschen**.
5. Klicken Sie in der Warnung auf **Ja**, um die Suche zu entfernen.

### Verwenden von Exchange Online PowerShell, Entfernen eines Compliance-Archivs

Bei diesem Beispiel wird zunächst das Compliance-Archiv "Hold-CaseId012" deaktiviert und anschließend die Postfachsuche entfernt.

```
Set-MailboxSearch "Hold-CaseId012" -InPlaceHoldEnabled $false
Remove-MailboxSearch "Hold-CaseId012"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailboxsearch](#).

### Woher wissen Sie, ob dieser Vorgang erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um die erfolgreiche Entfernung eines Compliance-Archivs zu überprüfen:

- Mithilfe der Exchange-Verwaltungskonsole sicher, dass die In-Place Hold in der Listenansicht die **Compliance - eDiscovery, Compliance - Archive** Registerkarte nicht angezeigt wird.
- Rufen Sie mit dem Cmdlet **Get-MailboxSearch** alle Postfachsuchvorgänge ab, und vergewissern Sie sich, dass die Suche, die Sie entfernt haben, nicht mehr aufgeführt ist. Ein Beispiel für das Abrufen einer Postfachsuche finden Sie in den Beispielen unter [Get-MailboxSearch](#).

[Zurück zum Seitenanfang](#)

# Compliance-eDiscovery

18.12.2018 • 55 minutes to read

## NOTE

Wir haben den 1 Juli 2017 Stichtag für das Erstellen von neuer Compliance-eDiscovery-suchen im Exchange Online (in Office 365 und Exchange Online-Plänen) verschoben. Aber später in diesem Jahr oder frühe nächste Jahr, nicht möglich, neue Suchvorgänge in Exchange Online zu erstellen. Zum Erstellen von eDiscovery-Suchen starten Sie [Inhaltssuche](#) in die Office 365-Sicherheit und Compliance Center verwenden. Nachdem wir neue Compliance-eDiscovery-suchen außer Betrieb nehmen, Sie vermutlich noch vorhandene Compliance-eDiscovery-suchen zu ändern, und erstellen neue Compliance-eDiscovery-suchen im Exchange Server und Exchange Hybrid-Bereitstellungen werden weiterhin unterstützt.

Wenn Ihre Organisation gerichtlichen Ermittlungen (im Zusammenhang mit der Unternehmensrichtlinien, Compliance oder Rechtsstreitigkeiten) entspricht, helfen In-Place eDiscovery in Microsoft Exchange Server und Exchange Online Discovery Suchvorgänge für relevante Inhalte innerhalb Ihnen Postfächer. Exchange Server und Exchange Online bieten auch Sammelsuche-Funktion und Integration mit Microsoft SharePoint 2013 und Microsoft SharePoint Online. Verwenden das eDiscovery Center in SharePoint, können Sie suchen nach und halten Sie alle Inhalte im Zusammenhang mit der Fall, einschließlich SharePoint 2013 und SharePoint Online-Websites, Dokumenten, Dateifreigaben indiziert von SharePoint (nur SharePoint 2013), Inhalt von Postfächern in Exchange und archivierten Lync 2013-Inhalt. Sie können auch In-Place eDiscovery in einer hybriden Exchange-Umgebung verwenden, um lokalen und cloudbasierten Postfächer in derselben Suche zu suchen.

## IMPORTANT

Compliance-eDiscovery ist ein leistungsfähiges Feature, das einem Benutzer mit den entsprechenden Berechtigungen für den Zugriff auf alle messaging Datensätze in der gesamten Organisation Exchange Server oder Exchange Online gespeichert potenziell ermöglicht. Es ist wichtig, steuern und überwachen Discovery-Aktivitäten, einschließlich ihrer Mitglieder der Rollengruppe "Discoveryverwaltung", Zuweisung von der Verwaltungsrolle Postfachsuche und Zuweisung von Postfachzugriff auf discoverypostfächer.

## Funktionsweise von Compliance-eDiscovery

Für die Compliance-eDiscovery-Suche werden die von der Exchange-Suche erstellten Inhaltsindizes verwendet. Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) stellt die Rollengruppe [Erkennungsverwaltung](#) zum Delegieren von Suchaufgaben an nicht technische Mitarbeiter bereit, ohne dass erhöhte Rechte erteilt werden müssen, mit denen ein Benutzer möglicherweise Änderungen an der Exchange-Konfiguration vornehmen kann. Die Exchange-Verwaltungskonsole stellt eine benutzerfreundliche Suchoberfläche für nicht technisches Personal wie z. B. Mitarbeiter der Rechtsabteilung, Richtlinienbeauftragte, Datensatzmanager und Mitarbeiter der Personalabteilung (Human Resources, HR) bereit.

Autorisierte Benutzer können Compliance-eDiscovery-Suchen durchführen, indem sie die Postfächer auswählen und dann Suchkriterien wie Stichwörter, Start- und Enddaten, Absender- und Empfängeradressen und Nachrichtentypen angeben. Nach der Suche können autorisierte Benutzer eine der folgenden Aktionen auswählen:

- **Schätzung der Suchergebnisse:** Diese Option liefert eine Schätzung der Gesamtgröße sowie die Anzahl der Elemente, die von der Suche basierend auf der angegebenen Kriterien zurückgegeben wird.
- **Vorschau der Suchergebnisse:** Diese Option bietet Ihnen eine Vorschau der Ergebnisse. Nachrichten,

die von jedem Postfach durchsucht zurückgegeben werden angezeigt.

- **Kopieren der Suchergebnisse:** mit dieser Option können Sie Nachrichten in ein discoverypostfach kopieren.
- **Suchergebnisse exportieren:** Nachdem die Suchergebnisse in ein discoverypostfach kopiert wurden, können Sie diese in eine PST-Datei exportieren.

The screenshot shows the Exchange admin center interface. On the left, a sidebar lists compliance management categories: recipients, permissions, organization, protection, mail flow, mobile, public folders, and unified messaging. The main area is titled 'in-place eDiscovery & hold' and contains a search bar and a table of search results. The table has columns: NAME, OLD STATUS, MODIFIED DATE, and CREATED BY. A context menu is open over the first result, with options 'Estimate search results' and 'Copy search results' highlighted. To the right of the table, a detailed view of the search results is shown, including the status 'Estimate Succeeded', run by 'Administrator', run on '8/20/2014 5:04 PM', size '36 MB', items '647', and a 'Preview search results' link.

## Exchange-Suche

Für die Compliance-eDiscovery-Suche werden die von der Exchange-Suche erstellten Inhaltsindizes verwendet. Die Exchange-Suche basiert nun auf Microsoft Search Foundation, einer umfassenden Suchplattform mit einer wesentlich verbesserten Indizierungs- und Abfrageleistung und Suchfunktionalität. Da Microsoft Search Foundation auch von anderen Office-Produkten verwendet wird, SharePoint 2013 eingeschlossen, wird eine höhere Interoperabilität und eine ähnliche Abfragesyntax für diese Produkte bereitgestellt.

Dank eines einzigen Inhaltsindizierungsmoduls müssen keine zusätzlichen Ressourcen zum Durchforsten und Indizieren von Postfachdatenbanken für die Compliance-eDiscovery-Suche verwendet werden, wenn Mitarbeiter von IT-Abteilungen eDiscovery-Anforderungen erhalten.

Die Compliance-eDiscovery-Suche verwendet KQL (Keyword Query Language) - eine Abfragesyntax, die der von der Sofortsuche in Microsoft Outlook und Outlook Web App verwendeten AQS (Advanced Query Syntax) ähnelt. Benutzer mit KQL-Kenntnissen können auf einfache Weise leistungsstarke Suchabfragen zum Durchsuchen von Inhaltsindizes erstellen.

Weitere Informationen zu den von der Exchange-Suche indizierten Dateiformaten finden Sie unter [File Formats Indexed By Exchange Search](#).

## Die Rollengruppe "Discoveryverwaltung" und Verwaltungsrollen

Damit autorisierte Benutzer Compliance-eDiscovery-Suchen durchführen können, müssen Sie die Benutzer der Rollengruppe [Discovery Management](#) hinzufügen. Diese Rollengruppe umfasst zwei Verwaltungsrollen: [Mailbox Search Role](#), die einem Benutzer das Ausführen einer Compliance-eDiscovery-Suche ermöglicht, und [Legal Hold Role](#), mit der Benutzer ein Postfach in einem Compliance-Archiv platzieren oder ein Beweissicherungsverfahren für das Postfach aktivieren können.

Standardmäßig werden Benutzern oder Exchange-Administratoren keine Berechtigungen zur Ausführung von Compliance-eDiscovery-Aufgaben zugewiesen. Exchange-Administratoren, die Mitglieder der Rollengruppe "Organisationsverwaltung" sind, können Benutzer zur Rollengruppe "Discoveryverwaltung" hinzufügen und benutzerdefinierte Rollengruppen erstellen, um die Berechtigungen für einen Discoverymanager auf einen bestimmten Benutzersatz zu beschränken. Weitere Informationen zum Hinzufügen von Benutzern zur Rollengruppe "Discoveryverwaltung" finden Sie unter [Zuweisen von eDiscovery-Berechtigungen in Exchange](#).

#### IMPORTANT

Wenn ein Benutzer noch nicht der Rollengruppe "Discoveryverwaltung" hinzugefügt wurde, oder der Postfachsuche Rolle nicht zur Verfügung, die **In-Place eDiscovery und -Archiv** -Benutzeroberfläche wird nicht angezeigt, in der Exchange-Verwaltungskonsole, und die Compliance-eDiscovery-Cmdlets sind nicht verfügbar in Exchange Online-PowerShell.

Durch das Überwachen von Änderungen an RBAC-Rollen (diese Funktion ist standardmäßig aktiviert) wird sichergestellt, dass die richtigen Datensätze gespeichert werden, um die Zuweisung der Rollengruppe "Discoveryverwaltung" nachzuverfolgen zu können. Sie können den Administrator-Rollengruppenbericht verwenden, um nach Änderungen an Administratorrollengruppen zu suchen. Weitere Informationen finden Sie unter [Search the role group changes or administrator audit logs](#).

## Benutzerdefinierte Verwaltungsbereiche für Compliance-eDiscovery

Sie können mithilfe eines benutzerdefinierten Verwaltungsbereichs lassen Sie bestimmte Personen oder Gruppen In-Place eDiscovery verwenden, um eine Teilmenge von Postfächern in der Exchange-Server oder Exchange Online-Organisation zu suchen. Angenommen, möchten Sie einen Discovery-Manager nur die Postfächer der Benutzer in einem bestimmten Standort oder jede Abteilung durchsuchen lassen. Zu diesem Zweck Erstellen eines benutzerdefinierten Verwaltungsbereichs, das einen benutzerdefinierten Empfängerfilter verwendet, um die steuern, welche Postfächer durchsucht werden können. Empfängerfilter Bereiche verwenden Filter basierend auf dem Empfängertyp oder anderen Empfängereigenschaften bestimmte Empfänger als Ziel.

Für Compliance-eDiscovery ist die einzige Eigenschaft auf ein Benutzerpostfach, die Sie verwenden können, um einen Empfängerfilter für einen benutzerdefinierten Bereich erstellen Verteilung der Gruppenmitgliedschaft. Bei Verwendung anderer Eigenschaften wie *CustomAttributeN*, *\_Abteilung\_* oder *PostalCode*, fällt für die Suche aus, wenn sie von einem Mitglied der Rollengruppe ausgeführt wird, die den benutzerdefinierten Bereich zugewiesen hat. Weitere Informationen finden Sie unter [Erstellen eines benutzerdefinierten Verwaltungsbereichs für Compliance - eDiscovery-suchen](#).

## Integration in SharePoint Server und SharePoint Online

Exchange Server und Exchange Online bieten Integration in SharePoint Server und SharePoint Online mit dem ein Discovery-Manager, um eDiscovery Center in SharePoint verwenden, um die folgenden Aufgaben auszuführen:

- **Suche und beibehalten Inhalte aus einem einzigen Standort:** ein autorisierten Discovery-Manager kann suchen und Aufbewahren von Inhalten in SharePoint und Exchange, einschließlich Lync Inhalte wie Instant messaging-Unterhaltungen und einem freigegebenen meeting Dokumente archiviert in der Exchange-Postfächer.
- **Fall-Verwaltung** Das eDiscovery Center verwendet einen Ansatz zur Fall-Verwaltung mit eDiscovery, der das Erstellen von Fällen und Suchen sowie für jeden Fall das Aufbewahren von Inhalten über verschiedene Repositorys hinweg ermöglicht.
- **Suchergebnisse exportieren:** ein Discovery-Manager kann eDiscovery Center verwenden, um die Suchergebnisse zu exportieren. Inhalt von Postfächern in den Suchergebnissen enthalten, wird in eine

PST-Datei exportiert.

SharePoint verwendet für Inhaltsindizierung und -abfrage ebenfalls Microsoft Search Foundation. Unabhängig davon, ob ein Discoverymanager die Exchange-Verwaltungskonsole oder das eDiscovery Center zum Durchsuchen von Exchange-Inhalten verwendet, werden dieselben Postfachinhalte zurückgegeben.

Bevor Sie eDiscovery Center in SharePoint zum Suchen von Exchange-Postfächern verwenden können, müssen Sie in lokalen Bereitstellungen Vertrauensstellung zwischen den beiden Anwendungen einrichten. In Exchange Server und SharePoint 2013, erfolgt dies OAuth-Authentifizierung verwenden. Weitere Informationen hierzu finden Sie unter [Konfigurieren von Exchange für SharePoint eDiscovery Center](#). eDiscovery-suchen aus SharePoint ausgeführt werden vom Exchange mithilfe von RBAC autorisiert. Für ein SharePoint-Benutzer zu einer eDiscovery-Suche von Exchange-Postfächern ausführen können müssen sie delegierte Discoveryverwaltung Berechtigung in Exchange zugewiesen werden. Um den Inhalt von Postfächern in einer eDiscovery-Suche mithilfe von SharePoint eDiscovery Center ausgeführt zurückgegebenen Vorschau anzeigen können, benötigen der Discovery-Manager ein Postfach in der gleichen Exchange-Organisation.

Schrittweise Anleitungen zum Einrichten eines eDiscovery Center in einer Office 365-Organisation finden Sie unter [Einrichten eines eDiscovery Center in SharePoint Online](#).

## eDiscovery in einer Exchange-Hybridbereitstellung

Um standortübergreifende eDiscovery-Suchen in einer Exchange Server-Hybrid-Organisation erfolgreich ausgeführt haben, müssen Sie (Open Authorization) OAuth-Authentifizierung zwischen Ihrer Exchange lokal und Exchange Online-Organisation konfigurieren, sodass Sie verwenden können Compliance-eDiscovery, um lokalen und cloudbasierten Postfächer zu suchen. OAuth-Authentifizierung ist ein Server-zu-Server-Authentifizierung-Protokoll, die Clientanwendungen zum Authentifizieren miteinander ermöglicht.

Die OAuth-Authentifizierung wird in den folgenden eDiscovery-Szenarien in einer Exchange-Hybridbereitstellung unterstützt:

- Durchsuchen lokaler Postfächer, für die die Exchange Online-Archivierung für cloudbasierte Archivpostfächer verwendet wird.
- Durchsuchen der lokalen und cloudbasierten Postfächer in derselben eDiscovery-Suche.
- Durchsuchen lokaler Postfächer mit dem eDiscovery Center in SharePoint Online.

Weitere Informationen zu den eDiscovery-Szenarien, für die die OAuth-Authentifizierung in einer Exchange-Hybridbereitstellung konfiguriert werden muss, finden Sie unter [Using Oauth Authentication to Support eDiscovery in an Exchange Hybrid Deployment](#). Schrittweise Anleitungen zum Konfigurieren der OAuth-Authentifizierung, sodass eDiscovery unterstützt wird, finden Sie unter [Configure OAuth Authentication Between Exchange and Exchange Online Organizations](#).

## Discoverypostfächer

Nachdem Sie eine Compliance-eDiscovery-Suche erstellt haben, können Sie die Suchergebnisse in ein Zielpostfach kopieren. Die Exchange-Verwaltungskonsole ermöglicht Ihnen die Auswahl eines Discoverypostfachs als Zielpostfach. Bei einem Discoverypostfach handelt es sich um einen speziellen Postfachtyp, mit dem die folgenden Funktionen bereitgestellt werden:

- **Einfachere und sichere Postfach Zielauswahl:** Wenn Sie der Exchange-Verwaltungskonsole verwenden, um Compliance-eDiscovery-Suchergebnisse kopieren, nur discoverypostfächer zur Verfügung gestellt werden als ein Repository, in dem die Suchergebnisse gespeichert. Sie müssen nicht über eine potenziell lange Liste von Postfächern in der Organisation zur Verfügung zu sortieren. Dadurch werden auch die Möglichkeit, ein Discovery-Manager versehentlich auswählen Postfach eines anderen Benutzers oder einer unsicheren Postfach in der sensible Nachrichten gespeichert.

- **Großes Postfach Speicherkontingent:** das Zielpostfach sollten in der Lage, eine große Datenmenge Nachricht speichern, die von einer Compliance-eDiscovery-Suche zurückgegeben werden kann. Standardmäßig haben discoverypostfächer ein Postfach Speichercontingent von 50 GB (Gigabyte). Diese Speichercontingent kann nicht erhöht werden.
- **Standardmäßig sicherer:** wie alle Postfachtypen, ein discoverypostfach zugeordnete Benutzer Active Directory-Konto verfügt. Dieses Konto ist jedoch standardmäßig deaktiviert. Nur Benutzer, die auf ein discoverypostfach zuzugreifen ausdrücklich genehmigt haben Zugriff darauf. Mitglieder der Rollengruppe "Discoveryverwaltung" werden das standarddiscoverypostfach Vollzugriffsberichtigungen zugewiesen. Eine beliebige zusätzliche discoverypostfächer, die Sie erstellen keinen Postfach Zugriffsberichtigungen und keinem Benutzer zugewiesen.
- **E-Mail-Übermittlung deaktiviert:** zwar sichtbar in Exchange-Adresslisten, können keine Benutzer in ein discoverypostfach e-Mail senden. E-Mail-Übermittlung an discoverypostfächer ist unzulässig, mithilfe der Übermittlung Einschränkungen. Dadurch wird die Integrität der Suchergebnisse in ein discoverypostfach kopiert beibehalten.

Exchange-Setup erstellt ein discoverypostfach mit dem Anzeigennamen **Discoverysuchpostfach**. Exchange Online PowerShell können Sie zusätzliche discoverypostfächer erstellen. Standardmäßig wird nicht die discoverypostfächer, die Sie erstellen Zugriffsberichtigungen Postfach zugewiesen haben. Sie können Vollzugriff-Berechtigungen für ein Discovery-Manager Zugriff auf Nachrichten in ein discoverypostfach kopiert zuweisen. Weitere Informationen hierzu finden Sie unter [Erstellen eines discoverypostfachs](#).

Für die Compliance-eDiscovery-Suche wird außerdem ein Systempostfach mit dem Anzeigennamen **SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}** zum Speichern von Compliance-eDiscovery-Metadaten verwendet. Systempostfächer werden weder in der Exchange-Verwaltungskonsole noch in Exchange-Adresslisten angezeigt. Bevor Sie in Organisationen mit lokalem Exchange eine Postfachdatenbank entfernen können, in der sich das Systempostfach für die Compliance-eDiscovery-Suche befindet, müssen Sie das Postfach in eine andere Postfachdatenbank verschieben. Wenn das Postfach entfernt wird oder beschädigt ist, können die Discoverymanager erst wieder eDiscovery-Suchen durchführen, nachdem das Postfach neu erstellt wurde. Weitere Informationen finden Sie unter [Re-Create the Discovery System Mailbox](#).

## Verwenden der Compliance-eDiscovery-Suche

Benutzer, die der Rollengruppe "Discoveryverwaltung" hinzugefügt wurden, können Compliance-eDiscovery-Suchen durchführen. Sie können eine Suche mithilfe der webbasierten Benutzeroberfläche in der Exchange-Verwaltungskonsole ausführen. Dies vereinfacht für Anwender wie Datensatzverwalter, Compliance-beauftragte oder Legal und Personalabteilung Compliance-eDiscovery nicht dazu verwenden. Sie können auch die Exchange Online PowerShell verwenden, um eine Suche durchzuführen. Weitere Informationen finden Sie unter [Erstellen einer Compliance - eDiscovery-Suche](#)

### NOTE

Compliance-eDiscovery können Sie in lokalen Organisationen Postfächer auf Servern mit Exchange Server-Postfach zu suchen. Verwenden Sie Suche in mehreren Postfächern auf einem Exchange 2010-Server, um Postfächer auf Exchange 2010-Postfachserver zu suchen. >> In einer hybridbereitstellung eine Umgebung ist, in dem einige Postfächer vorhanden sind, auf die lokalen Postfachserver und einige Postfächer in einer Cloud-basierten Organisation vorhanden sind, können Sie Compliance-eDiscovery-Suchen Ihrer cloudbasierten Postfächer mit Ausführen der Exchange-Verwaltungskonsole in Ihrer lokalen Organisation. Wenn Sie Nachrichten in ein discoverypostfach kopieren möchten, müssen Sie ein lokales Discovery-Postfach auswählen. Nachrichten von Cloud-basierten Postfächern, die in den Suchergebnissen zurückgegeben werden, werden in der angegebenen lokalen Discovery-Postfach kopiert. Weitere Informationen zu hybridbereitstellungen finden Sie unter [Hybridbereitstellungen in Exchange Server](#).

Ihnen das Erstellen einer Compliance-eDiscovery-Suche und verwendet ein Compliance-Archiv, um die Suchergebnisse aufzubewahren. Wenn Sie eine Compliance-eDiscovery-Suche erstellen, wird ein Suchobjekt im Compliance-eDiscovery-Systempostfach erstellt. Dieses Objekt kann bearbeitet werden, um die Suche zu starten, zu beenden, zu ändern und zu entfernen. Nachdem Sie die Suche erstellt haben, können Sie eine Schätzung der Suchergebnisse abrufen, die eine Schlüsselwortstatistik zur Ermittlung der Effektivität einer Abfrage umfasst. Sie können auch eine Livevorschau der bei der Suche zurückgegebenen Elemente anzeigen, in der Sie die Nachrichteninhalte, die Anzahl der von jedem Quellpostfach zurückgegebenen Nachrichten sowie die Gesamtzahl an Nachrichten anzeigen können. Diese Informationen können Sie bei Bedarf zur weiteren Optimierung Ihrer Abfrage verwenden.

Wenn Sie mit den Suchergebnissen zufrieden sind, können Sie sie in ein Discoverypostfach kopieren. Sie können auch die Exchange-Verwaltungskonsole oder Outlook verwenden, um ein Discoverypostfach oder Teile seiner Inhalte in eine PST-Datei zu exportieren.

Wenn Sie eine Compliance-eDiscovery-Suche erstellen, müssen Sie die folgenden Parameter angeben:

- **Name:** der Suchbegriff wird verwendet, um die Suche zu identifizieren. Wenn Sie die Suchergebnisse in ein discoverypostfach kopieren, wird ein Ordner in das discoverypostfach mit den Suchbegriff und der Zeitstempel zur eindeutigen Identifizierung von Suchergebnissen in ein discoverypostfach erstellt.
- **Postfächer:** Sie können auswählen, alle Postfächer in Ihrer Exchange-Server oder Exchange Online-Organisation durchsuchen, oder geben Sie die Postfächer zu suchen. Ein Benutzer der primären und archivpostfächer sind in der Suche enthalten. Wenn Sie die gleiche Suche verwenden, um Elemente in die Warteschleife stellen möchten, müssen Sie die Postfächer angeben. Sie können angeben, dass eine Verteilergruppe um Postfachbenutzer enthalten sind, die Mitglieder dieser Gruppe sind. Mitgliedschaft in der Gruppe wird einmal berechnet, wenn die Suche zu erstellen und nachfolgende Änderungen an der Gruppenmitgliedschaft werden in die Suche nicht automatisch wiedergegeben.

In Exchange Online können Sie auch Office 365-Gruppen als eine Inhaltsquelle angeben, sodass die das Gruppenpostfach durchsucht (oder archiviert) wird. Beachten Sie, dass beim Hinzufügen einer Office 365-Gruppe zu einer Compliance-eDiscovery-Suche nur das Gruppenpostfach durchsucht wird; die Postfächer der Gruppenmitglieder werden nicht durchsucht.

- **Suchabfrage:** Sie können enthalten alle Inhalt von Postfächern aus der angegebenen Postfächer oder verwenden Sie eine Suchabfrage zum Zurückgeben von Elementen, die für den Fall oder die Untersuchung mehr relevant sind. Sie können eine Suchabfrage die folgenden Parameter angeben:

- **Schlüsselwörter:** Sie können angeben, Schlüsselwörter und Ausdrücke zum Inhalt der Nachricht zu suchen. Sie können auch die logischen Operatoren **AND**, **OR** und **nicht** verwenden. Exchange Server unterstützt darüber hinaus auch **NEAR**-Operator, ermöglicht Ihnen die Suche nach einem Wort oder Ausdruck, der in einer anderen Wort oder Ausdruck in der Nähe ist.

Wenn Sie nach einer genauen Übereinstimmung eines Ausdrucks, der mehrere Wörter enthält, suchen möchten, müssen Sie den Ausdruck in Anführungszeichen setzen. Wenn Sie z. B. nach der Zeichenfolge "Planung und Wettbewerb" suchen, werden Nachrichten mit einer exakten Übereinstimmung für diese Zeichenfolge zurückgegeben. Wenn Sie hingegen **Planung AND Wettbewerb** angeben, werden Nachrichten zurückgegeben, die die Wörter **Planung** und **Wettbewerb** an einer beliebigen Position innerhalb der Nachricht enthalten.

Exchange Server unterstützt außerdem die Syntax der Keyword Query Language (KQL) für Compliance-eDiscovery-Suchen.

#### NOTE

Reguläre Ausdrücke werden in Compliance-eDiscovery-Suchen nicht unterstützt.

Logische Operatoren wie **AND** und **OR** müssen in Großbuchstaben angegeben werden, damit diese nicht als Suchzeichenfolgen, sondern als Operatoren behandelt werden. Zum Vermeiden von Fehlern oder Fehlinterpretationen sollten Sie bei jeder Suche mit mehreren logischen Operatoren eindeutige Klammern verwenden. Wenn Sie z. B. nach Nachrichten suchen, die entweder "WortA" oder "WortB" UND "WortC" oder "WortD" enthalten, verwenden Sie die folgende Syntax: **(WortA OR WortB) AND (WortC OR WortD)**.

- **Anfangs- und Enddatum:** standardmäßig nicht In-Place eDiscovery Suchvorgänge durch einen Datumsbereich beschränkt. Um während einer bestimmten Datumsbereich gesendeten Nachrichten zu suchen, können Sie die Suche eingrenzen, durch die Anfangs- und Enddatum angeben. Wenn Sie ein Enddatum angeben, werden die Suche die aktuellen Ergebnisse zurückgegeben, jedes Mal, wenn Sie ihn neu starten.
- **Absender und Empfänger:** um die Suche einzuschränken, können Sie angeben, der Absender oder Empfänger Nachrichten. Sie können e-Mail-Adressen verwenden, Anzeigen von Namen oder den Namen der Domäne ein, suchen Sie nach Objekten, die an oder von jeder Person in der Domäne gesendet. Beispielsweise e-Mail gesendeten oder gesendet an alle bei Contoso, Ltd., Suchen in der **von \*\*@contoso.com\*\*** angeben oder den **an / cc** Feld in der Exchange-Verwaltungskonsole. Sie können auch die Parameter *Absender* oder *Empfänger* in Exchange Online PowerShell **\*\*@contoso.com\*\*** angeben.
- **Nachrichtentypen:** Standardmäßig werden alle Nachrichtentypen durchsucht. Sie können die Suche einschränken, indem Sie bestimmte Nachrichtentypen wie e-Mails, Kontakte, Dokumente, Journal, Besprechungen, Notizen und Lync-Inhalt auswählen.

Der folgende Screenshot zeigt ein Beispiel für eine Suchabfrage in der Exchange-Verwaltungskonsole.

The screenshot shows the 'Suchabfrage' (Search Query) section of the Exchange Admin Center. It highlights several search parameters with callout boxes explaining their function:

- Suchmethode:** Shows 'Anhand von Kriterien filtern' selected, with a callout box explaining: 'Auswählen, um Stichwörter, Datumsbereich, Empfänger und Nachrichtentypen anzugeben' (Select to choose keywords, date range, recipient and message type).
- Stichwörter:** Shows '(verkaufen ODER kaufen) UND (Aktien ODER Anteile)' entered, with a callout box explaining: 'Nach Stichwörtern oder Ausdrücken suchen und logische Operatoren wie AND, OR, NEAR und NOT verwenden' (Search for keywords or expressions and use logical operators like AND, OR, NEAR and NOT).
- Datumsbereich:** Shows 'Startdatum angeben' checked with '2013 Januar 1' and 'Enddatum angeben' checked with '2013 Dezember 31', both with callout boxes explaining: 'Nach Nachrichten in einem Datumsbereich suchen' (Search for messages in a date range).
- Von:** Shows 'john@woodgrovebank.com' and 'estherv@contoso.com' with 'Benutzer hinzufügen...' buttons, with a callout box explaining: 'Nach Nachrichten suchen, die von bestimmten Benutzern gesendet oder empfangen wurden; mit OR-Operator verbunden' (Search for messages sent or received by specific users; connected with an OR operator).
- Zu durchsuchende Nachrichtentypen:** Shows 'Alle Nachrichtentypen' selected, with a callout box explaining: 'Alle Nachrichtentypen durchsuchen oder bestimmte Typen auswählen' (Search all message types or select specific types).

Bei der Verwendung von Compliance-eDiscovery-Suchen müssen Sie außerdem Folgendes beachten:

- **Anlagen:** Compliance-eDiscovery durchsucht Anlagen vom Exchange-Suche unterstützt. Weitere Informationen hierzu finden Sie unter [Default Filter für die Exchange-Suche](#). In lokalen Bereitstellungen können Sie Unterstützung für zusätzliche Dateitypen hinzufügen, durch die Installation Suchfilter (auch als iFilter bezeichnet) für den Dateityp auf Postfachservern.

- **Nicht durchsuchbare Elemente:** nicht durchsuchbare Elementen werden Postfachelemente, die von der Exchange-Suche indiziert werden können. Gründe für die sie nicht indiziert werden enthalten den Mangel an einen installierten Suchfilter für eine angefügte Datei, einen Fehler Filter und verschlüsselte Nachrichten. Für eine erfolgreiche eDiscovery-Suche möglicherweise erforderlich, damit solche Elemente zur Überprüfung Ihrer Organisation. Beim Kopieren von Suchergebnissen in ein discoverypostfach oder Exportieren in eine PST-Datei können Sie nicht durchsuchbare Elemente einschließen. Weitere Informationen finden Sie unter [nicht durchsuchbare Elemente in Exchange eDiscovery](#).
- **Verschlüsselte Elemente:** Da Nachrichten, die mit S/MIME verschlüsselt werden nicht von der Exchange-Suche indiziert wurde, nicht In-Place eDiscovery diese Nachrichten suchen. Wenn Sie die Option zum Einschließen von nicht durchsuchbaren Elementen in den Suchergebnissen auswählen, werden diese verschlüsselte S/MIME-Nachrichten in das discoverypostfach kopiert.
- **IRM-geschützte Elemente:** Nachrichten mithilfe von Information Rights Management (IRM) geschützt werden von Exchange-Suche indiziert werden und daher in den Suchergebnissen enthalten, wenn sie Abfrageparametern übereinstimmen. Nachrichten müssen mithilfe eines Active Directory-Rechteverwaltungsdienste (AD RMS)-Clusters in derselben Active Directory-Gesamtstruktur wie der Postfachserver geschützt werden. Weitere Informationen finden Sie unter [Information Rights Management](#).

#### **IMPORTANT**

Wenn Exchange-Suche indiziert eine IRM-geschützten Nachricht aufgrund eines Fehlers Entschlüsselung fehlschlägt oder IRM deaktiviert ist, ist nicht die geschützte Nachricht zur Liste der fehlerhaften Elemente hinzugefügt. Wenn Sie die Option zum Einschließen von nicht durchsuchbaren Elementen in den Suchergebnissen auswählen, können die Ergebnisse nicht IRM-geschützten Nachrichten enthalten, die nicht entschlüsselt werden konnten. >> IRM-geschützte Nachrichten in einer Suche aufnehmen möchten, können Sie eine neue Suche zum Einschließen von Nachrichten mit Anlagen .rmsg erstellen. Sie können die Abfragezeichenfolge `attachment:rmsg` alle IRM-geschützten Nachrichten in den angegebenen Postfächern, Suche, ob erfolgreich oder nicht indiziert. Dies kann einige Duplikierung von Suchergebnissen in Szenarios führen, in dem eine Suche Nachrichten zurückgibt, die die Suchkriterien erfüllt, einschließlich der IRM-geschützten Nachrichten, die erfolgreich indiziert wurden. Die Suche zurück nicht IRM-geschützte Nachrichten, die nicht indiziert werden konnten. >> Einer zweiten Suche für alle IRM-geschützte Nachrichten enthält außerdem die IRM-geschützten Nachrichten, die erfolgreich indiziert und in der ersten Suche zurückgegeben wurden. Darüber hinaus können die IRM-geschützte Nachrichten von der zweiten Suche zurückgegebenen die Suchkriterien wie Schlüsselwörter für die erste Suche nicht überein.

- **Deduplizierung:** Wenn Sie Suchergebnisse in ein discoverypostfach kopieren, können Sie Deduplizierung der Suchergebnisse, die nur eine Instanz einer eindeutigen Nachricht in das discoverypostfach kopieren. Deduplizierung bietet folgende Vorteile:

- Niedrigere Speicheranforderungen und geringere Größe des Discoverypostfachs aufgrund der verringerten Anzahl von kopierten Nachrichten.
- Geringere Arbeitslast für Discoverymanager, Rechtsberater und andere Personen, die die Ergebnisse der Suche durchsehen.
- Geringere eDiscovery-Kosten, abhängig von der Anzahl von doppelten Elementen, die aus den Suchergebnissen ausgeschlossen werden.

## Schätzung, Vorschau und Kopieren von Suchergebnissen

Nach Abschluss einer Compliance-eDiscovery-Suche können Sie eine Schätzung der Suchergebnisse im Detailbereich der Exchange-Verwaltungskonsole anzeigen. Die Schätzwerte umfassen die Anzahl von zurückgegebenen Elementen und die Gesamtgröße dieser Elemente. Sie können auch eine

Schlüsselwortstatistik anzeigen, die Details zur Anzahl von Elementen angibt, die für jedes Schlüsselwort in der Suchabfrage zurückgegeben wurden. Diese Informationen sind nützlich, um die Effektivität der Abfrage zu ermitteln. Wenn die Abfrage zu allgemein ist, wird möglicherweise ein zu großer Datensatz angezeigt, für dessen Durchsicht mehr Ressourcen benötigt und höhere eDiscovery-Kosten erzeugt werden. Wenn die Suche zu eingeschränkt ist, werden möglicherweise nur sehr wenige oder gar keine Datensätze angezeigt. Sie können die Schätzwerte und die Schlüsselwortstatistik dazu verwenden, die Abfrage gemäß Ihren Anforderungen zu optimieren.

**NOTE**

In Exchange enthalten Server und Exchange Online schlüsselwortstatistiken außerdem Statistiken für nicht-Schlüsselwort Eigenschaften wie Datumsangaben, Nachrichtentypen und Absender/Empfänger in einer Suchabfrage.

Sie können auch eine Vorschau der Suchergebnisse anzeigen, um sicherzustellen, dass die zurückgegebenen Nachrichten die Inhalte umfassen, nach denen Sie suchen. Basierend auf der Vorschau können Sie die Abfrage bei Bedarf optimieren. Die eDiscovery-Suchvorschau zeigt die Anzahl von Nachrichten, die vom jedem durchsuchten Postfach zurückgegeben wurden, und gibt die Gesamtzahl an Nachrichten an, die von der Suche zurückgegeben wurden. Die Vorschau wird schnell generiert und erfordert nicht, dass Nachrichten in ein Discoverypostfach kopiert werden.

Wenn Sie mit der Menge und Qualität der Suchergebnisse zufrieden sind, können Sie sie in ein Discoverypostfach kopieren. Beim Kopieren von Nachrichten haben Sie folgende Möglichkeiten:

- **Nicht durchsuchbare Elemente einschließen:** Details zu den Arten von nicht durchsuchbaren, als Elemente finden Sie unter der eDiscovery Aspekte im vorherigen Abschnitt zu suchen.
- **Deduplizierung aktivieren:** Deduplizierung verringert, einschließlich nur eine einzelne Instanz eines eindeutigen Datensatzes aus, wenn mehrere Instanzen in einem oder mehreren der durchsuchten Postfächern gefunden werden das Dataset.
- **Vollständige Protokollierung aktivieren:** nur grundlegende Protokollierung ist standardmäßig aktiviert, beim Kopieren von Elementen. Sie können Informationen über alle Datensätze, die von der Suche zurückgegebenen einfügen vollständige Protokollierung aktivieren.
- **Senden Sie mir Informationen nach Abschluss die Kopie:** eine Compliance-eDiscovery-Suche kann potenziell eine große Anzahl von Datensätzen zurück. Die Fehlermeldungen in ein discoverypostfach kopieren kann eine lange dauern. Verwenden Sie diese Option, um eine e-Mail-Benachrichtigung zu erhalten, wenn der Kopiervorgang abgeschlossen ist. Einfacher Zugriff mit Outlook Web App enthält die Benachrichtigung einen Link zu dem Speicherort in ein discoverypostfach, in dem die Nachrichten kopiert werden.

Weitere Informationen finden Sie unter [eDiscovery-Suchergebnisse in ein Discoverypostfach kopieren](#).

## Exportieren von Suchergebnissen in eine PST-Datei

Nachdem die Suchergebnisse in ein Discoverypostfach kopiert wurden, können Sie sie in eine PST-Datei exportieren.

Nach dem Export der Suchergebnisse in eine PST-Datei können Sie oder andere Benutzer sie in Outlook öffnen, um die in den Suchergebnissen zurückgegebenen Nachrichten zu lesen oder zu drucken. Weitere Informationen finden Sie unter [Exportieren von eDiscovery-Suchergebnissen in eine PST-Datei](#).

## Unterschiedliche Suchergebnisse

Da die Compliance-eDiscovery Live-Daten durchsucht, ist es möglich, dass zwei Suchläufe derselben Inhaltsquellen mit derselben Suchabfrage unterschiedliche Ergebnisse zurückgeben. Die geschätzten Suchergebnisse können ebenfalls von den tatsächlichen Suchergebnissen abweichen, die in ein Discoverypostfach kopiert werden. Das passiert auch, wenn dieselbe Suche innerhalb kurzer Zeit wiederholt wird. Es gibt verschiedene Faktoren, die sich auf die Konsistenz der Suchergebnisse auswirken:

- Die kontinuierliche Indizierung eingehender E-Mails, da die Exchange-Suche ständig die Postfachdatenbanken und die Transportpipelines Ihrer Organisation durchforstet und indiziert.
- Löschen von E-Mails durch Benutzer oder automatisierte Prozesse.
- Massenimport von großen Mengen an E-Mails, deren Indizierung Zeit erfordert.

Falls Sie unterschiedliche Ergebnisse für dieselbe Suche erhalten, erwägen Sie die Aufbewahrung von Postfächern, um den Inhalt beizubehalten, führen Sie die Suche außerhalb der Spitzenzeiten durch oder lassen Sie genügend Zeit nach dem Importieren großer Mengen an E-Mails.

## Protokollierung für Compliance-eDiscovery-Suchen

Für Compliance-eDiscovery-Suchen stehen zwei Arten von Protokollierung zur Verfügung:

- **Grundlegende Protokollierung:** grundlegende Protokollierung ist standardmäßig für alle Compliance-eDiscovery-suchen aktiviert. Es enthält Informationen über die Suche und, wer es durchgeführt. Informationen zur grundlegenden Protokollierung erfassten Informationen im Textkörper der e-Mail-Nachricht an das Postfach, in die Suchergebnissen gespeichert werden, gesendet wird angezeigt. Die Nachricht befindet sich im Ordner erstellt, um die Suchergebnisse zu speichern.
- **Vollständige Protokollierung:** vollständige Protokollierung enthält Informationen zu sämtlichen Nachrichten, die von der Suche zurückgegebenen. Diese Informationen werden in einer durch Trennzeichen getrennten Werten (CSV)-Datei, die an die e-Mail-Nachricht, die die grundlegende Protokollierungsinformationen enthält bereitgestellt. Der Name der Suche wird für den Namen der CSV-Datei verwendet. Diese Informationen können für die Einhaltung von Bestimmungen oder zur Archivierung erforderlich sein. Um die vollständige Protokollierung aktivieren möchten, müssen Sie die Option **vollständige Protokollierung aktivieren** auswählen, beim Kopieren von Suchergebnissen in ein discoverypostfach in der Exchange-Verwaltungskonsole. Wenn Sie Exchange Online PowerShell verwenden, geben Sie die vollständige Protokollierungsoption mit dem Parameter *LogLevel*.

#### NOTE

Wenn Exchange Online PowerShell zum Erstellen oder Ändern einer Compliance-eDiscovery-Suche, können Sie auch die Protokollierung deaktivieren.

Das Search-Protokoll enthält, wenn die Suchergebnisse in ein discoverypostfach, Protokolle Cmdlets auch von der Exchange-Verwaltungskonsole verwendet, Exchange oder Exchange Online PowerShell zu erstellen, kopieren außer ändern oder Entfernen von Compliance-eDiscovery-suchen. Diese Informationen werden in die Administrator-Überwachungsprotokolleinträge protokolliert. Weitere Informationen hierzu finden Sie unter [Administrator Audit Logging](#).

## Compliance-eDiscovery und Compliance-Archiv

Im Rahmen von eDiscovery-Anfragen müssen Sie möglicherweise Inhalt von Postfächern zu erhalten, bis ein Rechtsprozesses oder Untersuchung freigegeben wird. Nachrichten gelöscht oder geändert, indem die Postfachbenutzer oder Prozesse auch beibehalten werden müssen. In Exchange Server erfolgt dies mithilfe der In-Place Hold. Weitere Informationen hierzu finden Sie unter [Compliance-Archiv und Aufbewahrung für eventuelle Rechtsstreitigkeiten](#).

In Exchange Server, können Sie den Assistenten zum **Compliance - eDiscovery, Compliance - Archive** zum Suchen von Elementen und Erhaltung für, solange sie für eDiscovery erforderlich sind oder zu anderen Anforderungen gerecht. Wenn Sie die gleiche Suche für Compliance-eDiscovery und Compliance-Archiv verwenden, beachten Sie sollten Folgendes:

- Die Option zum Durchsuchen aller Postfächer kann nicht verwendet werden. Sie müssen die gewünschten Postfächer oder Verteilergruppen auswählen.
- Sie können eine Compliance-eDiscovery-Suche nicht entfernen, wenn die Suche auch für ein Compliance-Archiv verwendet wird. Sie müssen zuerst die Compliance-Archiv-Option in einer Suche deaktivieren und die Suche dann entfernen.

## Aufbewahrung von Postfächern zu Compliance-eDiscovery-Zwecken

Wenn ein Mitarbeiter eine Organisation verlässt, wird das Mitarbeiterpostfach in der Regel deaktiviert oder entfernt. Wenn Sie ein Postfach deaktivieren, wird es vom Benutzerkonto getrennt, verbleibt jedoch für einen bestimmten Zeitraum (standardmäßig 30 Tage) weiterhin in der Postfachdatenbank. Der Assistent für verwaltete Ordner verarbeitet keine getrennten Postfächer, und Aufbewahrungsrichtlinien werden in diesem Zeitraum nicht angewendet. Sie können die Inhalte eines getrennten Postfachs nicht durchsuchen. Bei Ablauf des für die Postfachdatenbank konfigurierten Aufbewahrungszeitraums für gelöschte Postfächer wird das Postfach aus der Postfachdatenbank entfernt.

#### IMPORTANT

In Exchange Online kann die Compliance-eDiscovery-Funktion Inhalte in inaktiven Postfächern durchsuchen. Inaktive Postfächer sind Postfächer, die in einem Compliance-Archiv platziert oder einem Beweissicherungsverfahren unterliegen und anschließend entfernt werden. Inaktive Postfächer werden so lange beibehalten, bis sie im Archiv abgelegt werden. Nachdem ein inaktives Postfach aus dem Compliance-Archiv entfernt oder das Beweissicherungsverfahren aufgehoben wurde, wird es endgültig gelöscht. Weitere Informationen finden Sie unter [Manage Inactive Mailboxes in Exchange Online](#).

Wenn es in lokalen Bereitstellungen in Ihrer Organisation erforderlich ist, Aufbewahrungseinstellungen auf Nachrichten von Mitarbeitern anzuwenden, die nicht länger in der Organisation tätig sind, oder wenn Sie ein Postfach eines ehemaligen Mitarbeiters für eine fortlaufende oder zukünftige eDiscovery-Suche beibehalten müssen, dürfen Sie das Postfach weder deaktivieren noch entfernen. Sie können die folgenden Schritte

ausführen, um sicherzustellen, dass kein Zugriff auf das Postfach möglich ist und keine neuen Nachrichten an das Postfach übermittelt werden.

1. Deaktivieren Sie das Active Directory-Benutzerkonto mit **Active Directory-Benutzer und -Computer** oder anderen Active Directory oder Konto Bereitstellungstools oder Skripts. Dies verhindert, dass Postfach Anmeldung mit dem Benutzerkonto zugeordnet.

#### IMPORTANT

Benutzer mit Vollzugriff Postfach werden weiterhin auf das Postfach zugreifen. Um den Zugriff durch andere zu verhindern, müssen Sie die Berechtigung "Vollzugriff" aus dem Postfach entfernt. Informationen zum Postfach Vollzugriffsberechtigungen für ein Postfach zu entfernen finden Sie unter [Verwalten von Berechtigungen für Empfänger](#).

2. Festlegen der Nachrichtengröße für Nachrichten, die von gesendet oder beispielsweise von den Postfachbenutzer auf einen sehr niedrigen Wert 1 KB empfangen werden können. Verhindert die Zustellung der neuen e-Mail-Nachrichten in und aus dem Postfach. Weitere Informationen hierzu finden Sie unter [Konfigurieren der Nachrichtengröße für ein Postfach](#).
3. Konfigurieren Sie Übermittlungseinschränkungen für das Postfach, sodass niemand Nachrichten an das Postfach senden kann. Weitere Informationen finden Sie unter [Konfigurieren von Nachrichtenübermittlungseinschränkungen für ein Postfach](#).

#### IMPORTANT

Sie müssen die oben genannten Schritte und weitere Prozesse zur Kontoverwaltung ausführen, die in Ihrer Organisation erforderlich sind, jedoch ohne das Postfach zu deaktivieren oder zu entfernen oder das zugeordnete Benutzerkonto zu entfernen.

Wenn Sie die Postfachaufbewahrung zur Verwaltung der Nachrichtenaufbewahrung oder für die Compliance-eDiscovery-Suche implementieren möchten, müssen Sie die Mitarbeiterfluktuation berücksichtigen. Die langfristige Aufbewahrung von Postfächern ehemaliger Mitarbeiter belegt zusätzlichen Speicherplatz auf den Postfachservern und vergrößert die Active Directory-Datenbank, da das zugeordnete Benutzerkonto für denselben Zeitraum beibehalten werden muss. Zusätzlich kann es erforderlich sein, die Prozesse für Kontobereitstellung und -verwaltung in Ihrer Organisation zu ändern.

## Compliance-eDiscovery-Begrenzungen und Einschränkungsrichtlinien

In Exchange Server und Exchange Online werden die Ressourcen, die In-Place eDiscovery belegen kann über einschränkungsrichtlinien gesteuert.

Die Standardeinschränkungsrichtlinie enthält folgende Parameter.

PARAMETER	BESCHREIBUNG	STANDARDWERT
DiscoveryMaxConcurrency	Die maximale Anzahl der Compliance-eDiscovery-Suchen, die in Ihrer Organisation gleichzeitig ausgeführt werden können	2 <b>Hinweis:</b> Wenn eine eDiscovery-Suche gestartet wird, während zwei vorherigen Suchvorgänge weiterhin ausgeführt werden, wird die dritte Suche nicht in eine Warteschlange und stattdessen fehl. Sie müssen warten, bis eine der vorherigen Suchvorgänge beendet wird, bevor Sie erfolgreich eine neue Suche gestartet werden können.

PARAMETER	BESCHREIBUNG	STANDARDWERT
DiscoveryMaxMailboxes	Die maximale Anzahl von Postfächern, die in einer einzelnen Compliance-eDiscovery-Suche durchsucht werden können.	Exchange Online: 10,000 <sup>1</sup> Exchange Server: 5.000
DiscoveryMaxStatsSearchMailboxes	Die maximale Anzahl von Postfächern, die in einer einzelnen Compliance-eDiscovery-Suche durchsucht werden können, die die Anzeige von Schlüsselwortstatistiken erlaubt.	100 <b>Hinweis:</b> Nachdem Sie eine Schätzung der eDiscovery-Suche ausgeführt haben, können Sie Schlüsselwortstatistiken anzeigen. Diese Statistiken zeigen Details über die Anzahl der Elemente, die für jedes Schlüsselwort, das in der Suchabfrage zurückgegeben. Wenn mehr als 100 Quellpostfächer in der Suche enthalten sind, wird ein Fehler zurückgegeben, wenn Sie versuchen, Schlüsselwortstatistiken anzuzeigen.
DiscoveryMaxKeywords	Die maximale Anzahl von Schlüsselwörtern, die in einer einzelnen Compliance-eDiscovery-Suche angegeben werden können.	500
DiscoveryMaxSearchResultsPageSize	Die maximale Anzahl von Elementen, die auf einer einzelnen Vorschauseite der Compliance-eDiscovery-Suchergebnisse angezeigt werden.	200
DiscoverySearchTimeoutPeriod	Die Zeitdauer in Minuten, während der eine Compliance-eDiscovery-Suche ausgeführt wird, bevor eine Zeitüberschreitung auftritt.	10 Minuten

#### NOTE

<sup>1</sup> Wenn Sie eine eDiscovery-Suche über das eDiscovery Center in SharePoint Online in einer Office 365-Organisation starten, können Sie maximal 1500 Postfächer in einem einzelnen Suchvorgang durchsuchen.

In Exchange können Sie Server ändern, die Standardwerte für diese Parameter individuell an Ihre Anforderungen oder erstellen zusätzliche einschränkungsrichtlinien und Benutzer mit Berechtigung für delegierte Discoveryverwaltung zuweisen. Die Standardwerte für diese Einschränkung Parameter können nicht geändert werden, in Exchange Online.

## Dokumentation zu Compliance-eDiscovery

Die folgende Tabelle enthält Links zu Themen, in denen Sie weitere Informationen zu Compliance-eDiscovery und dessen Verwaltung finden.

THEMA	BESCHREIBUNG

THEMA	BESCHREIBUNG
<a href="#">Zuweisen von eDiscovery-Berechtigungen in Exchange</a>	Erfahren Sie, wie Sie einem Benutzer in der Exchange-Verwaltungskonsole Zugriff auf Compliance-eDiscovery zum Durchsuchen von Exchange-Postfächern gewähren. Wenn Sie einen Benutzer zur Rollengruppe "Discoveryverwaltung" hinzufügen, kann dieser auch das eDiscovery Center in SharePoint 2013 und SharePoint Online verwenden, um Exchange-Postfächer zu durchsuchen.
<a href="#">Erstellen eines Discoverypostfachs</a>	Erfahren Sie, wie Exchange Online PowerShell verwenden, um ein discoverypostfach erstellen und Zugriffsberechtigungen zuweisen.
<a href="#">Erstellen einer Compliance-eDiscovery-Suche</a>	Erfahren Sie, wie Sie eine Compliance-eDiscovery-Suche erstellen und wie Sie eDiscovery-Suchergebnisse schätzen und eine Vorschau davon anzeigen.
<a href="#">Nachrichteneigenschaften und Suchoperatoren für Compliance-eDiscovery</a>	Erfahren Sie, welche E-Mail-Nachrichteneigenschaften mithilfe der Compliance-eDiscovery-Funktion durchsucht werden können. Dieses Thema bietet Syntaxbeispiele für jede Eigenschaft, Informationen zu Suchoperatoren wie <b>AND</b> und <b>OR</b> sowie zu anderen Suchabfragemethoden wie z. B. Verwenden doppelter Anführungszeichen (" ") und Präfixplatzhaltern.
<a href="#">Search limits for In-Place eDiscovery in Exchange Online</a>	Erfahren Sie über die Beschränkungen für Compliance-eDiscovery in Exchange Online, mit denen die Integrität und Qualität von eDiscovery-Diensten für Office 365-Organisationen sichergestellt werden.
<a href="#">Start or Stop an In-Place eDiscovery Search</a>	Erfahren Sie, wie Sie eDiscovery-Suchen starten, beenden und neu starten.
<a href="#">Modify an In-Place eDiscovery Search</a>	Erfahren Sie, wie Sie eine vorhandene eDiscovery-Suche ändern.
<a href="#">Kopieren Sie eDiscovery-Suchergebnisse in ein Discoverypostfach.</a>	Erfahren Sie, wie Sie die Ergebnisse einer eDiscovery-Suche in ein Discoverypostfach kopieren.
<a href="#">Exportieren von eDiscovery-Suchergebnissen in eine PST-Datei</a>	Erfahren Sie, wie Sie die Ergebnisse einer eDiscovery-Suche in eine PST-Datei exportieren.
<a href="#">Erstellen eines benutzerdefinierten Verwaltungsbereichs für die Compliance-eDiscovery-Suche</a>	Erfahren Sie, wie Sie mit benutzerdefinierten Verwaltungsbereichen die Anzahl der Postfächer einschränken können, die ein Discovery-Manager durchsuchen kann.
<a href="#">Remove an In-Place eDiscovery Search</a>	Erfahren Sie, wie Sie eine eDiscovery-Suche löschen.
<a href="#">Suchen und Löschen von Nachrichten</a>	Erfahren Sie, wie Sie mit dem Cmdlet <b>Search-Mailbox</b> E-Mail-Nachrichten suchen und löschen können.
<a href="#">Verkleinern eines Discoverypostfachs in Exchange</a>	Verwenden Sie dieses Verfahren, um ein Discoverypostfach, das größer als 50 GB ist, zu verkleinern.

THEMA	BESCHREIBUNG
<a href="#">Löschen und Neuerstellen des Standarddiscoverypostfachs in Exchange</a>	Erfahren Sie, wie Sie ein Standarddiscoverypostfach löschen, es neu erstellen und ihm dann erneut Berechtigungen zuweisen können. Verwenden Sie dieses Verfahren, wenn das Postfach die Größenbeschränkung von 50 GB überschritten hat und Sie die Suchergebnisse nicht benötigen.
<a href="#">Re-Create the Discovery System Mailbox</a>	Hier erfahren Sie, wie das discoverypostfach System neu erstellt. Diese Aufgabe wird nur für Exchange Server-Organisationen gelten.
<a href="#">Using Oauth Authentication to Support eDiscovery in an Exchange Hybrid Deployment</a>	Erfahren Sie mehr über die eDiscovery-Szenarien in einer hybriden Exchange-Bereitstellung, die es erforderlich machen, dass Sie die OAuth-Authentifizierung konfigurieren.
<a href="#">Konfigurieren von Exchange für SharePoint eDiscovery Center</a>	Erfahren Sie, wie Exchange Server konfigurieren, sodass Sie das eDiscovery Center in SharePoint 2013 zum Suchen von Exchange-Postfächern verwenden können.
<a href="#">Unsearchable Items in Exchange eDiscovery</a>	Erfahren Sie mehr über Postfachelemente, die nicht von der Exchange-Suche indiziert werden und in eDiscovery-Suchergebnissen als nicht durchsuchbare Elemente zurückgegeben werden.

Weitere Informationen zu eDiscovery in Office 365, Exchange Server, SharePoint 2013 und Lync 2013 finden Sie unter [häufig gestellte Fragen zu eDiscovery](#).

# Zuweisen von eDiscovery-Berechtigungen in Exchange

18.12.2018 • 4 minutes to read

Wenn die Benutzer Microsoft Exchange Server In-Place eDiscovery verwenden können sollen, müssen Sie zuerst autorisieren, indem die Rollengruppe "Discoveryverwaltung" hinzugefügt. Mitglieder der Rollengruppe "Discoveryverwaltung" haben Postfach Vollzugriffsberechtigungen für das discoverypostfach, das vom Exchange-Setup erstellt wird.

#### Caution

Mitglieder der Rollengruppe "Discoveryverwaltung" können vertrauliche Nachrichteninhalt zugreifen. Insbesondere können diese Member [In-Place eDiscovery](#) Durchsuchen aller Postfächer in Ihrer Exchange-Organisation, die Preview-Nachrichten (und anderen Postfachelementen), in ein discoverypostfach kopieren und die kopierten Nachrichten in eine PST-Datei exportieren. Diese Berechtigung ist in den meisten Unternehmen Legal, Compliance oder Personalabteilung gewährt. >

Weitere Informationen zur Rollengruppe "Discoveryverwaltung" finden Sie unter [Discovery Management](#). Informationen zur rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) finden Sie unter [Understanding Role Based Access Control](#).

Sie interessieren sich für Szenarien, in denen dieses Verfahren verwendet wird? Siehe die folgenden Themen:

- [Erstellen einer Compliance-eDiscovery-Suche](#)
- [Erstellen oder Entfernen eines Compliance-Archivs](#)

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Rollengruppen" im Thema [Role Management Permissions](#) .
- In der Standardeinstellung nicht der Rollengruppe "Discoveryverwaltung" als Mitglieder enthalten. Administratoren mit der Rolle Organization Management können auch nicht zum Erstellen oder Verwalten von Discovery Suchvorgänge ohne die Rollengruppe "Discoveryverwaltung" hinzugefügt wird.
- In Exchange halten Server, Mitglied der Organization Management Rollengruppe ein [Compliance-Archiv und Aufbewahrung für eventuelle Rechtsstreitigkeiten](#) alle Postfach zu platzieren, um Inhalte auf erstellen kann. Um ein abfragebasiertes Compliance-Archiv zu erstellen, muss der Benutzer ein Mitglied der Rollengruppe "Discoveryverwaltung" sein oder dürfen die Postfachsuche Rolle zugewiesen haben.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## Hinzufügen eines Benutzers zur Rollengruppe Discoveryverwaltung mithilfe des EAC

1. Navigieren Sie zu **Berechtigungen > Administratorrollen**.
2. Klicken Sie in der Listenansicht **Discoveryverwaltung** wählen, und klicken Sie dann auf **Bearbeiten**

3. Klicken Sie in der **Rollengruppe**, klicken Sie unter **Mitgliederauf Hinzufügen**
4. Wählen Sie in **Mitglieder auswählen** mindestens einen Benutzer aus, klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **OK**.
5. Klicken Sie in **Rollengruppe** auf **Speichern**.

## Verwenden von Exchange Online PowerShell zum Hinzufügen eines Benutzers zur der Rollengruppe "Discoveryverwaltung"

In diesem Beispiel wird der Benutzer „Bsuneja“ zur Rollengruppe Discoveryverwaltung hinzugefügt.

```
Add-RoleGroupMember -Identity "Discovery Management" -Member Bsuneja
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Add-RoleGroupMember](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie die Rollengruppe "Discoveryverwaltung" den Benutzer hinzugefügt haben, führen Sie folgende Schritte aus:

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Administratorrollen**.
2. Wählen Sie in der Listenansicht den Eintrag **Discoveryverwaltung** aus.
3. Überprüfen Sie im Detailbereich, ob der Benutzer unter **Mitglieder** aufgeführt wird.

Sie können auch diesen Befehl ausführen, um die Mitglieder der Rollengruppe "Discoveryverwaltung" zu listen.

```
Get-RoleGroupMember -Identity "Discovery Management"
```

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Erstellen einer Compliance-eDiscovery-Suche

18.12.2018 • 17 minutes to read

## NOTE

Wir haben den 1 Juli 2017 Stichtag für das Erstellen von neuer Compliance-eDiscovery-suchen im Exchange Online (in Office 365 und Exchange Online-Plänen) verschoben. Aber später in diesem Jahr oder frühe nächste Jahr, nicht möglich, neue Suchvorgänge in Exchange Online zu erstellen. Zum Erstellen von eDiscovery-Suchen starten Sie [Inhaltssuche](#) in die Office 365-Sicherheit und Compliance Center verwenden. Nachdem wir neue Compliance-eDiscovery-suchen außer Betrieb nehmen, Sie vermutlich noch vorhandene Compliance-eDiscovery-suchen zu ändern, und erstellen neue Compliance-eDiscovery-suchen im Exchange Server und Exchange Hybrid-Bereitstellungen werden weiterhin unterstützt.

Verwenden Sie [Compliance - eDiscovery](#), um über den gesamten Inhalt des Postfachs, einschließlich der gelöschten Objekte und der ursprünglichen Versionen geänderter Objekte für Benutzer, die auf [Compliance-Archiv und Aufbewahrung für eventuelle Rechtsstreitigkeiten](#) platziert suchen.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Compliance-eDiscovery" im Thema [Messaging Policy and Compliance Permissions](#).
- Zum Erstellen von eDiscovery-suchen müssen Sie eine SMTP-Adresse in der Organisation haben, den Sie die Suche in erstellen. Daher müssen Sie in Exchange Online ein lizenzierte Exchange Online (Plan 2) Postfach zum Erstellen von eDiscovery-suchen haben. In einer hybriden Exchange-Organisation benötigen Ihre lokale Exchange-Postfach ein entsprechendes Benutzerkonto von e-Mail in Office 365-Organisation, damit Sie Exchange Online-Postfächern suchen können. Oder, wenn Sie sich mit einem Konto anmelden, die nur in Office 365, wie das Administratorkonto eines Mandanten, vorhanden ist dieses Konto muss zugewiesen werden eine Lizenz Exchange Online (Plan 2).
- Exchange Server-Setup erstellt ein discoverypostfach **Discoverysuchpostfach** zum Kopieren von Suchergebnissen aufgerufen. Die Discoverysuchpostfach ist auch in der Standardeinstellung in Exchange Online erstellt. Sie können zusätzliche discoverypostfächer erstellen. Weitere Informationen hierzu finden Sie unter [Erstellen eines discoverypostfachs](#).
- Beim Erstellen einer Compliance-eDiscovery-Suche wird Nachrichten, die in den Suchergebnissen zurückgegeben werden nicht automatisch in ein discoverypostfach kopiert. Nachdem Sie die Suche erstellt haben, können Sie im Exchange Administrationscenter (EAC) schätzen und eine Vorschau der Suchergebnisse oder in ein discoverypostfach kopieren. Weitere Informationen hierzu finden Sie unter:
  - [Estimate or preview search results](#)(weiter unten in diesem Thema)
  - [Kopieren Sie eDiscovery-Suchergebnisse in ein Discoverypostfach.](#)
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen einer Compliance-eDiscovery-Suche mithilfe der Exchange-Verwaltungskonsole

Wie bereits erklärt, müssen Sie sich für das Erstellen einer eDiscovery-Suche bei einem Benutzerkonto anmelden, das in Ihrer Organisation über eine SMTP-Adresse verfügt.

1. Wechseln Sie zu **Verwaltung der Richtlinientreue > Compliance - eDiscovery und -Archiv**.
2. Klicken Sie auf **neue**
3. Geben Sie auf der Seite **Name und Beschreibung** im **Compliance-eDiscovery und -Archiv**, einen Namen für die Suche ein, fügen Sie eine optionale Beschreibung hinzu, und klicken Sie dann auf **Weiter**.
4. Wählen Sie auf der Seite **Postfächer** Postfächer zu suchen. Sie können in allen Postfächern suchen oder Auswählen bestimmter zu suchen. In Exchange Online können Sie auch die Office 365-Gruppen als eine Inhaltsquelle für die Suche auswählen.

#### IMPORTANT

Sie können die Option **alle Postfächer durchsuchen** um aller Postfächer im Archiv zu platzieren. Um eine In-Place Hold zu erstellen, müssen Sie **Angeben von Postfächern zu suchenauswählen**. Weitere Informationen finden Sie unter [Create or Remove an In-Place Hold](#).

5. Füllen Sie auf der Seite **Suchabfrage** die folgenden Felder aus:

- **Alle Inhalte der Benutzerpostfächer einschließen:** Wählen Sie diese Option, um alle Inhalte in die ausgewählten Postfächer in der Warteschleife platziert. Wenn Sie diese Option auswählen, können nicht Sie zusätzliche Suchkriterien angeben.
- **Filter basierend auf Kriterien:** Wählen Sie diese Option, um Suchkriterien, einschließlich von Schlüsselwörtern, Start- und Enddaten, Absender und Empfänger-Adressen und Nachrichtentypen.

## Neu: In-Situ-eDiscovery und -Speicher

### Suchabfrage

The screenshot shows the search query interface with various search parameters highlighted by pink boxes and arrows:

- Alle Inhalte berücksichtigen** (radio button) leads to a note: "Auswählen, um Stichwörter, Datumsbereich, Empfänger und Nachrichtentypen anzugeben".
- Anhand von Kriterien filtern** (radio button) leads to a note: "Auswählen, um Stichwörter, Datumsbereich, Empfänger und Nachrichtentypen anzugeben".
- Stichwörter:** (verkaufen ODER kaufen) UND (Aktien ODER Anteile) leads to a note: "Nach Stichwörtern oder Ausdrücken suchen und logische Operatoren wie AND, OR, NEAR und NOT verwenden".
- Startdatum angeben:** (checkbox checked) leads to a note: "Nach Nachrichten in einem Datumsbereich suchen".
- Enddatum angeben:** (checkbox checked) leads to a note: "Nach Nachrichten suchen, die von bestimmten Benutzern gesendet oder empfangen wurden; mit OR-Operator verbunden".
- Von:** john@woodgrovebank.com leads to a note: "Nach Nachrichten suchen, die von bestimmten Benutzern gesendet oder empfangen wurden; mit OR-Operator verbunden".
- An/Cc/Bcc:** estherv@contoso.com leads to a note: "Nach Nachrichten suchen, die von bestimmten Benutzern gesendet oder empfangen wurden; mit OR-Operator verbunden".
- Zu durchsuchende Nachrichtentypen:** Alle Nachrichtentypen leads to a note: "Alle Nachrichtentypen durchsuchen oder bestimmte Typen auswählen".
- Nachrichtentypen auswählen...** leads to a note: "Alle Nachrichtentypen durchsuchen oder bestimmte Typen auswählen".

### NOTE

Die Felder **Von:** und **An/Cc/Bcc:** sind durch einen **OR**-Operator in der Suchabfrage verbunden, die beim Ausführen der Suche erstellt wird. Das bedeutet, dass eine Nachricht, die von einem der angegebenen Benutzer gesendet oder empfangen wird (und den anderen Suchkriterien entspricht), in den Suchergebnissen enthalten ist. > Die Datumsangaben werden mit einem **UND**-Operator verbunden.

6. Markieren Sie auf der Seite **Einstellungen für Compliance-Archiv** das Kontrollkästchen **Inhalt, der mit der Suchanfrage übereinstimmt, in ausgewählten Postfächern aufbewahren**, und wählen Sie dann eine der folgenden Optionen aus, um Objekte im Compliance-Archiv zu platzieren:

- **In einer Warteschleife verbleibt:** Wählen Sie diese Option zum Platzieren der zurückgegebenen Elemente in einer aufzubewahren. Elemente in der Warteschleife bleiben, bis Sie das Postfachs aus der Suche entfernen oder entfernen die Suche erhalten.
- **Geben Sie Anzahl der Tage speichern Elemente relativ zu ihrer Empfangsdatum:** mit dieser Option können Sie um Elemente für einen bestimmten Zeitraum zu halten. Beispielsweise können Sie diese Option, wenn Ihre Organisation erfordert, dass alle Nachrichten mindestens sieben Jahre lang aufbewahrt werden. Sie können eine zeitbasierten Compliance-Archiv zusammen mit einer Aufbewahrungsrichtlinie stellen Sie sicher, dass Elemente in sieben Jahren gelöscht werden.

### IMPORTANT

Wenn Postfächer oder Elemente aus rechtlichen Gründen in einem Compliance-Archiv platziert werden, empfiehlt es sich im Allgemeinen, die Elemente dauerhaft beizubehalten oder die Archivierung zu beenden, wenn der Fall oder die Untersuchung beendet ist.

7. Klicken Sie auf **Fertig stellen**, speichern Sie die Suche und um eine Schätzung der Gesamtgröße sowie die Anzahl der Elemente, die zurückgegeben werden, indem die Suche anhand der angegebenen Kriterien zurückzugeben. Schätzungen werden im Detailfenster angezeigt. Klicken Sie auf **Aktualisieren** zum Aktualisieren der Informationen im Detailbereich angezeigt.

[Zurück zum Seitenanfang](#)

# Verwenden von Exchange Online PowerShell zum Erstellen einer Compliance-eDiscovery-Suche

In diesem Beispiel wird die Compliance-eDiscovery-Suche mit dem Namen „Discovery-Caseld012“ nach Objekten mit den Schlüsselwörtern „Contoso“ und „ProjectA“ erstellt, die außerdem die folgenden Kriterien erfüllen:

- Startdatum: 1/1/2009
- Enddatum: 12/31/2011
- Quellpostfach: DG-Finance
- Zielpostfach: Discoverysuchpostfach
- Nachrichtentypen: E-Mail
- Einschließen von nicht durchsuchbaren Elementen in der Suchstatistik
- Protokollstufe: Vollständig

## IMPORTANT

Wenn Sie bei der Ausführung einer Compliance-eDiscovery-Suche zusätzliche Such-Parameter nicht angeben, werden alle Elemente in der angegebenen Quellpostfächer in den Ergebnissen zurückgegeben. Wenn Sie Postfächer suchen nicht angeben, werden alle Postfächer in Ihrer Organisation Exchange oder Exchange Online durchsucht.

```
New-MailboxSearch "Discovery-CaseId012" -StartDate "01/01/2009" -EndDate "12/31/2011" -SourceMailboxes "DG-Finance" -TargetMailbox "Discovery Search Mailbox" -SearchQuery '"Contoso" AND "Project A"' -MessageTypes Email -IncludeUnsearchableItems -LogLevel Full
```

## NOTE

Wenn Sie die Parameter *StartDate* und *EndDate* verwenden, müssen Sie das Datumsformat mm/tt/jjjj verwenden, selbst wenn Ihr PC für ein anderes Datumsformat, wie z. B. tt/mm/jjjj konfiguriert ist. Wenn Sie z. B. nach Nachrichten suchen, die zwischen dem 1. April 2013 und dem 1. Juli 2013 versandt wurden, geben Sie **04/01/2013** und **07/01/2013** als Start- und Enddatum ein.

In diesem Beispiel wird die Compliance-eDiscovery-Suche mit dem Namen „HRCase090116“ erstellt, die nach E-Mail-Nachrichten sucht, die von Alex Darrow und Sara Davis im Jahr 2015 gesendet wurden.

```
New-MailboxSearch "HRCase090116" -StartDate "01/01/2015" -EndDate "12/31/2015" -SourceMailboxes alexd,sarad -SearchQuery 'From:alexd@contoso.com AND To:sarad@contoso.com' -MessageTypes Email -TargetMailbox "Discovery Search Mailbox" -IncludeUnsearchableItems -LogLevel Full
```

Nachdem mit Exchange Online PowerShell eine Compliance-eDiscovery-Suche erstellen, müssen Sie die Suche beginnen mit dem **Start-MailboxSearch** -Cmdlet zum Kopieren von Nachrichten in das discoverypostfach im Parameter *TargetMailbox* angegeben. Weitere Informationen hierzu finden Sie unter [eDiscovery-Suchergebnisse in ein Discoverypostfach kopieren](#).

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-MailboxSearch](#).

[Zurück zum Seitenanfang](#)

# Verwenden des EAC zum Schätzen von Suchergebnissen oder zur Anzeige in einer Vorschau

Nach der Erstellung einer Compliance-eDiscovery-Suche können Sie die Exchange-Verwaltungskonsole verwenden, um eine Schätzung und Vorschau der Suchergebnisse zu erhalten. Wenn Sie eine neue Suche mit dem Cmdlet **New-MailboxSearch** erstellt haben, können Sie Exchange Online PowerShell verwenden, um eine Schätzung der Suchergebnisse zu erhalten, um die Suche zu starten. Sie können Exchange Online PowerShell Vorschau von Nachrichten, die in den Suchergebnissen zurückgegeben.

1. Navigieren Sie zu **Verwaltung der Richtlinientreue > Compliance - eDiscovery und -Archiv**.
2. Wählen Sie in dieser Listenansicht die Compliance-eDiscovery-Suche aus, und führen Sie dann eine der folgenden Aktionen aus:

- Klicken Sie auf **Suche**  > **Schätzung der Suchergebnisse** zurückgegeben wird eine Schätzung der Gesamtgröße und Anzahl der Elemente, die von der Suche zurückgegeben werden, basierend auf der angegebenen Kriterien. Durch Auswählen dieser Option wird die Suche und führt eine Schätzung.

Suche Schätzungen werden im Detailfenster angezeigt. Klicken Sie auf **Aktualisieren**  zum Aktualisieren der Informationen im Detailbereich angezeigt.

- Klicken Sie im Detailbereich auf **Vorschau auf Suchergebnisse anzeigen**, um eine Vorschau auf die Suchergebnisse anzuzeigen, nachdem die Suchabschätzung abgeschlossen ist. Wenn Sie diese Option auswählen, wird das Fenster **Vorschau der eDiscovery-Suche** geöffnet. Alle Nachrichten, die von den durchsuchten Postfächern zurückgegeben wurden, werden angezeigt.

## NOTE

Die Postfächer, die durchsucht wurden, werden im rechten Bereich im Fenster **eDiscovery-Suchvorschau** aufgelistet. Für jedes Postfach werden auch die Anzahl der zurückgegebenen Elemente und die Gesamtgröße der diese Elemente angezeigt. Alle von der Suche zurückgegebenen Elemente werden im rechten Bereich aufgelistet und nach neuesten oder ältesten Datum sortiert werden können. Elemente aus jedem Postfach können nicht im rechten Bereich angezeigt werden, indem Sie auf ein Postfach im linken Bereich. Um die von einem bestimmten Postfach zurückgegebenen Elemente anzuzeigen, können Sie die Suchergebnisse kopieren und anzeigen, die Elemente in das discoverypostfach.

The screenshot shows the Exchange admin center's compliance management section. On the left, there's a navigation menu with links like recipients, permissions, compliance management (which is selected), organization, protection, mail flow, mobile, public folders, and unified messaging. The main area has a search bar with placeholder text: "Search the mailboxes in your organization for email and other message types that contain specific keywords. You can create a new search, or edit and restart an existing search below." Below the search bar is a toolbar with icons for creating a new search, editing, and refresh. A dropdown menu is open over the search bar, showing options: "Estimate search results" (highlighted with a red box) and "Copy search results". To the right of the search bar is a table header with columns: NAME, OLD STATUS, MODIFIED DATE, and CREATED BY. Below the header, a row shows "Search All Mailboxes" with a timestamp "3/19/2014 11:06 AM". The search results table is currently empty. On the far right, there's a sidebar with search details: "Search All Mailboxes", "Hold: None", "Status: Estimate Succeeded", "Run by: Administrator", "Run on: 8/20/2014 5:04 PM", "Size: 36 MB", "Items: 647", and a "Preview search results" link (highlighted with a red box).

[Zurück zum Seitenanfang](#)

## Verwenden von Exchange Online PowerShell, Schätzung der Suchergebnisse

Sie können den *EstimateOnly*-Switch verwenden, um eine Schätzung der Suchergebnisse zu erhalten, ohne die Ergebnisse in ein Discovery-Postfach zu kopieren. Sie müssen mit dem Cmdlet **Start-MailboxSearch** eine Suche vom Typ "Nur schätzen" ausführen. Anschließend können Sie mithilfe des Cmdlets **Get-MailboxSearch** die geschätzten Suchergebnisse abrufen.

Sie würden z. B. die folgenden Befehle ausführen, um eine neue eDiscovery-Suche zu erstellen und anschließend eine Schätzung der Suchergebnisse anzuzeigen:

```
New-MailboxSearch "FY13 Q2 Financial Results" -StartDate "04/01/2013" -EndDate "06/30/2013" -SourceMailboxes "DG-Finance" -SearchQuery '"Financial" AND "Fabrikam"' -EstimateOnly -IncludeKeywordStatistics
```

```
Start-MailboxSearch "FY13 Q2 Financial Results"
```

```
Get-MailboxSearch "FY13 Q2 Financial Results"
```

Um die Informationen der geschätzten Suchergebnisse anzuzeigen können Sie den folgenden Befehl ausführen:

```
Get-MailboxSearch "FY13 Q2 Financial Results" | Format-List  
Name,Status,LastRunBy,LastStartTime,LastEndTime,Sources,SearchQuery,ResultSizeEstimate,ResultNumberEstimate,Errors,KeywordHits
```

[Zurück zum Seitenanfang](#)

## Weitere Informationen zu eDiscovery-Suchen

- Nachdem Sie eine neue eDiscovery-Suche erstellt haben, können Sie die Suchergebnisse in das Discovery-

Postfach kopieren und die Ergebnisse als PST-Datei speichern. Weitere Informationen finden Sie unter:

- [Kopieren Sie eDiscovery-Suchergebnisse in ein Discoverypostfach.](#)
- [Exportieren von eDiscovery-Suchergebnissen in eine PST-Datei](#)
- Wenn Sie eine eDiscovery-Suchergebnisschätzung (mit Schlüsselwörtern in den Suchkriterien) durchgeführt haben, können Sie die Schlüsselwortstatistik anzeigen, indem Sie im Detailbereich für die ausgewählte Suche auf **Schlüsselwortstatistik anzeigen** klicken. Diese Statistik enthält detaillierte Informationen über die Anzahl der Elemente, die für jedes in der Suchanfrage verwendete Schlüsselwort zurückgegeben werden. Wenn allerdings mehr als 100 Quellpostfächer in die Suche einbezogen werden, wird beim Versuch, die Schlüsselwortstatistik anzuzeigen, eine Fehlermeldung zurückgegeben. Wenn Sie die Schlüsselwortstatistik anzeigen möchten, dürfen nicht mehr als 100 Postfächer in die Suche aufgenommen werden.
- Wenn Sie **Get-MailboxSearch** zum Abrufen von Informationen zu einer eDiscovery-Suche in Exchange Online verwenden, müssen Sie angeben des Namens einer Suche auf eine vollständige Liste der Suche Eigenschaften zurückgeben. beispielsweise `Get-MailboxSearch "Contoso Legal Case"`. Wenn Sie das Cmdlet **Get-MailboxSearch** ohne Parameter ausführen, werden nicht die folgenden Eigenschaften zurückgegeben:
  - SourceMailboxes
  - Quellen
  - SearchQuery
  - ResultsLink
  - PreviewResultsLink
  - Fehler

Der Grund dafür ist, dass viele Ressourcen erforderlich sind, um diese Eigenschaften für alle eDiscovery-Suchvorgänge in Ihrer Organisation zurückzugeben.

[Zurück zum Seitenanfang](#)

# Exportieren von eDiscovery-Suchergebnissen in eine PST-Datei

18.12.2018 • 10 minutes to read

Sie können das eDiscovery-Export-Tool in der Exchange-Verwaltungskonsole (EAC), um die Ergebnisse einer Compliance-eDiscovery-Suche in eine Outlook-Datendatei zu exportieren verwenden, die auch eine PST-Datei bezeichnet wird. Administratoren können die Ergebnisse der Suche für andere Personen innerhalb Ihrer Organisation, wie Leiter der Personalabteilung oder Datensatzverwalter, oder entgegengesetzte einholen in rechtlichen Fall verteilen. Nachdem die Suchergebnisse in eine PST-Datei exportiert werden, können Sie oder andere Benutzer öffnen sie in Outlook zu überprüfen oder Drucken von Nachrichten, die in den Suchergebnissen zurückgegeben. PST-Dateien können auch in der Drittanbieter-eDiscovery und reporting-Applikationen geöffnet werden. In diesem Thema zeigt, wie Sie dies als auch eine beliebige möglicherweise Probleme zu beheben.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Die benötigte Zeit ist je nach Anzahl und Größe der exportierten Suchergebnisse unterschiedlich.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter „In-Situ-eDiscovery“ im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#).
- Der Computer, den Sie verwenden, um die Suchergebnisse in eine PST-Datei exportieren muss die folgenden Voraussetzungen erfüllen:
  - 32- oder 64-Bit-Versionen von Windows 7 und höher
  - Microsoft .NET Framework 4.7
  - Einen unterstützten Browser:
    - Internet Explorer 10 und höher
- ODER
  - Mozilla Firefox oder Google Chrome. Wenn Sie eine der folgenden Browser verwenden, installieren Sie die ClickOnceErweiterung. Informationen zur Installation des ClickOnce-Add-Ins finden Sie unter [Mozilla ClickOnce-Add-Ons](#) oder [ClickOnce für Google Chrome](#).
- An das Konto, das Sie exportieren möchten, muss ein aktives Postfach angefügt sein.
- Stellen Sie sicher, dass die Einstellungen für lokales Intranet in Internet Explorer korrekt eingerichtet sind. Stellen Sie sicher, dass [https://\\*.outlook.com](https://*.outlook.com) zur Zone für lokales Intranet hinzugefügt wurde.
- Stellen Sie sicher, dass die folgenden URLs nicht in der Zone der vertrauenswürdigen Websites aufgeführt sind:
  - [https://\\*.outlook.com](https://*.outlook.com)
  - <https://r4.res.outlook.com>
  - [https://\\*.res.outlook.com](https://*.res.outlook.com)
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter

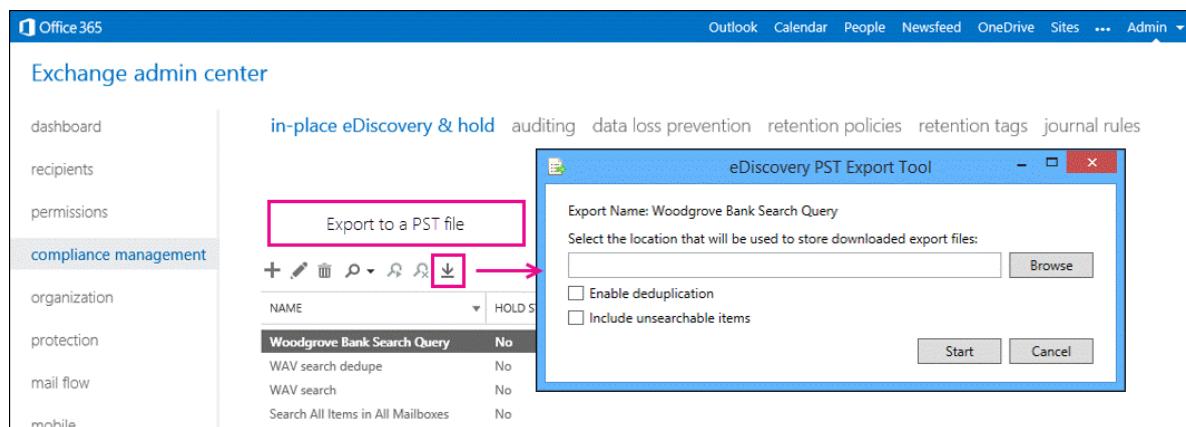
Tastenkombinationen für die Exchange-Verwaltungskonsole.

**TIP**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden des Exchange-Verwaltungskonsole zum Exportieren der In-Situ-eDiscovery-Suchergebnisse in eine PST-Datei

1. Wechseln Sie zu **Verwaltung der Richtlinientreue > Compliance - eDiscovery und -Archiv**.
2. Wählen Sie in der Listenansicht die Compliance-eDiscovery-Suche aus, deren Ergebnisse Sie exportieren möchten, und klicken Sie auf die Option **In eine PST-Datei exportieren**.



3. Gehen Sie im Fenster **eDiscovery-PST-Exporttool** folgendermaßen vor:

- Klicken Sie auf **Durchsuchen**, und geben Sie das Verzeichnis an, in das die PST-Datei heruntergeladen werden soll.
- Klicken Sie auf das Kontrollkästchen **Entfernung von Duplikaten aktivieren**, um doppelte Nachrichten auszuschließen. Es wird nur eine einzelne Instanz einer Nachricht in die PST-Datei aufgenommen.
- Wählen Sie das Kontrollkästchen **Nicht durchsuchbare Elemente einschließen** aus, um Postfachelemente zu berücksichtigen, die nicht durchsucht werden konnten (z. B. Nachrichten mit Anhängen, die Dateitypen enthalten, die von der Exchange-Suche nicht indiziert werden konnten). Nicht durchsuchbare Elemente werden in eine separate PST-Datei exportiert.

**IMPORTANT**

Das Einschließen nicht durchsuchbarer Elemente beim Export von eDiscovery-Suchergebnissen dauert längern, wenn Postfächer viele nicht durchsuchbare Elemente enthalten. Folgen Sie zum Reduzieren der Dauer des Exports von Suchergebnissen und Verhindern großer PST-Exportdateien den folgenden Empfehlungen: > Erstellen Sie mehrere eDiscovery-Suchvorgänge, damit bei jeder Suche weniger Quellpostfächer durchsucht werden müssen. > Wenn Sie sämtliche Postfachinhalte innerhalb eines bestimmten Datumsbereichs (bei Weglassen der Angabe von Schlüsselwörtern in den Suchkriterien) exportieren, werden alle nicht durchsuchbaren Elemente in diesem Datumsbereich automatisch in die Suchergebnisse einbezogen. Aktivieren Sie deshalb nicht das Kontrollkästchen **Nicht durchsuchbare Elemente einschließen**.

4. Klicken Sie auf **Start**, um die Suchergebnisse in eine PST-Datei zu exportieren.

Es wird ein Fenster angezeigt, das Statusinformationen über den Exportvorgang anzeigt.

## Weitere Informationen

- Eine Möglichkeit der Verkleinerung von PST-Exportdateien ist das ausschließliche Exportieren der nicht durchsuchbaren Elemente. Erstellen oder bearbeiten Sie dazu eine Suche, geben Sie ein Startdatum in der Zukunft an, und entfernen Sie alle Schlüsselwörter aus dem Feld **Schlüsselwörter**. Dadurch werden keine Suchergebnisse zurückgegeben. Wenn Sie die Suchergebnisse kopieren oder exportieren und das Kontrollkästchen **Nicht durchsuchbare Elemente einschließen** aktivieren, werden die undurchsuchbaren Elemente in das Discoverypostfach kopiert oder in eine PST-Datei exportiert.
- Falls Sie Deduplizierung aktiviert haben, werden alle Suchergebnisse in eine einzige PST-Datei exportiert. Wenn Sie Deduplizierung nicht aktivieren, wird für jedes durchsuchte Postfach eine separate PST-Datei exportiert. Wie bereits erwähnt, werden nicht durchsuchbare Elemente in eine separate PST-Datei exportiert.
- Zusätzlich zu den PST-Dateien, welche die Suchergebnisse enthalten, werden zwei weitere Datei exportiert:
  - Eine Konfigurationsdatei (TXT-Datei), die Informationen über die PST-Exportanforderung enthält, wie z. B. den Namen der zu exportierenden eDiscovery-Suche, Datum und Zeit des Exports, Aktivierung von Deduplizierung und nicht durchsuchbaren Elementen, die Suchabfrage sowie die durchsuchten Quellpostfächer.
  - Ein Protokoll der Suchergebnisse (CSV-Datei), das einen Eintrag für jede in den Suchergebnissen zurückgegebene Nachricht enthält. Jeder Eintrag identifiziert das Quellpostfach, in dem sich die Nachricht befindet. Falls Sie Deduplizierung aktiviert haben, können Sie damit alle Postfächer identifizieren, die doppelte Nachrichten enthalten.
- Der Name der Suche ist der erste Teil des Dateinamens jeder Datei, die exportiert wird. Außerdem werden Datum und Uhrzeit der Exportanforderung an den Dateinamen jeder PST-Datei und an das Ergebnisprotokoll angehängt.
- Weitere Informationen zu Deduplizierung und nicht durchsuchbaren Elementen finden Sie unter:
  - [Schätzung, Vorschau und Kopieren von Suchergebnissen](#)
  - [Unsearchable Items in Exchange eDiscovery](#)
- Informationen zum Exportieren von eDiscovery-Suchergebnissen aus dem eDiscovery Center in SharePoint oder SharePoint Online finden Sie unter [Exportieren von eDiscovery-Inhalten und Erstellen von Berichten](#).

## Problembehandlung

SYMPTOM	MÖGLICHE URSCHE
Exportieren in eine PST-Datei nicht möglich.	Dem Konto ist kein aktives Konto angefügt. Sie benötigen ein aktives Konto, um die PST-Datei zu exportieren. Ihre Version von Internet Explorer ist nicht mehr aktuell. Versuchen Sie, Internet Explorer auf Version 10 oder höher zu aktualisieren. Oder verwenden Sie einen anderen Browser. Die Suchkriterien, die Sie in die Abfrage <b>Auf Kriterien basierter Filter</b> eingegeben haben, sind falsch. Es wurde beispielsweise ein Benutzername anstelle einer E-Mail-Adresse eingegeben. Weitere Informationen zum Filtern basierend auf Kriterien finden Sie unter <a href="#">Ändern einer Compliance-eDiscovery-Suche</a> .

SYMPTOM	MÖGLICHE URSCHE
Das Exportieren von Suchergebnissen ist einem bestimmten Computer nicht möglich. Der Export funktioniert auf einem anderen Computer wie erwartet.	In der <b>Anmeldeinformationsverwaltung</b> wurden die falschen Windows-Anmeldeinformationen gespeichert. Löschen Sie Ihre Anmeldeinformationen ein, und melden Sie sich erneut an.
Das eDiscovery-PST-Exporttool kann nicht gestartet werden.	Die Einstellungen für die Zone für lokales Intranet wurden in Internet Explorer nicht korrekt eingerichtet. Vergewissern Sie sich, dass *.outlook.com, *.office365.com, *.sharepoint.com und *.onmicrosoft.com den vertrauenswürdigen Websites der Zone für lokales Intranet hinzugefügt wurden. Informationen zum Hinzufügen dieser Websites zur Zone vertrauenswürdiger Sites in Internet Explorer finden Sie unter <a href="#">Sicherheitszonen: Hinzufügen oder Entfernen von Websites</a> .

# Nachrichteneigenschaften und Suchoperatoren für Compliance-eDiscovery

18.12.2018 • 17 minutes to read

In diesem Thema werden die Eigenschaften des Exchange-e-Mail-Nachrichten, können Sie mithilfe von Compliance-eDiscovery Suchen & im Exchange Server und Exchange Online halten. Das Thema beschreibt auch boolesche Suchoperatoren und anderen Techniken der Search-Abfrage, die Sie verwenden können, um eDiscovery-Suchergebnisse verfeinern.

Compliance-eDiscovery verwendet Keyword Query Language (KQL). Weitere Informationen dazu finden Sie unter [Keyword Query Language - Syntaxverweis](#).

## Durchsuchbare Eigenschaften in Exchange

In der folgenden Tabelle sind Eigenschaften von E-Mails aufgelistet, nach denen in einer Compliance-eDiscovery-Suche oder mithilfe von **New-MailboxSearch** oder des Cmdlets **Set-MailboxSearch** gesucht werden kann. Die Tabelle enthält ein Beispiel für die *property:value*-Syntax für jede Eigenschaft und eine Beschreibung der für jedes Beispiel zurückgegebenen Suchergebnisse.

EIGENSCHAFT	BESCHREIBUNG DER EIGENSCHAFT	BEISPIELE	VON DEN BEISPIELEN ZURÜCKGEGBENE SUCHERGEBNISSE
Anhang	Die Namen der an eine E-Mail angefügten Dateien.	Attachment:annualreport.ppt Anhang:Jahresbericht*	Nachrichten, an die eine Datei namens Jahresbericht.ppt angehängt ist. Im zweiten Beispiel werden, wenn Sie das Platzhalterzeichen verwenden, Nachrichten mit dem Wort "Jahresbericht" im Dateinamen eines Anhangs zurückgegeben.
Bcc	Das Feld „BCC“ einer E-Mail-Nachricht. <sup>1</sup>	Bcc:pilarp@contoso.com bcc:pilarp bcc:"Pilar Pinilla"	In allen Beispielen werden Nachrichten mit dem Namen "Pilar Pinilla" im Bcc-Feld zurückgegeben.
Kategorie	Die Kategorien, nach denen gesucht wird. Kategorien können durch Benutzer mithilfe von Outlook oder Outlook Web App definiert werden. Die folgenden Werte sind möglich: blau grün orange violett rot gelb	Kategorie:="Rote Kategorie"	Nachrichten, denen in den Quellpostfächern die rote Kategorie zugewiesen wurde.

EIGENSCHAFT	BESCHREIBUNG DER EIGENSCHAFT	BEISPIELE	VON DEN BEISPIelen ZURÜCKGEgebene Suchergebnisse
Cc	Das Feld „CC“ einer E-Mail-Nachricht. <sup>1</sup>	cc:pilarp@contoso.com cc:”Pilar Pinilla”	In beiden Fällen Nachrichten mit dem Namen “Pilar Pinilla” im CC-Feld.
Von	Der Absender einer E-Mail-Nachricht. <sup>1</sup>	FROM:pilarp@contoso.com FROM:contoso.com	Nachrichten, die vom angegebenen Benutzer oder einer bestimmten Domäne gesendet wurden.
Wichtigkeit	Die Wichtigkeit einer E-Mail-Nachricht, die ein Absender festlegen kann, wenn er eine Nachricht sendet. Standardmäßig werden Nachrichten mit normaler Wichtigkeit gesendet, außer wenn der Absender die Wichtigkeit auf <b>Hoch</b> oder <b>Niedrig</b> setzt.	Wichtigkeit:Hoch Wichtigkeit:Mittel Wichtigkeit:Niedrig	Nachrichten, deren Wichtigkeit auf “Hoch”, “Mittel” bzw. “Niedrig” eingestellt ist.
Art	Der Nachrichtentyp, nach dem gesucht wird. Mögliche Werte: contacts docs email faxes im journals meetings notes posts rssfeeds tasks voicemail	Art:email Art:email OR Art:im OR Art:Voicemail	E-Mails, die den Suchkriterien entsprechen. Im zweiten Beispiel werden E-Mails, Instant Messaging-Konversationen und Sprachnachrichten zurückgegeben, die den Suchkriterien entsprechen.
Teilnehmer	Alle Felder mit Personen in einer E-Mail-Nachricht. Diese Felder sind „Von“, „An“, „CC“ und „BCC“. <sup>1</sup>	participants:garthf@contoso.com participants:contoso.com	Nachrichten, die von oder an garthf@contoso.com gesendet wurden. Im zweiten Beispiel werden alle Nachrichten zurückgegeben, die von oder an einen Benutzer in der Domäne contoso.com gesendet wurden.
Empfangen	Das Datum, an dem eine E-Mail-Nachricht von einem Empfänger empfangen wurde.	received:04/15/2014 empfangene>= 01/01/2014 und empfangenen<= 03/31/2014	Nachrichten, die am 15. April 2014 empfangen wurden. Im zweiten Beispiel werden alle Nachrichten zurückgegeben, die zwischen dem 1. Januar 2014 und dem 31. März 2014 empfangen wurden.

EIGENSCHAFT	BESCHREIBUNG DER EIGENSCHAFT	BEISPIELE	VON DEN BEISPIelen ZURÜCKGEGBENE SUCHERGEBNISSE
Empfänger	Alle Felder mit Empfängern in einer E-Mail-Nachricht. Diese Felder sind „An“, „CC“ und „BCC“. <sup>1</sup>	recipients:garthf@contoso.com Recipients:contoso.com	Nachrichten, die an garthf@contoso.com gesendet wurden. Im zweiten Beispiel werden Nachrichten zurückgegeben, die an einen beliebigen Empfänger in der Domäne contoso.com geschickt wurden.
Gesendet	Das Datum, an dem eine E-Mail vom Absender gesendet wurde.	sent:07/01/2014 gesendet>= 06/01/2014 und gesendet<= 07/01/2014	Nachrichten, die am angegebenen Tag oder im angegebenen Datumsbereich gesendet wurden.
Größe	Die Größe eines Elements in Byte.	Größe>26214400 Größe: 1..1048576	Nachrichten mit mehr als 25 MB. Im zweiten Beispiel werden Nachrichten mit einer Größe von 1 bis 1.048.576 Byte (1 MB) zurückgegeben.
Betreff	Der Text in der Betreffzeile einer E-Mail.	Betreff:"Vierteljährliche Finanzdaten" Betreff:northwind	Nachrichten mit dem exakten Ausdruck „Vierteljährliche Finanzdaten“ in der Betreffzeile. Im zweiten Beispiel werden alle Nachrichten mit dem Wort "northwind" in der Betreffzeile zurückgegeben.
An	Das Feld „An“ einer E-Mail-Nachricht. <sup>1</sup>	to:annb@contoso.com an:annb an:"Ann Beebe"	In allen Beispielen wegen Nachrichten zurückgegeben, in deren Zeile "An" der Name "Ann Beebe" angegeben ist.

#### NOTE

<sup>1</sup> Für den Wert einer Empfängereigenschaft können Sie die SMTP-Adresse, den Anzeigenamen oder den Alias verwenden, um einen Benutzer anzugeben. Sie können z. B. annb@contoso.com, Annb oder „Ann Beebe“ verwenden, um den Benutzer Ann Beebe anzugeben.

## Unterstützte Suchoperatoren

Boolesche Suche Operatoren wie **und**, **oder**, helfen Ihnen die mehr präzise Postfachsuchvorgänge definieren, indem Sie ein- oder Ausschließen von bestimmten Wörtern in der Suchabfrage. Andere Techniken, wie mit eigenschaftsoperatoren (z. B. >= oder...), Anführungszeichen, Klammern und Platzhalter helfen Ihnen bei der Optimierung von Suchabfragen eDiscovery. Die folgende Tabelle enthält die Operatoren, die Sie zum Eingrenzen oder Erweitern der Suchergebnisse verwenden können.

## IMPORTANT

Sie müssen boolesche Operatoren in einer Suchabfrage in Großbuchstaben angeben. Verwenden Sie beispielsweise **\*AND\*** und nicht **\*and\***. Bei Suchoperatoren in Kleinbuchstaben in Suchabfragen wird ein Fehler zurückgegeben.

OPERATOR	VERWENDUNG	BESCHREIBUNG
AND	Wort1 AND Wort2	Gibt zurück, die alle angegebenen Schlüsselwörter enthalten Nachrichten oder <code>property:value</code> Ausdrücke.
+	Wort1 +Wort2 +Wort3	<p>Gibt die Elemente, die <i>entweder</i> enthalten <code>keyword2</code> oder <code>keyword3</code> <i>und</i>, die ebenfalls enthalten <code>keyword1</code> . Aus diesem Grund in diesem Beispiel wird die Abfrage entspricht <code>(keyword2 OR keyword3) AND keyword1</code></p> <p>Beachten Sie, dass die Abfrage <code>keyword1 + keyword2</code> (mit einem Leerzeichen nach der + Symbol) ist nicht identisch mit dem <b>AND</b> - Operator. Mit dieser Abfrage wäre gleichbedeutend mit <code>"keyword1 + keyword2"</code> und Zurückgeben von Elementen mit der genauen Phase <code>"keyword1 + keyword2"</code> .</p>
ODER	Wort1 OR Wort2	Gibt zurück, die eine oder mehrere der angegebenen Schlüsselwörter enthalten Nachrichten oder <code>property:value</code> Ausdrücke.
NOT	Wort1 NOT Wort2 NOT Von:"Ann Beebe"	<p>Schließt Nachrichten, die durch ein Schlüsselwort angegeben oder eine <code>property:value</code> Ausdruck. Beispielsweise <code>NOT from:"Ann Beebe"</code> schließt von Ann Beebe gesendete Nachrichten.</p>
-	Wort1 - Wort2	Identisch mit der <b>nicht</b> -Operator. Diese Abfrage gibt Elementen, die <code>keyword1</code> und schließt Elemente, die enthalten <code>keyword2</code> .
NEAR	Wort1 NEAR(n) Wort2	Gibt Nachrichten mit Wörter, die nahe beieinander, sind zurück, wobei n die Anzahl der Wörter auseinander entspricht. Beispielsweise <code>best NEAR(5) worst</code> gibt Nachrichten, in dem das Wort "schlechtesten" innerhalb von fünf Wörtern von "beste ist". Wenn keine Zahl angegeben wird, ist der Standardabstand acht Wörter.

OPERATOR	VERWENDUNG	BESCHREIBUNG
:	Eigenschaftswert	Der Doppelpunkt (:) in der <code>property:value</code> Syntax gibt an, dass der Wert der Eigenschaft gesucht wird gleich dem angegebenen Wert ist. Beispielsweise <code>recipients:garthf@contoso.com</code> gibt alle an garthf@contoso.com gesendeten Nachrichten.
<	Eigenschaft < Wert	Zeigt an, dass die Eigenschaft, nach der gesucht wird, kleiner ist als der angegebene Wert. <sup>1</sup>
>	Eigenschaft > Wert	Zeigt an, dass die Eigenschaft, nach der gesucht wird, größer ist als der angegebene Wert. <sup>1</sup>
<=	Eigenschaft <= Wert	Zeigt an, dass die Eigenschaft, nach der gesucht wird, kleiner gleich dem angegebenen Wert ist. <sup>1</sup>
>=	Eigenschaft >= Wert	Zeigt an, dass die Eigenschaft, nach der gesucht wird, größer gleich dem angegebenen Wert ist. <sup>1</sup>
..	Eigenschaft: Wert1... Wert2	Zeigt an, dass die Eigenschaft, nach der gesucht wird, größer gleich Wert1 und kleiner gleich Wert2 ist. <sup>1</sup>
""	"fair Value" Betreff:"Vierteljährliche Finanzdaten"	Verwenden Sie doppelte Anführungszeichen ("") für einen exakten Ausdruck oder Begriff in Schlüsselwort suchen und <code>property:value</code> Suchabfragen.
*	cat* Betreff:set*	Präfix Platzhaltersuche (, in dem das Sternchen wird am Ende eines Worts platziert) für NULL oder mehr Zeichen in Schlüsselwörtern übereinstimmen oder <code>property:value</code> Abfragen. Beispielsweise <code>subject:set*</code> Nachrichten, die den Satz von Word, Setup, Einstellung (sowie andere Wörter, die mit "Set" beginnen) enthalten in die Betreffzeile zurückgegeben.
()	(fair OR frei) AND Von:contoso.com (IPO OR Initiale) AND (Aktien OR Anteile) (Vierteljährige Finanzdaten)	Klammern gruppieren boolesche Ausdrücke <code>property:value</code> Elemente und Schlüsselwörter. Beispielsweise <code>(quarterly financials)</code> Elemente, die die Wörter vierteljährliche enthalten und Finanzen zurückgegeben.

## NOTE

Verwenden Sie <sup>1</sup> diesen Operator für Eigenschaften, die Datum oder numerischen Werte besitzen.

## Nicht unterstützte Zeichen in Suchabfragen

Nicht unterstützte Zeichen in einer Suchabfrage führen gewöhnlich zu einem Suchfehler oder zu unerwarteten Ergebnissen. Nicht unterstützte Zeichen sind häufig ausgeblendet und werden der Abfrage hinzugefügt, wenn Sie die Abfrage oder Teile davon aus anderen Anwendungen (z. B. Microsoft Word oder Microsoft Excel) in das Schlüsselwortfeld auf der Abfrageseite der In-Situ-eDiscovery-Suchabfrage kopieren.

Im Folgenden finden Sie eine Liste der nicht unterstützten Zeichen für eine In-Situ-eDiscovery-Suchabfrage.

- **Typografische Anführungszeichen:** Smart einfachen und doppelte Anführungszeichen (auch als "typografische" bezeichnet) werden nicht unterstützt. Bei einer Suchabfrage kann nur gerader Anführungszeichen verwendet werden.
- **Nicht druckbare und Steuerzeichen:** nicht druckbare und Steuerzeichen keine schriftliche Symbol, wie ein alphanumerische Zeichen darstellen. Beispiele für nicht druckbare und Steuerzeichen Zeichen, das Formatieren von Text oder separaten Textzeilen enthalten.
- **Links nach rechts und rechts-nach-links-Zeichen:** Hierbei handelt es sich um Steuerzeichen verwendet, um die Ausrichtung des Textes für Links-nach-rechts-Sprachen (wie Englisch und Spanisch) und rechts-nach-links-Sprachen (wie Arabisch und Hebräisch) anzugeben.
- **Kleinbuchstaben boolesche Operatoren:** Wie vorherige erläutert, Sie müssen Großbuchstabe boolesche Operatoren, wie **und** und **oderin** einer Suchabfrage verwenden. Beachten Sie, dass die Abfragesyntax häufig anzeigt, dass ein booleschen Operators verwendet wird, obwohl Kleinbuchstabe Operatoren verwendet werden können. beispielsweise `(WordA or WordB) and (WordC or WordD)`.

**Wie können Sie nicht unterstützte Zeichen in Ihren Suchabfragen verhindern?** Die beste Möglichkeit zur Verhinderung nicht unterstützter Zeichen besteht darin, die Abfrage direkt in das Schlüsselwortfeld einzugeben. Alternativ können Sie eine Abfrage aus Word oder Excel kopieren und in einem Nur-Text-Editor, z. B. Microsoft Editor, in eine Datei einfügen. Speichern Sie dann die Textdatei, und wählen Sie **ANSI** in der Dropdownliste **Codierung** aus. Dadurch werden alle Formatierungen und nicht unterstützten Zeichen entfernt. Anschließend können Sie die Abfrage aus der Textdatei kopieren und im Schlüsselwort-Abfragefeld einfügen.

## Tipps und Tricks für die Suche

- Schlüsselwortsuchen unterscheiden nicht zwischen Groß- und Kleinschreibung. Beispielsweise geben **katze** und **KATZE** dieselben Ergebnisse zurück.
- Ein Leerzeichen zwischen zwei Schlüsselwörter oder zwei `property:value` Ausdrücke ist identisch mit **AND**. Beispielsweise `from:"Sara Davis" subject:reorganization` gibt alle Sara Davis gesendete Nachrichten, die die Word **Neuorganisation** in der Betreffzeile enthalten.
- Verwenden Sie Syntax, die entspricht der `property:value` Format. Werte Groß-/Kleinschreibung nicht beachtet, und sie dürfen nicht nach dem Operator ein Leerzeichen besitzen. Ist ein Leerzeichen, werden Ihre beabsichtigte Wert nur Volltextindex gesucht. Beispielsweise **an: Pilarp** Suchvorgänge für "Pilarp" als Schlüsselwort, statt die Daten für Nachrichten, die an Pilarp gesendet wurden.
- Wenn Sie nach einer Empfängereigenschaft wie An, Von, Cc oder Empfänger suchen, können Sie eine SMTP-Adresse, einen Alias oder einen Anzeigenamen verwenden, um einen Empfänger anzugeben. Sie können z. B. `pilarp@contoso.com`, `pilarp` oder "Pilar Pinilla" verwenden.
- Sie können nur die Platzhaltersuche Präfix verwenden – beispielsweise `**Katze*` oder **festgelegt\***.

Platzhaltersuche Suffix (\*Katze) oder einer Teilzeichenfolge Platzhaltersuche (\*Katze\*) werden nicht unterstützt.

- Wenn Sie nach einer Eigenschaft suchen, verwenden Sie doppelte Anführungszeichen (" "), wenn der Suchwert aus mehreren Wörtern besteht. Für **Betreff:Budget Q1** werden z. B. Nachrichten zurückgegeben, deren „Betreff“-Zeile **Budget** enthält und denen irgendwo in der Nachricht oder einer der Nachrichteneigenschaften **Q1** vorkommt. Für **Betreff:"Budget Q1"** werden alle Nachrichten zurückgegeben, deren „Betreff“-Zeile **Budget Q1** enthält.

# Suchbeschränkungen für Compliance-eDiscovery in Exchange Online

18.12.2018 • 16 minutes to read

Auf Compliance-eDiscovery-Suchen in Exchange Online und Office 365 werden verschiedene Arten von Beschränkungen angewendet. Diese Beschränkungen sind nützlich, um die Integrität und Qualität der Dienste sicherzustellen, die an Office 365-Organisationen bereitgestellt werden. In den meisten Fällen können diese Beschränkungen nicht geändert werden, doch es ist wichtig, sie zu kennen, um sie bei der Planung, Ausführung und Problembehandlung von eDiscovery-Suchen zu berücksichtigen.

## Quellpostfachbeschränkungen

Bei Compliance-eDiscovery ist die Anzahl der Quellpostfächer, die in einer einzelnen Suche angegeben werden können, beschränkt. In der folgenden Tabelle werden diese Beschränkungen beschrieben, und es werden Alternativen für ihre Umgehung vorgeschlagen. Diese Beschränkungen gelten für eDiscovery-Suchen, die mit dem Exchange-Verwaltungskonsole (EAC) oder der Remote Windows PowerShell erstellt wurden.

BESCHREIBUNG DER BESCHRÄNKUNG	GRENZWERT	WEITERE INFORMATIONEN UND VORGESCHLAGENE PROBLEMUMGEHUNGEN
Die maximale Anzahl von Postfächern, die in einer einzelnen Compliance-eDiscovery-Suche durchsucht werden können.	10,000	<p>Wenn Ihre Organisation mehr als 10.000 Postfächer aufweist, können Sie die Option <b>Alle Postfächer durchsuchen</b> auf der Seite <b>Postfächer</b> in der EAC nicht verwenden. Um eine große Anzahl von Postfächern zu durchsuchen (insgesamt bis zu 10.000 Postfächer), können Sie die Benutzer in Verteilergruppen oder dynamische Verteilergruppen einteilen und dann auf der Seite <b>Postfächer</b> in der EAC eine Gruppe festlegen.<sup>1</sup></p> <p>Eine Umgehungslösung für diese Beschränkung ist die Verwendung der Funktion „Compliance-Suche“ im Office 365 Compliance Center, bei der es keinen Grenzwert für die Anzahl der Postfächer gibt, die in einem einzelnen Suchvorgang durchsucht werden können. Sie führen eine Suche im Compliance Center durch, um alle Postfächer in Ihrer Organisation zu durchsuchen, sodass diejenigen identifiziert werden, die Suchergebnisse enthalten. Sie können anschließend diese Liste der Postfächer als Quellpostfächer für eine Compliance-eDiscovery-Suche in der Exchange-Verwaltungskonsole verwenden. Weitere Informationen finden Sie unter <a href="#">Verwenden der Compliance-Suche in Ihrem eDiscovery-Workflow</a>.</p>
Die maximale Anzahl von Postfächern, die in einer einzelnen Compliance-eDiscovery-Suche durchsucht werden können, die die Anzeige von Schlüsselwortstatistiken erlaubt.	100	<p>Nach der Ausführung einer eDiscovery-Suchergebnisschätzung können Sie die Schlüsselwortstatistik anzeigen. Diese Statistik enthält detaillierte Informationen über die Anzahl der Elemente, die für jedes in der Suchabfrage verwendete Schlüsselwort zurückgegeben werden. Wenn mehr als 100 Quellpostfächer in die Suche einbezogen werden, wird beim Versuch, die Schlüsselwortstatistik anzuzeigen, eine Fehlermeldung zurückgegeben.</p> <p>Um die Schlüsselwortstatistik anzuzeigen, verringern Sie die Anzahl der Quellpostfächer auf 100 oder weniger, und führen Sie die Suchergebnisschätzung erneut aus. Wenn Sie mit der Suchabfrage zufrieden sind, können Sie weitere Quellpostfächer zur Suche hinzufügen und dann die Suchergebnisse kopieren oder exportieren.</p>

BESCHREIBUNG DER BESCHRÄNKUNG	GRENZWERT	WEITERE INFORMATIONEN UND VORGESCHLAGENE PROBLEMUMGEHUNGEN
Die maximale Anzahl der Postfächer, die in einem Compliance-Archiv in einer einzelnen Compliance-eDiscovery-Suche angegeben werden können	10,000	<p>Sie können bei einer einzelnen eDiscovery-Suche bis zu 10.000 Postfächer im Compliance-Archiv platzieren. Wenn Sie jedoch die Option <b>Alle Postfächer durchsuchen</b> auf der Seite <b>Quellen</b> auswählen, werden Sie ein Compliance-Archiv für diese Suche nicht aktivieren können. Um eine große Anzahl von Postfächern mithilfe eines einzigen Compliance-Archivs zu platzieren, verwenden Sie Verteilergruppen oder dynamische Verteilergruppen, um Postfächer zu gruppieren, und geben Sie dann eine dieser Gruppen auf der Seite <b>Postfächer</b> in der EAC an.<sup>1</sup></p> <p>Eine bessere Option für das Platzieren einer großen Anzahl von Postfächern ist die Verwendung eines Beweissicherungsverfahrens. Die Verwendung vieler einzelner Compliance-eDiscovery-Suchen für die Platzierung von Postfächern wird nicht empfohlen. Weitere Informationen finden Sie unter <a href="#">Place all mailboxes on hold</a>.</p>

#### NOTE

<sup>1</sup> Gruppenmitgliedschaft wird nur dann berechnet, wenn die Suche oder eine Platzierung erstellt wird. Wenn ein Benutzer zur Gruppe hinzugefügt wird, nachdem die Suche erstellt wurde, wird das Benutzerpostfach nicht automatisch als ein Quellpostfach hinzugefügt. Sie müssen die Suche bearbeiten und das Postfach hinzufügen. Dasselbe gilt, wenn ein Benutzer aus einer Gruppe entfernt wird, die für die Erstellung einer Suche oder eines Archivs verwendet wird. Sie müssen die Suche bearbeiten, um das Postfach zu entfernen.

## Exchange-Verwaltungskonsole-Grenzwerte

Auch bei der Verwendung der EAC zum Erstellen und Ausführen von Compliance-eDiscovery-Suchen gibt es Beschränkungen. Sie betreffen hauptsächlich die Anzahl der Quellpostfächer, die in der EAC angezeigt werden, wenn Sie die zu durchsuchenden Quellpostfächer auswählen. In der folgenden Tabelle werden diese Beschränkungen beschrieben, und es werden Alternativen für ihre Umgehung vorgeschlagen.

BESCHREIBUNG DER BESCHRÄNKUNG	GRENZWERT	WEITERE INFORMATIONEN UND VORGESCHLAGENE PROBLEMUMGEHUNGEN
Die maximale Anzahl der Postfächer, die beim Erstellen einer neuen Compliance-eDiscovery- oder Compliance-Archiv-Suche in der Postfachauswahl für die Auswahl der Quellpostfächer angezeigt werden	500	<p>Es werden nur 500 Postfächer, Verteilergruppen und dynamische Verteilergruppen in der Postfachauswahl aufgelistet, aus denen Sie beim Erstellen einer neuen Suche Quellpostfächer auswählen können. Es wird eine Nachricht angezeigt, die darauf hinweist, dass mehr Empfänger vorhanden sind, als angezeigt werden. Hier sind einige Problemumgehungen für diese Beschränkung:</p> <p>Verwenden Sie das Suchfeld, um ein Postfach zu finden, das in der Postfachauswahl nicht aufgelistet ist.</p> <p>Verwenden Sie Verteilergruppen oder dynamische Verteilergruppen, um viele Postfächer zu gruppieren. Wählen Sie dann die Gruppe aus der Postfachliste aus, oder suchen Sie es mithilfe des Suchfelds. Gruppen werden in Quellpostfächer erweitert, wenn Sie eine eDiscovery-Suche erstellen.</p> <p>Wählen Sie <b>Alle Postfächer durchsuchen</b> auf der Seite <b>Postfach</b> aus, wenn Ihre Organisation weniger als 10.000 Postfächer umfasst und Sie keine Postfächer im Archiv platzieren werden.</p> <p>Verwenden Sie Verteilergruppen oder dynamische Verteilergruppen, um Benutzer zu gruppieren, wenn Sie mehr als 500 Postfächer im Compliance-Archiv platzieren möchten.</p>

BESCHREIBUNG DER BESCHRÄNKUNG	GRENZWERT	WEITERE INFORMATIONEN UND VORGESCHLAGENE PROBLEMUMGEHUNGEN
Die maximale Anzahl von Postfächern, die angezeigt werden, wenn Sie eine Compliance-eDiscovery- oder Compliance-Archiv-Suche bearbeiten	3,000	<p>Bis zu 3.000 Postfächer werden angezeigt auf <b>der Seite in der Exchange-Verwaltungskonsole</b> beim Bearbeiten einer Compliance-eDiscovery-Suche oder halten. Das Suchfeld können Sie zum Hinzufügen eines Postfachs in die Liste der Quellen finden ein Postfach, das nicht aufgeführt ist, im Auswahltool Postfach (maximal 500 Empfänger werden im Auswahltool Postfach aufgeführt). Um ein Postfach zu entfernen, die aufgeführt wird, können Sie wählen Sie sie aus und klicken Sie dann auf <b>Entfernen</b>. Um ein Postfach zu entfernen, die nicht aufgeführt ist, müssen Sie Exchange Online PowerShell verwenden, um es zu entfernen. Beispielsweise sind folgende Befehle ausführen, um den Benutzer Ann Beebe aus einer Compliance-Archivs mit dem Namen ContosoHold zu entfernen.</p> <pre>\$SourceMailboxes = Get-MailboxSearch "ContosoHold" \$SourceMailboxes.Sources.Remove("/o=contoso/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=28e3edb87e294229annb") Set-MailboxSearch "ContosoHold" -SourceMailboxes \$SourceMailboxes.Sources</pre> <p>Der erste Befehl erstellt eine Variable, die die Eigenschaften von ContosoHold enthält. Der zweite Befehl entfernt die Benutzerin Ann Beebe (durch die Angabe des Werts der Eigenschaft <b>LegacyExchangeDN</b>) aus der Liste der Quellpostfächer. Der dritte Befehl bearbeitet ContosoHold mit der aktualisierten Liste von Quellpostfächern.</p> <p>Um einen Benutzer zu einem Compliance-Archiv hinzuzufügen, verwenden Sie die folgende Syntax des zweiten Befehls im vorherigen Beispiel.</p> <pre>\$SourceMailboxes.Sources.Add("&lt;LegacyExchangeDN of the user&gt;")</pre> <p><b>Hinweis:</b> die <b>Quellen</b>-Eigenschaft einer Compliance-eDiscovery-Suche oder eine In-Place Hold identifiziert die Quellpostfächer durch ihre <b>LegacyExchangeDN</b>-Eigenschaft. Da diese Eigenschaft ein Benutzerpostfach eindeutig identifiziert wird, verhindert mithilfe der <b>Quellen</b>-Eigenschaft hinzufügen oder Entfernen von das falsche Postfach. Dadurch wird auch um Probleme zu vermeiden, wenn zwei Postfächer die gleichen Alias oder die primäre SMTP-Adresse verfügen.</p>

## Sonstige Beschränkungen

In der folgenden Tabelle werden weitere Beschränkungen beschrieben, die sich auf Compliance-eDiscovery-Suchen auswirken.

BESCHREIBUNG DER BESCHRÄNKUNG	GRENZWERT	WEITERE INFORMATIONEN
-------------------------------	-----------	-----------------------

BESCHREIBUNG DER BESCHRÄNKUNG	GRENZWERT	WEITERE INFORMATIONEN
Die maximale Anzahl der Compliance-eDiscovery-Suchen, die in Ihrer Organisation gleichzeitig ausgeführt werden können	2	<p>Wenn eine eDiscovery-Suche gestartet wird, während zwei andere Suchvorgänge ausgeführt werden, wird die dritte Suche nicht in die Warteschlange eingereiht, sondern es tritt bei dieser ein Fehler auf. Sie müssen warten, bis eine der ausgeführten Suchen abgeschlossen ist, bevor sie eine neue Suche starten können.</p> <p>Sowohl auf Schätzungen basierende Suchen als auch Kopiesuchen werden in Compliance-eDiscovery-Suchen ebenfalls berücksichtigt. Das heißt, wenn Sie gleichzeitig eine auf Schätzungen basierende Suche und eine Kopiesuche ausführen, können Sie keine weitere Suche starten, bis eine der ausgeführten Suchen abgeschlossen ist. Sie können jedoch die Suchergebnisse in der Vorschau anzeigen oder aus einer anderen Suche exportieren, während zwei Suchen ausgeführt werden.</p>
Die maximale Anzahl von Schlüsselwörtern, die in einer einzelnen Compliance-eDiscovery-Suchabfrage angegeben werden können	500	<p>Boolesche Operatoren, wie <b>AND</b> und <b>OR</b> werden nicht für die Gesamtzahl der Schlüsselwörter gezählt. Beispielsweise die Stichwortabfrage <code>cat AND dog AND bird AND fish</code> besteht aus vier Schlüsselwörtern.</p>
Die maximale Anzahl von Elementen, die auf der Suchvorschauseite der Compliance-eDiscovery-Suchergebnisse angezeigt werden	200	<p>Wenn Sie die Suchergebnisse in der Vorschau anzeigen, werden die durchsuchten Postfächer im rechten Bereich auf der Vorschauseite der eDiscovery-Suche angezeigt. Für jedes Postfach werden außerdem die Anzahl der zurückgegebenen Elemente und die Gesamtgröße dieser Elemente angezeigt. Von der Suche zurückgegebene Elemente werden im rechten Bereich aufgelistet. Bis zu 200 Elemente werden auf der Vorschauseite angezeigt.</p> <p><b>Hinweis:</b> Elemente aus jedem Postfach können nicht im rechten Bereich angezeigt werden, indem Sie auf ein Postfach im linken Bereich. Um die von einem bestimmten Postfach zurückgegebenen Elemente anzuzeigen, können Sie die Suchergebnisse kopieren und anzeigen, die Elemente in das discoverypostfach.</p>
Die maximale Anzahl von Stichwörtern, die in allen Compliance-Archiven für ein einzelnes Postfach angegeben werden kann.	500	<p>Wenn mehrere In-Situ-Speicher für das Postfach eines Benutzers aktiviert sind, ist die maximale Anzahl von Stichwörtern in allen Suchabfragen 500. Der Grund hierfür ist, dass Exchange Online alle Stichwortsuchparameter aus allen In-Situ-Speichern mithilfe des Operators <b>OR</b> kombiniert. Wenn Archivabfragen mehr als 500 Stichwörter enthalten, werden sämtliche Inhalte des Postfachs archiviert und nicht bloß die Inhalte, die mit den Suchkriterien abfragebasierter Archive übereinstimmen. Alle Inhalte werden archiviert, bis die Gesamtzahl von Stichwörtern in allen Compliance-Archiven auf 500 oder weniger verringert wird. Das Archivieren aller Postfachinhalte entspricht der Funktionalität eines Beweissicherungsverfahrens.</p>

BESCHREIBUNG DER BESCHRÄNKUNG	GRENZWERT	WEITERE INFORMATIONEN
Maximale Anzahl zurückgegebener Varianten, wenn ein Präfixplatzhalter zum Suchen eines exakten Ausdrucks in einer Stichwortsuchabfrage oder ein Präfixplatzhalter und der Operator <b>NEAR</b> verwendet werden.	10,000	Für nicht-Satz Abfragen verwenden wir einen spezielle Präfix Index. Dies teilt uns nur mit, dass ein Wort in einem Dokument, das nicht im Dokument Auftretens auftritt. Um eine Abfrage Phrase ausführen müssen wir die Position innerhalb des Dokuments für die Wörter im Ausdruck verglichen werden soll. Dies bedeutet, dass wir den Präfix Index für Phrase Abfragen verwendet werden können. In diesem Fall werden wir intern die Abfrage mit alle möglichen Wörter, das das Präfix erweitert, erweitern (d. h. "Zeit*" erweitern können Sie auf "Zeit OR Timer OR Zeiten OR Timex OR eingegrenzte oder..."). 10.000 ist die maximale Anzahl von Varianten, die das Wort, nicht die Anzahl der Dokumente, die mit der Abfrage übereinstimmen erweitert werden kann. Für nicht-Satz Begriffe sind keine Obergrenze.

# Erstellen eines Discoverypostfachs

18.12.2018 • 6 minutes to read

Microsoft Exchange Server-Setup wird standardmäßig ein discoverypostfach erstellt. In Exchange Online ist ein discoverypostfach auch in der Standardeinstellung erstellt. Discoverypostfächer dienen als Ziel Postfächer für die [Compliance - eDiscovery](#)-Suche in der Exchange-Verwaltungskonsole (EAC). Sie können zusätzliche discoverypostfächer nach Bedarf erstellen. Nachdem Sie ein neues discoverypostfach erstellen, müssen Sie die entsprechenden Benutzer Vollzugriffsberechtigungen zuweisen, damit sie eDiscovery-Suchergebnissen zugreifen können, die in das discoverypostfach kopiert werden.

**Caution**

Nachdem ein Discovery-Manager die Ergebnisse einer eDiscovery-Suche in ein Discoverypostfach kopiert hat, kann das Postfach potenziell vertrauliche Informationen enthalten. Sie sollten den Zugriff auf Discoverypostfächer daher kontrollieren und sicherstellen, dass nur autorisierte Benutzer darauf zugreifen können.

Weitere Informationen finden Sie unter [Discoverypostfächer](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Erstellen von Discoverypostfächern" im Thema [Berechtigungen für Messagingrichtlinien und Kompatibilität](#).
- Für Discoverypostfächer gilt ein Postfachspeicherkontingent von 50 GB. Dieses Speicherkontingent kann nicht erhöht werden.
- Sie können nicht der Exchange-Verwaltungskonsole verwenden, um ein discoverypostfach erstellen oder Zuweisen von Berechtigungen darauf zugreifen. Sie müssen Exchange Online PowerShell verwenden. Verwenden Sie in Office 365 Remote-PowerShell mit Ihrer Exchange Online-Organisation verbunden ist.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

**TIP**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## (Optional) Schritt 1: Herstellen einer Verbindung mit Exchange Online mithilfe der Remote-PowerShell

Sie müssen nur diesen Schritt ausführen, wenn Sie eine Exchange Online oder Office 365-Organisation haben. Wenn Sie Exchange Server-Organisation haben, wechseln Sie mit dem nächsten Schritt fort, und führen Sie den Befehl im Exchange Online PowerShell.

1. Öffnen Sie auf Ihrem lokalen Computer Windows PowerShell, und führen Sie dann den folgenden Befehl aus.

```
$UserCredential = Get-Credential
```

```
<span data-ttu-id="2111a-133">Klicken Sie im Dialogfeld **Windows PowerShell anmelden** Geben Sie Benutzername und Kennwort für Office 365 globaler Administrator-Konto ein, und klicken Sie dann auf **OK**.</span><span class="sxs-lookup"><span data-stu-id="2111a-133">In the **Windows PowerShell Credential Request** dialog box, type username and password for an Office 365 global admin account, and then click **OK**.</span></span>
```

2. Führen Sie den folgenden Befehl aus.

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection
```

3. Führen Sie den folgenden Befehl aus.

```
Import-PSSession $Session
```

4. Um zu prüfen, ob Sie mit Ihrer Exchange Online-Organisation verbunden sind, führen Sie den folgenden Befehl aus, um eine Liste aller Postfächer in Ihrer Organisation abzurufen.

```
Get-Mailbox
```

Weitere Informationen oder Hinweise bei Problemen mit der Verbindung zu Ihrer Exchange Online-Organisation finden Sie unter [Herstellen einer Verbindung mit Exchange Online mithilfe der Remote-PowerShell](#).

## Schritt 2: Erstellen eines Discoverypostfachs

In diesem Beispiel wird das Discoverypostfach "SearchResults" erstellt.

```
New-Mailbox -Name SearchResults -Discovery
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [new-Mailbox](#).

Um eine Liste aller Discoverypostfächer in einer Exchange-Organisation anzuzeigen, führen Sie den folgenden Befehl aus:

```
Get-Mailbox -Resultsize unlimited -Filter {RecipientTypeDetails -eq "DiscoveryMailbox"}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-Mailbox](#).

## Schritt 3: Zuweisen von Berechtigungen zu einem Discoverypostfach

Sie müssen Benutzern oder Gruppen explizit die Berechtigung zum Öffnen des von Ihnen erstellten Discoverypostfachs zuweisen. Verwenden Sie die folgende Syntax, um einem Benutzer oder einer Gruppe die Berechtigung zum Öffnen eines Discoverypostfachs und zum Anzeigen der Suchergebnisse zu gewähren:

```
Add-MailboxPermission <Name of the discovery mailbox> -User <Name of user or group> -AccessRights FullAccess -InheritanceType all
```

Mit dem folgenden Befehl wird der Gruppe Litigation-Manager zum Beispiel Vollzugriff zugewiesen, sodass die Mitglieder dieser Gruppe das Discoverypostfach "Fabrikam Litigation" öffnen können.

```
Add-MailboxPermission "Fabrikam Litigation" -User "Litigation Managers" -AccessRights FullAccess -  
InheritanceType all
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Add-MailboxPermission](#).

## Weitere Informationen

- Standardmäßig haben Mitglieder der Rollengruppe "Discoveryverwaltung" nur auf das standardmäßige Discovery-Suchpostfach Vollzugriff. Sie müssen der Rollengruppe "Discoveryverwaltung" explizit den Vollzugriff zuweisen, damit die Mitglieder ein von Ihnen erstelltes Discoverypostfach öffnen können.
- Auch wenn das Discoverypostfach in der Exchange-Adressenliste angezeigt wird, können die Benutzer keine E-Mail-Nachrichten an dieses Postfach senden. Die E-Mail-Zustellung an Discoverypostfächer ist aufgrund von Zustellungseinschränkungen unzulässig. Auf diese Weise wird die Integrität der Suchergebnisse gewährleistet, die in ein Discoverypostfach kopiert werden.
- Ein Discoverypostfach kann nicht für einen anderen Zweck wiederverwendet oder in einen anderen Postfachtyp umgewandelt werden.
- Sie können ein Discoverypostfach ebenso löschen wie jeden anderen Postfachtyp.

# Erstellen eines benutzerdefinierten Verwaltungsbereichs für die Compliance-eDiscovery-Suche

18.12.2018 • 19 minutes to read

Sie können mithilfe eines benutzerdefinierten Verwaltungsbereichs lassen Sie bestimmte Personen oder Gruppen In-Place eDiscovery verwenden, um eine Teilmenge von Postfächern in Ihrer Exchange Online-Organisation zu suchen. Angenommen, möchten Sie einen Discovery-Manager nur die Postfächer der Benutzer in einem bestimmten Standort oder jede Abteilung durchsuchen lassen. Hierzu können Sie einen benutzerdefinierten Verwaltungsbereich erstellen. Dieser benutzerdefinierten Verwaltungsbereich verwendet einen Empfängerfilter steuern, welche Postfächer durchsucht werden können. Empfängerfilter Bereiche verwenden Filter basierend auf dem Empfängertyp oder anderen Empfängereigenschaften bestimmte Empfänger als Ziel.

Für Compliance-eDiscovery ist die einzige Eigenschaft auf ein Benutzerpostfach, die Sie verwenden können, um einen Empfängerfilter für einen benutzerdefinierten Bereich erstellen Verteilung Gruppenmitgliedschaft (tatsächlichen Eigenschaftenamen ist *MemberOfGroup*). Bei Verwendung anderer Eigenschaften wie *CustomAttributeN*, *\_Abteilung\_* oder *PostalCode*, fällt für die Suche aus, wenn sie von einem Mitglied der Rollengruppe ausgeführt wird, die den benutzerdefinierten Bereich zugewiesen hat.

Weitere Informationen zu Verwaltungsbereichen finden Sie unter:

- [Grundlegendes zu Verwaltungsrollenbereichen](#)
- [Grundlegendes zu Verwaltungsrollenbereichs-Filtern](#)

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 15 Minuten
- Wie bereits erwähnt, können Sie nur die Gruppenmitgliedschaft als Empfängerfilter verwenden, um einen benutzerdefinierten Empfängerfilterbereich zu erstellen, der für eDiscovery verwendet werden soll. Alle anderen Empfängereigenschaften können nicht zum Einrichten eines benutzerdefinierten Bereichs für eDiscovery-Suchen verwendet werden. Beachten Sie, dass die Mitgliedschaft in einer dynamischen Verteilergruppe ebenfalls nicht verwendet werden kann.
- Führen Sie die Schritte 1 bis 3 durch, damit ein Discovery-Manager die Suchergebnisse einer eDiscovery-Suche exportiert, bei der ein benutzerdefinierter Verwaltungsbereich verwendet wird.
- Wenn Ihr Discovery-Manager keine Vorschau der Suchergebnisse anzeigen muss, können Sie Schritt 4 überspringen.
- Wenn Ihr Discovery-Manager die Suchergebnisse nicht kopieren muss, können Sie Schritt 5 überspringen.

## Schritt 1: Organisieren von Benutzern in Verteilergruppen für eDiscovery

Um eine Teilmenge der Postfächer in Ihrer Organisation zu durchsuchen oder um den Bereich der Quellpostfächer einzuschränken, die ein Discovery-Manager durchsuchen kann, müssen Sie die Teilmenge der Postfächer in einer oder mehreren Verteilergruppen zusammenfassen. Wenn Sie einen benutzerdefinierten Verwaltungsbereich in Schritt 2 erstellen, verwenden Sie diese Verteilergruppen als Empfängerfilter zum Erstellen

eines benutzerdefinierten Verwaltungsbereichs. Dadurch erhält ein Discovery-Manager die Möglichkeit, nur die Postfächer der Benutzer zu durchsuchen, die Mitglied einer bestimmten Gruppe sind.

Sie können bereits vorhandene Verteilergruppen mit eDiscovery verwenden oder neue Verteilergruppen erstellen. Unter [Weitere Informationen](#) am Ende dieses Themas erhalten Sie Tipps zum Erstellen von Verteilergruppen, die verwendet werden können, um den Umfang von eDiscovery-Suchen festzulegen.

## Schritt 2: Erstellen eines benutzerdefinierten Verwaltungsbereichs

Nun erstellen Sie einen benutzerdefinierten Verwaltungsbereich, der durch die Mitgliedschaft einer Verteilergruppe (mithilfe des Empfängerfilters *MemberOfGroup*) definiert ist. Wenn dieser Bereich zu einer Rollengruppe für eDiscovery verwendet angewendet wird, können die Mitglieder der Rollengruppe die Postfächer der Benutzer suchen, die Mitglieder der Verteilergruppe sind, die zum Erstellen des benutzerdefinierten Verwaltungsbereichs verwendet wurde.

Dieses Verfahren verwendet Exchange Online PowerShell-Befehle, um einen benutzerdefinierten Bereich mit dem Namen Ottawa-Benutzer eDiscovery Bereich zu erstellen. Es gibt die Verteilergruppe namens Ottawa-Benutzer für den Empfängerfilter des benutzerdefinierten Bereichs an.

1. Führen Sie diesen Befehl aus, um die Eigenschaften der Gruppe "Ottawa-Benutzer" (Ottawa Users) abzurufen und in einer Variablen zu speichern, die im nächsten Befehl verwendet wird.

```
$DG = Get-DistributionGroup -Identity "Ottawa Users"
```

2. Führen Sie diesen Befehl aus, um einen benutzerdefinierten Verwaltungsbereich basierend auf der Mitgliedschaft in der Verteilergruppe "Ottawa-Benutzer" (Ottawa Users) zu erstellen.

```
New-ManagementScope "Ottawa Users eDiscovery Scope" -RecipientRestrictionFilter "MemberOfGroup -eq '$($DG.DistinguishedName)'"
```

<span data-ttu-id="568be-139">Der Distinguished Name der Verteilergruppe, der in der Variablen \*\*\*\$DG\*\*\* enthalten ist, wird zum Erstellen des Empfängerfilters für den neuen Verwaltungsbereich verwendet.</span><span class="sxs-lookup"><span data-stu-id="568be-139">The distinguished name of the distribution group, which is contained in the variable \*\*\*\$DG\*\*\*, is used to create the recipient filter for the new management scope.</span></span>

## Schritt 3: Erstellen einer Verwaltungsrollengruppe

In diesem Schritt erstellen Sie eine neue Verwaltungsrollengruppe und weisen den in Schritt 2 erstellten benutzerdefinierten Bereich zu. 2. Fügen Sie die Rollen "Gesetzliche Aufbewahrungsfrist" und "Postfachsuche" hinzu, sodass die Rollenmitglieder Compliance-eDiscovery-Suchen durchführen und Compliance-Archive oder das Beweissicherungsverfahren für Postfächer festlegen können. Sie können dieser Rollengruppe auch Mitglieder hinzufügen, die dann die Postfächer der Mitglieder der Verteilergruppe durchsuchen können, die zum Erstellen des benutzerdefinierten Bereichs in Schritt 2 verwendet wurde.

In den folgenden Beispielen wird die Sicherheitsgruppe Ottawa-Benutzer eDiscovery-Managern als Mitglieder dieser Rollengruppe hinzugefügt. Exchange Online PowerShell oder der Exchange-Verwaltungskonsole können für diesen Schritt.

### Verwenden von Exchange Online PowerShell zum Erstellen einer verwaltungsrollengruppe

Führen Sie diesen Befehl aus, um eine neue Rollengruppe zu erstellen, die den in Schritt 2 erstellten benutzerdefinierten Bereich verwendet. 2. Mit dem Befehl werden auch die Rollen "Gesetzliche Aufbewahrungsfrist" und "Postfachsuche" und die Sicherheitsgruppe "eDiscovery-Manager für Ottawa-Benutzer"

(Ottawa Users eDiscovery Managers) als Mitglieder der neuen Rollengruppe hinzugefügt.

```
New-RoleGroup "Ottawa Discovery Management" -Roles "Mailbox Search", "Legal Hold" -CustomRecipientWriteScope  
"Ottawa Users eDiscovery Scope" -Members "Ottawa Users eDiscovery Managers"
```

### Erstellen einer Verwaltungsrollengruppe im Exchange Admin Center

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Administratorrollen**, und klicken Sie dann auf **New**
2. Geben Sie unter **Neue Rollengruppe** die folgenden Informationen an:
  - **Name:** Geben Sie einen beschreibenden Namen für die neue Rollengruppe. In diesem Beispiel würden Sie Ottawa Discovery Management verwenden.
  - **Bereich schreiben:** Wählen Sie den benutzerdefinierten Verwaltungsbereich, die Sie in Schritt 2 erstellt haben. In diesem Bereich wird auf der neuen Rollengruppe angewendet werden.
  - **Rollen:** Klicken Sie auf **Add** , und der neuen Rollengruppe die Rollen **Gesetzliche Aufbewahrungsfrist** und **Postfachsuche** hinzuzufügen.
  - **Member:** Klicken Sie auf **Add** , und wählen Sie die Benutzer, Sicherheitsgruppe oder Rollengruppen, die Sie als Mitglieder der neuen Rollengruppe hinzufügen möchten. In diesem Beispiel werden die Mitglieder der Sicherheitsgruppe **Ottawa-Benutzer eDiscovery-Manager** können nur die Postfächer der Benutzer zu suchen, die Mitglieder der Verteilergruppe "**Ottawa-Benutzer**" sind.
3. Klicken Sie auf **Speichern**, um die Rollengruppe zu erstellen.

Nachfolgend finden Sie ein Beispiel, wie das Fenster **Neue Rollengruppe** anschließend aussieht.

new role group

\*Name:  
Ottawa Discovery Management

Description:  
The role group uses the Ottawa Users eDiscovery Scope to limit the mailboxes that can be searched by the Ottawa eDiscovery Managers only to members of the Ottawa Users distribution group.

Write scope:  
Ottawa Users eDiscovery Scope

Roles:  
+ -

NAME
Legal Hold
Mailbox Search

Members:  
+ -

NAME	DISPLAY NAME
Ottawa Users eDiscovery Managers	Ottawa Users e...

save cancel

## (Optional) Schritt 4: Hinzufügen von Discovery-Managern als Mitglieder der Verteilergruppe, die zum Erstellen des benutzerdefinierten Verwaltungsbereichs verwendet wurde

Diesen Schritt müssen Sie nur ausführen, wenn ein Discovery-Manager eine Vorschau der eDiscovery-Suchergebnisse anzeigen soll.

Führen Sie diesen Befehl aus, um die Sicherheitsgruppe "eDiscovery-Manager für Ottawa-Benutzer" (Ottawa Users eDiscovery Managers) als Mitglied der Verteilergruppe "Ottawa-Benutzer" (Ottawa Users) hinzuzufügen.

```
Add-DistributionGroupMember -Identity "Ottawa Users" -Member "Ottawa Users eDiscovery Managers"
```

Der Exchange-Verwaltungskonsole können auch die Mitglieder einer Verteilergruppe hinzufügen. Weitere Informationen finden Sie unter [Erstellen und Verwalten von Verteilergruppen](#).

## (Optional) Schritt 5: Hinzufügen eines Discoverypostfachs als Mitglied der Verteilergruppe, die zum Erstellen des benutzerdefinierten Verwaltungsbereichs verwendet wurde

Diesen Schritt müssen Sie nur ausführen, wenn ein Discovery-Manager eDiscovery-Suchergebnisse kopieren soll.

Führen Sie diesen Befehl aus, um das Discoverypostfach "Ottawa-Discoverypostfach" (Ottawa Discovery Mailbox) als Mitglied der Verteilergruppe "Ottawa-Benutzer" (Ottawa Users) hinzuzufügen.

```
Add-DistributionGroupMember -Identity "Ottawa Users" -Member "Ottawa Discovery Mailbox"
```

#### NOTE

Zum Öffnen eines Discoverypostfachs und Anzeigen der Suchergebnisse muss Discovery-Managern Vollzugriff für das Discoverypostfach gewährt werden. Weitere Informationen finden Sie unter [Erstellen eines Discoverypostfachs](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Im Folgenden sind einige Möglichkeiten aufgeführt, wie Sie überprüfen können, ob die benutzerdefinierten Verwaltungsbereiche für eDiscovery erfolgreich implementiert wurden. Vergewissern Sie sich bei der Überprüfung, dass der Benutzer, der die eDiscovery-Suchen ausführt, ein Mitglied der Rollengruppe ist, die den benutzerdefinierten Verwaltungsbereich verwendet.

- Erstellen Sie eine eDiscovery-Suche, und wählen Sie die Verteilergruppe, mit der der benutzerdefinierte Verwaltungsbereich erstellt wurde, als Quelle der zu durchsuchenden Postfächer aus. Alle Postfächer sollten erfolgreich durchsucht werden.
- Erstellen einer eDiscovery-Suche, und suchen Sie die Postfächer der Benutzer, die Mitglieder der Verteilergruppe, die zum Erstellen des benutzerdefinierten Verwaltungsbereichs verwendet wurde, werden nicht. Die Suche sollte fehl, da der Discovery-Manager nur Postfächer für Benutzer suchen kann, die Mitglieder der Verteilergruppe sind, die zum Erstellen des benutzerdefinierten Verwaltungsbereichs verwendet wurde. In diesem Fall ein Fehler wie "kann nicht zum Durchsuchen Postfachs < Name des Postfachs >, da der aktuelle Benutzer keinen Zugriff auf das Postfach Berechtigungen" zurückgegeben.
- Erstellen Sie eine eDiscovery-Suche, und durchsuchen Sie die Postfächer der Benutzer, die Mitglieder der Verteilergruppe sind, die zum Erstellen des benutzerdefinierten Bereichs verwendet wurde. Schließen Sie in diese Suche auch die Postfächer der Benutzer ein, die keine Mitglieder sind. Die Suche sollte teilweise erfolgreich sein. Die Postfächer der Mitglieder der Verteilergruppe, mit der der benutzerdefinierte Verwaltungsbereich erstellt wurde, sollten erfolgreich durchsucht werden. Das Durchsuchen der Postfächer der Benutzer, die keine Mitglieder der Gruppe sind, sollte fehlschlagen.

## Weitere Informationen

- Da Verteilergruppen in diesem Szenario nicht zur Nachrichtenübermittlung sondern zum Festlegen des Umfangs von eDiscovery-Suchen verwendet werden, sollten Sie Folgendes erwägen, wenn Sie Verteilergruppen für eDiscovery erstellen und konfigurieren:
  - Erstellen Sie eine geschlossene Mitgliedschaft Verteilergruppen, sodass Mitglieder hinzugefügt oder nur durch die Gruppenbesitzer aus der Gruppe entfernt werden können. Wenn Sie die Gruppe in Exchange Online PowerShell erstellen möchten, verwenden Sie die Syntax `MemberJoinRestriction closed` und `MemberDepartRestriction closed`.
  - Aktivieren Sie Moderation der Gruppe, sodass eine beliebige Nachricht an die Gruppe zuerst an die Gruppenmoderatoren gesendet wird, die genehmigen oder ablehnen die Nachricht entsprechend anpassen können. Wenn Sie die Gruppe in Exchange Online PowerShell erstellen möchten, verwenden Sie die Syntax `ModerationEnabled $true`. Wenn Sie die Exchange-Verwaltungskonsole verwenden, können Sie die Moderation aktivieren, nachdem die Gruppe erstellt wird.

- Ausblenden der Verteilergruppe freigegebenen Adressbuch der Organisation. Verwenden der Exchange-Verwaltungskonsole oder über das Cmdlet **Set-DistributionGroup**, nachdem die Gruppe erstellt wird. Wenn Sie Exchange Online PowerShell verwenden, verwenden Sie die Syntax `HiddenFromAddressListsEnabled $true`.

Im folgenden Beispiel erstellt der erste Befehl eine Verteilergruppe mit geschlossener Mitgliedschaft und aktiverter Moderation. Der zweite Befehl blendet die Gruppe im freigegebenen Adressbuch aus.

```
New-DistributionGroup -Name "Vancouver Users eDiscovery Scope" -Alias VancouverUserseDiscovery -MemberJoinRestriction closed -MemberDepartRestriction closed -ModerationEnabled $true
```

```
Set-DistributionGroup "Vancouver Users eDiscovery Scope" -HiddenFromAddressListsEnabled $true
```

Weitere Informationen zum Erstellen und Verwalten von Verteilergruppen finden Sie unter [Erstellen und Verwalten von Verteilergruppen](#).

- Obwohl Sie nur die Mitgliedschaft in Verteilergruppen als Empfängerfilter für einen für eDiscovery genutzten benutzerdefinierten Verwaltungsbereich verwenden können, können Sie jedoch Benutzer dieser Verteilergruppe mithilfe weiterer Empfängereigenschaften hinzufügen. Hier sind einige Beispiele dafür, wie mit den Cmdlets **Get-Mailbox** und **Get-Recipient** eine bestimmte Gruppe von Benutzern basierend auf allgemeinen Benutzer- oder Postfachattributen zurückgegeben wird.

```
Get-Recipient -RecipientTypeDetails UserMailbox -ResultSize unlimited -Filter 'Department -eq "HR"'
```

```
Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize unlimited -Filter 'CustomAttribute15 -eq "VancouverSubsidiary"'
```

```
Get-Recipient -RecipientTypeDetails UserMailbox -ResultSize unlimited -Filter 'PostalCode -eq "98052"'
```

```
Get-Recipient -RecipientTypeDetails UserMailbox -ResultSize unlimited -Filter 'StateOrProvince -eq "WA"'
```

```
Get-Mailbox -RecipientTypeDetails UserMailbox -ResultSize unlimited -OrganizationalUnit "namsr01a002.sdf.exchangelabs.com/Microsoft Exchange Hosted Organizations/contoso.onmicrosoft.com"
```

- Sie können die Beispiele aus dem vorherigen Aufzählungszeichen klicken Sie dann zum Erstellen einer Variablen, die mit dem Cmdlet **Add-DistributionGroupMember** verwendet werden, um eine Gruppe von Benutzern an eine Verteilergruppe hinzufügen. Im folgenden Beispiel wird der erste Befehl eine Variable, die alle Benutzerpostfächer enthält, die für die *Abteilung* -Eigenschaft den Wert **Vancouver** in ihr Konto besitzen erstellt. Im zweiten Befehl wird der Verteilergruppe Vancouver Benutzer diese Benutzer hinzugefügt.

```
$members = Get-Recipient -RecipientTypeDetails UserMailbox -ResultSize unlimited -Filter 'Department -eq "Vancouver"'
```

```
$members | ForEach {Add-DistributionGroupMember "Ottawa Users" -Member $_.Name}
```

- Mit dem Cmdlet **Add-RoleGroupMember** können Sie ein Mitglied einer bestehenden Rollengruppe hinzufügen, mit der der Umfang von eDiscovery-Suchen festgelegt wird. Der folgende Befehl beispielsweise fügt den Benutzer "admin@ottawa.contoso.com" der Rollengruppe "Ottawa-Discoveryverwaltung" (Ottawa Discovery Management) hinzu.

```
Add-RoleGroupMember "Vancouver Discovery Management" -Member paralegal@vancouver.contoso.com
```

Sie können auch der Exchange-Verwaltungskonsole verwenden, um Mitglieder zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie im Abschnitt "Hinzufügen von Mitgliedern zu einer Rollengruppe" in [Manage Role Group Members](#).

- In Exchange Online können Sie einen benutzerdefinierten Verwaltungsbereich, der für eDiscovery verwendet wird, nicht zum Durchsuchen inaktiver Postfächer verwenden. Der Grund dafür ist, dass das inaktive Postfach nicht Mitglied einer Verteilergruppe sein kann. Nehmen wir beispielsweise an, dass ein Benutzer Mitglied einer Verteilergruppe ist, die verwendet wurde, um einen benutzerdefinierten Verwaltungsbereich für eDiscovery zu erstellen. Der Benutzer verlässt die Organisation und sein Postfach wird deaktiviert (durch Aktivieren des Beweissicherungsverfahrens oder des Compliance-Archivs und Löschen des zugehörigen Office 365-Benutzerkontos). Daraufhin ist der Benutzer als Mitglied aus allen Verteilergruppen entfernt, einschließlich der Gruppe, die zur Erstellung des benutzerdefinierten Verwaltungsbereichs für eDiscovery verwendet wurde. Versucht ein Discovery-Manager (der Mitglied der Rollengruppe ist, die dem benutzerdefinierten Verwaltungsbereich zugeordnet ist), das inaktive Postfach zu durchsuchen, tritt ein Fehler auf. Um inaktive Postfächer durchsuchen zu können, muss der Discovery-Manager Mitglied der Rollengruppe "Discoveryverwaltung" oder einer anderen Rollengruppe sein, die über Berechtigungen zum Durchsuchen der gesamten Organisation verfügt.

Weitere Informationen zu inaktiven Postfächern finden Sie unter [Inactive mailboxes in Exchange Online](#).

# Verkleinern eines Discoverypostfachs in Exchange

18.12.2018 • 14 minutes to read

Haben Sie ein Discoverypostfach, das die Größenbeschränkung von 50 GB überschritten hat? Sie können dieses Problem beheben, indem Sie neue Discoverypostfächer erstellen und die Suchergebnisse aus dem großen Discoverypostfach in die neuen Postfächer kopieren.

## Aus welchen Gründen kann dies nötig sein?

In Exchange ist Server und Exchange Online, die maximale Größe der discoverypostfächer, die zum Speichern von Compliance-eDiscovery-Suchergebnissen verwendet werden, 50 GB. Bevor Sie die aktuelle maximale Größe konnten Sie erhöhen müssen discoverypostfächer wesentlich größer als 50 GB ergab das Speichercontingent auf mehr als 50 GB. Es gibt drei Probleme mit discoverypostfächer, die größer als 50 GB sind:

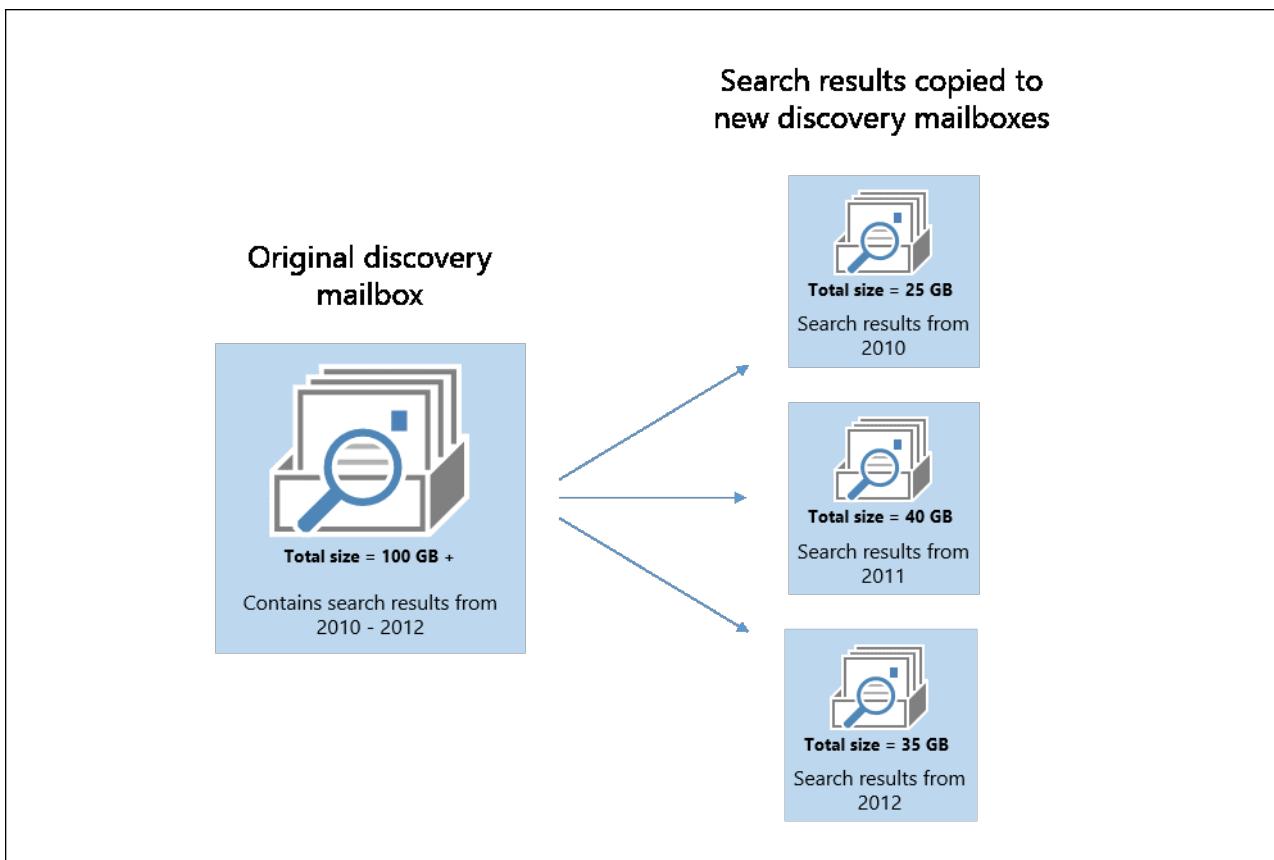
- Sie werden nicht unterstützt.
- Sie können nicht zu Office 365 migriert werden.
- Wenn sie discoverypostfächer in Exchange Server 2010 sind, können sie auf höhere Versionen aktualisiert werden.

## Der Prozess auf einen Blick

Hier ist eine kurze Übersicht über die erforderlichen Schritte für das Verkleinern eines Discoverypostfachs, das die Größenbeschränkung von 50 GB überschritten hat:

1. [Schritt 1: Erstellen von Discoverypostfächern](#) zusätzliche Discoverypostfächer, um die Suchergebnisse an diese zu verteilen.
2. [Schritt 2: Kopieren der Suchergebnisse an ein Discoverypostfach](#) die Suchergebnisse vom vorhandenen Discoverypostfach zu einem oder mehreren der neuen Discoverypostfächer.
3. [Schritt 3: Löschen von eDiscovery-Suchen](#) eDiscovery-Suchen aus dem ursprünglichen Discoverypostfach, um es zu verkleinern.

Mit der hier dargestellten Strategie werden die Suchergebnisse aus dem ursprünglichen Discoverypostfach in separate eDiscovery-Suchvorgänge gruppiert, die auf Datumsbereichen basieren. Auf diese Weise können Sie schnell viele Suchergebnisse in ein neues Discoverypostfach kopieren. Die folgende Grafik veranschaulicht diesen Ansatz.



## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen dieser Aufgabe: Die benötigte Zeit ist je nach Anzahl und Größe der Suchergebnisse, die an verschiedene Discoverypostfächer kopiert werden, unterschiedlich.
- Führen Sie den folgenden Befehl aus, um die Größe der Discoverypostfächer in Ihrer Organisation festzulegen.

```
Get-Mailbox -RecipientTypeDetails DiscoveryMailbox | Get-MailboxStatistics | Format-List
DisplayName,TotalItemSize
```

- Legen Sie fest, ob Sie einige oder alle Suchergebnisse aus dem Discoverypostfach behalten müssen, das die Größenbeschränkung von 50 GB überschritten hat. Befolgen Sie die Schritte in diesem Thema, um Suchergebnisse beizubehalten, indem Sie sie an ein anderes Discoverypostfach kopieren. Wenn Sie die Ergebnisse einer bestimmten eDiscovery-Suche nicht beibehalten müssen, können Sie die Suche löschen, wie in Schritt 3 erklärt. Durch das Löschen einer Suche werden die Suchergebnisse aus dem Discoverypostfach gelöscht.
- Wenn Sie keine der Suchergebnisse aus einem Discoverypostfach benötigen, das die Größenbeschränkung von 50 GB überschritten hat, können Sie es löschen. Wenn es sich um das Standarddiscoverypostfach handelt, das bei der Bereitstellung Ihrer Exchange-Organisation erstellt wurde, können Sie das Postfach erneut erstellen. Weitere Informationen finden Sie unter [Löschen und Neuerstellen des Standarddiscoverypostfachs in Exchange](#).
- Bei aktuellen Rechtsstreitigkeiten sollten Sie die Ergebnisse ausgewählter eDiscovery-Suchvorgänge in PST-Dateien exportieren. Damit bleiben die Ergebnisse aus einer bestimmten Suche intakt. Zusätzlich zu den PST-Dateien mit den Suchergebnissen wird auch ein Suchergebnisprotokoll (im CSV-Dateiformat) exportiert, das einen Eintrag für jede in den Suchergebnissen zurückgegebene Nachricht enthält. Jeder Eintrag in dieser Datei identifiziert das Quellpostfach, in dem sich die Nachricht befindet. Weitere Informationen finden Sie unter [Exportieren von eDiscovery-Suchergebnissen in eine PST-Datei](#).

Nachdem Sie die Suchergebnisse in PST-Dateien exportiert haben, müssen Sie Outlook verwenden, um sie bei Bedarf in ein neues Discoverypostfach zu importieren.

## Schritt 1: Erstellen von Discoverypostfächern

Der erste Schritt besteht darin, zusätzliche Discoverypostfächer zu erstellen, damit Sie die Suchergebnisse aus dem Discoverypostfach kopieren können, das die Größenbeschränkung überschritten hat. Legen Sie basierend auf der Größenbeschränkung für Discoverypostfächer von 50 GB fest, wie viele zusätzliche Discoverypostfächer Sie benötigen, und installieren Sie diese. Dann müssen Sie Benutzern oder Gruppen die erforderlichen Berechtigungen zum Öffnen dieser neuen Discoverypostfächer zuweisen.

1. Führen Sie den folgenden Befehl aus, um ein neues Discoverypostfach zu erstellen.

```
New-Mailbox -Name <discovery mailbox name> -Discovery
```

2. Führen Sie den folgenden Befehl aus, um einem Benutzer oder einer Gruppe Berechtigungen zum Öffnen des Discoverypostfachs und zum Anzeigen der Suchergebnisse zuzuweisen:

```
Add-MailboxPermission <discovery mailbox name> -User <name of user or group> -AccessRights FullAccess -InheritanceType all
```

## Schritt 2: Kopieren der Suchergebnisse an ein Discoverypostfach

Im nächsten Schritt wird das Cmdlet "**New-MailboxSearch**" mit um die Suchergebnisse aus vorhandenen discoverypostfach in ein neues discoverypostfach zu kopieren, die Sie im vorherigen Schritt erstellt haben. Dieses Verfahren verwendet die *StartDate* und *EndDate* -Parameter, um die Suchergebnisse in Batches zu begrenzen, die nicht größer als 50 GB sind. Dies erfordert möglicherweise einige Tests (durch die Suchergebnisse schätzen) auf Größe entsprechend der Suchergebnisse.

1. Führen Sie den folgenden Befehl aus, um eine neue eDiscovery-Suche zu erstellen.

```
New-MailboxSearch -Name "Search results from 2010" -SourceMailboxes "Discovery Search Mailbox" -StartDate "01/01/2010" -EndDate "12/31/2010" -TargetMailbox "Discovery Mailbox Backup 01" -EstimateOnly -StatusMailRecipients admin@contoso.com
```

<span data-ttu-id="bfd2a-152">In diesem Beispiel werden die folgenden Parameter verwendet:</span><span class="sxs-lookup"><span data-stu-id="bfd2a-152">This example uses the following parameters:</span></span>

- *Name*: dieser Parameter gibt den Namen der neuen eDiscovery-Suche. Da die Suche durch gesendete und empfangene Datumsangaben festgelegt ist, empfiehlt es sich, dass der Name der Suche den Datumsbereich enthält.
- *SourceMailboxes*: dieser Parameter gibt das standarddiscoverypostfach an. Sie können auch den Namen einer anderen discoverypostfachs angeben, die die maximale Größe überschritten hat.
- *StartDate* und *EndDate*: Diese Parameter geben den Datumsbereich der Suchergebnisse in das standarddiscoverypostfach zum Einschließen in den Suchergebnissen.

#### NOTE

Verwenden Sie für das Datum selbst dann das kurze Datumsformat mm/tt/jjjj, wenn bei den regionalen Einstellungen auf dem lokalen Computer ein anderes Format konfiguriert ist, z. B. tt.mm.jjjj. Verwenden Sie beispielsweise **03/01/2014**, um den 1. März 2014 anzugeben.

- **TargetMailbox:** dieser Parameter gibt an, dass die Suchergebnisse in das discoverypostfach mit dem Namen "Discovery Mailbox Backup 01" kopiert werden sollen.
  - **EstimateOnly:** Diese Option gibt an, dass nur eine Schätzung der Anzahl der Elemente, die zurückgegeben werden, bereitgestellt wird, wenn die Suche gestartet wird. Wenn Sie diese Option nicht angeben, werden Nachrichten in der Zielpostfach kopiert, wenn die Suche gestartet wird. Mit dieser Option können Sie die passen Sie die Datumsbereiche bei Bedarf zu erhöhen oder Verringern der Anzahl der Suchergebnisse.
  - **StatusMailRecipients:** dieser Parameter gibt an, dass die Statusnachricht an den angegebenen Empfänger gesendet werden soll.
2. Nachdem die Suche erstellt wurde, starten Sie ihn mithilfe der Exchange Online PowerShell oder der Exchange-Verwaltungskonsole (EAC).
- **Verwenden von Exchange Online PowerShell:** Führen Sie den folgenden Befehl zum Starten der Suche im vorherigen Schritt erstellt haben. Da die Option *EstimateOnly* enthalten ist, wenn die Suche erstellt wurde, wird nicht die Suchergebnisse in das zieldiscoverypostfach kopiert werden.

```
Start-MailboxSearch "Search results from 2010"
```

- **Mit der Exchange-Verwaltungskonsole:** Wechseln Sie zur **Verwaltung der Richtlinientreue > Compliance - eDiscovery und -Archiv**. Wählen Sie die Suche im vorherigen Schritt erstellt haben, klicken Sie auf **Suche** , und klicken Sie dann auf **Schätzung der Suchergebnisse**.
  - 3. Passen Sie bei Bedarf den Datumsbereich an, um die Menge der zurückgegebenen Suchergebnisse zu vergrößern oder zu verkleinern. Wenn Sie den Datumsbereich ändern, führen Sie die Suche erneut aus, um eine neue Schätzung der Ergebnisse zu erhalten. Ziehen Sie eine Änderung des Namens für die Suche in Betracht, um den neuen Datumsbereich darzustellen.
  - 4. Wenn Sie testen der Suche abgeschlossen haben, verwenden Sie Exchange Online PowerShell oder der Exchange-Verwaltungskonsole zum Kopieren von der Suchergebnissen auf das zieldiscoverypostfach.
- **Verwenden von Exchange Online PowerShell:** Führen Sie die folgenden Befehle aus, um die Suchergebnisse zu kopieren. Sie müssen die Option *EstimateOnly* entfernen, bevor Sie die Suchergebnisse kopieren können.

```
Set-MailboxSearch "Search results from 2010" -EstimateOnly $false
```

```
Start-MailboxSearch "Search results from 2010"
```

- **Mit der Exchange-Verwaltungskonsole:** Wechseln Sie zur **Verwaltung der Richtlinientreue > Compliance - eDiscovery und -Archiv**. Wählen Sie die Suche, klicken Sie auf **Suche** , und klicken Sie dann auf **Kopieren der Suchergebnisse**.

Weitere Informationen finden Sie unter [eDiscovery-Suchergebnisse in ein Discoverypostfach kopieren](#).

5. Wiederholen Sie die Schritte 1 bis 4, um neue Suchen für weitere Datumsbereiche zu erstellen. Schließen Sie

den Datumsbereich in den Namen der neuen Suchvorgänge ein, um den Bereich der Ergebnisse anzugeben. Verwenden Sie verschiedene Discoverypostfächer als Zielpostfach, um sicherzustellen, dass keins der Discoverypostfächer die Größenbeschränkung von 50 GB überschreitet.

## Schritt 3: Löschen von eDiscovery-Suchen

Nachdem Sie die Suchergebnisse aus dem ursprünglichen Discoverypostfach an ein anderes Discoverypostfach kopiert haben, können Sie die ursprünglichen eDiscovery-Suchen löschen. Durch das Löschen einer eDiscovery-Suche werden die Suchergebnisse aus dem Discoverypostfach gelöscht, in dem diese Suchergebnisse gespeichert werden.

Bevor Sie eine Suche löschen, können Sie den folgenden Befehl ausführen, um die Größe der Suchergebnisse, die an ein neues Discoverypostfach kopiert wurden, für alle Suchvorgänge in Ihrer Organisation zu ermitteln.

```
Get-MailboxSearch | Format-List Name,TargetMailbox,ResultSizeCopied
```

Exchange Online PowerShell oder der Exchange-Verwaltungskonsole können Sie um eine eDiscovery-Suche zu löschen.

- **Verwenden von Exchange Online PowerShell:** Führen Sie den folgenden Befehl aus.

```
Remove-MailboxSearch -Identity <name of search>
```

- **Mit der Exchange-Verwaltungskonsole:** Wechseln Sie zur **Verwaltung der Richtlinientreue > Compliance - eDiscovery und -Archiv**. Wählen Sie die Suche, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Nachdem Sie die eDiscovery-Suchen gelöscht haben, um die Ergebnisse aus dem Discoverypostfach zu löschen, in dem sie gespeichert waren, führen Sie den folgenden Befehl aus, um die Größe eines ausgewählten Discoverypostfachs anzuzeigen.

```
Get-Mailbox <name of discovery mailbox> | Get-MailboxStatistics | Format-List TotalItemSize
```

# Löschen und Neuerstellen des StandardDiscoverypostfachs in Exchange

18.12.2018 • 3 minutes to read

Exchange Online PowerShell können Sie das standardDiscoverypostfach zu löschen, neu zu erstellen und dann Berechtigungen zuweisen.

## Aus welchen Gründen kann dies nötig sein?

In Exchange ist Server und Exchange Online, die maximale Größe des standardDiscoverypostfachs 50 GB. Es wird verwendet, um Compliance-eDiscovery-Suchergebnisse zu speichern. Bevor Sie die maximale Größe geändert wurde, konnte Organisationen das Speichercontingent auf mehr als 50 GB erhöhen. Daher konnte discoverypostfächer auf mehr als 50 GB vergrößert werden. Es gibt drei Probleme mit einem standardDiscoverypostfach, die größer als 50 GB ist:

- Es wird nicht unterstützt.
- Es kann nicht zu Office 365 migriert werden.
- Wenn es das standardDiscoverypostfach in Exchange Server 2010 ist, kann es zu Exchange Server 2013 oder höher aktualisiert werden.

Wie Sie diese Probleme beheben, richtet sich danach, ob Sie die Suchergebnisse aus einem StandardDiscoverypostfach mit mehr als 50 GB speichern möchten.

MÖCHTEN SIE DIE SUCHERGEWINNISSE SPEICHERN?	AKTION...
Nein	Führen Sie die Schritte in diesem Abschnitt aus, um das StandardDiscoverypostfach zu löschen und anschließend neu zu erstellen.
Ja	Führen Sie die unter <a href="#">Verkleinern eines Discoverypostfachs in Exchange</a> beschriebenen Schritte aus.

## Mithilfe von Exchange Online PowerShell löschen und Neuerstellen des standardDiscoverypostfachs

### NOTE

Sie können das Exchange-Verwaltungskonsole (EAC) nicht verwenden, da Discoverypostfächer im EAC nicht angezeigt werden.

1. Führen Sie den folgenden Befehl aus, um das StandardDiscoverypostfach zu löschen.

```
Remove-Mailbox "DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}"
```

2. Geben Sie in der Meldung, in der aufgefordert werden, zu bestätigen, dass Sie das Postfach und das entsprechende Active Directory-Benutzerobjekt löschen möchten, Y ein, und drücken Sie die EINGABETASTE.

Wenn Sie im nächsten Schritt das Discoverypostfach erstellen, wird ein neues Benutzerobjekt in Active Directory erstellt.

3. Führen Sie den folgenden Befehl aus, um das Standarddiscoverypostfach neu zu erstellen.

```
New-Mailbox -Name "DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}" -Alias  
"DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}" -DisplayName "Discovery Search Mailbox" -  
Discovery
```

4. Führen Sie den folgenden Befehl aus, um die Berechtigungen der Rollengruppe "Discoveryverwaltung" zum Öffnen des Standarddiscoverypostfachs und Anzeigen der Suchergebnisse zuzuweisen.

```
Add-MailboxPermission "DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}" -User "Discovery  
Management" -AccessRights FullAccess -InheritanceType all
```

# Verhinderung von Datenverlust

18.12.2018 • 16 minutes to read

Enthält Informationen Sie zu DLP-Richtlinien im Exchange-Server und Exchange Online, einschließlich, was sie enthalten und wie sie zu testen. Sie lernen auch ein neues Feature in Exchange DLP kennen.

Die Verhinderung von Datenverlust (Data Loss Prevention, DLP) ist ein wichtiger Aspekt in Messagingsystemen von Unternehmen, da E-Mails in sehr hohem Maß in der geschäftskritischen Kommunikation verwendet werden, die häufig vertrauliche Daten umfasst. DLP-Funktionen vereinfachen die Verwaltung von vertraulichen Daten erheblich und tragen so dazu bei, die Anforderungen an die Richtlinientreue für solche Daten einzuhalten und die Verwendung dieser Daten in E-Mails zu verwalten, ohne die Produktivität der Benutzer einzuschränken. Sehen Sie sich das folgende Video an, um einen konzeptionellen Überblick über DLP zu erhalten.

DLP-Richtlinien sind einfache Pakete, die Gruppen von Bedingungen, enthalten die bestehen von Transportregeln, Aktionen und Ausnahmen, die Sie in der Exchange-Verwaltungskonsole (EAC) zu erstellen und aktivieren Sie dann auf Filter e-Mail-Nachrichten und Anlagen. Sie können eine DLP-Richtlinie zu erstellen, jedoch nicht aktiviert, es werden sollen. Dadurch können Sie ohne Beeinträchtigung der e-Mail-Fluss Ihrer Richtlinien zu testen. DLP-Richtlinien können die volle Leistungsfähigkeit vorhandene Transportregeln verwenden. Tatsächlich wurden eine Reihe von neuen Typen von Transportregeln in Microsoft Exchange Server und Exchange Online erstellt, um neue DLP-Funktion zu erreichen. Eine wichtige neue Feature von Transportregeln ist ein neuer Ansatz zum Klassifizieren von vertraulichen Informationen, der in der e-Mail-Fluss Verarbeitung integriert werden kann. Dieses neue DLP-Features führt Tiefe Content-Analyse über Schlüsselwort entspricht, Wörterbuch Übereinstimmungen, Auswertung für reguläre Ausdrücke und andere Inhalte Prüfung Inhalte zu erkennen, die Organisationseinheit DLP-Richtlinien verletzen. Weitere Informationen zu Transportregeln finden Sie unter [Transport Rules](#) (Exchange Server) oder [e-Mail-Flussregeln \(Transportregeln\)](#) in Exchange Online und [Integration von vertraulichen Informationen Regeln mit Transportregeln](#). Sie können auch die DLP-Richtlinien mithilfe von Exchange Online PowerShell-Cmdlets verwalten. Weitere Informationen zu und Richtlinientreue-Cmdlets finden Sie unter [Messaging Policy and Compliance Cmdlets](#).

Zusätzlich zu den anpassbaren DLP-Richtlinien selbst, können Sie auch e-Mail-Absender informieren, möglicherweise zu einer Ihrer Richtlinien verletzen – sogar, bevor er eine entsprechende Nachricht gesendet. Hierzu können Sie Richtlinientipps konfigurieren. Richtlinientipps ähneln e-Mail-Infos und können konfiguriert werden, um eine kurze Notiz im Microsoft Outlook 2013-Client darzustellen, die Informationen zu möglichen Verstöße an eine Person Erstellen einer Nachricht bereitstellt. In Exchange Online und Exchange Server werden auch Richtlinieninfos in Outlook Web App und OWA for Devices angezeigt. Weitere Informationen finden Sie unter [Tipps zu Richtlinien](#).

## NOTE

Exchange Online: DLP ist eine Premium-Funktion, die ein Exchange Online – Plan 2-Abonnement erforderlich sind. Weitere Informationen finden Sie unter [Exchange Online-Lizenzierung](#). > Exchange Server: DLP ist eine Premium-Funktion, die eine Exchange Enterprise Client Access License (CAL) erforderlich sind. Weitere Informationen zu Clientzugriffsliczenzen und Terminalserverlizenzerziehung finden Sie unter [Exchange Server-Lizenzierung](#). > **Exchange Enterprise CAL mit Diensten:** wird eine Notiz von Wenn Sie eine Exchange Enterprise CAL mit Diensten Kunden mit einer hybridbereitstellung sind, müssen Sie dabei einige Postfächer auf lokale und einige in Exchange Online Verhalten unterschieden. DLP-Richtlinien gelten in Exchange Online. Aus diesem Grund müssen von einem lokalen Benutzer an einen anderen lokalen Benutzer gesendete Nachrichten nicht DLP-Richtlinien angewendet, da die Nachricht nicht die lokale Infrastruktur verlassen.

Verwaltungsaufgaben im Zusammenhang mit Data Loss Prevention suchen? Finden Sie unter [DLP Procedures](#) (Exchange Server) oder [DLP-Prozeduren](#) (Exchange Online).

## Einrichten von Richtlinien zum Schutz vertraulicher Daten

Mit den Funktionen zur Verhinderung von Datenverlust können Sie verschiedene Kategorien vertraulicher Informationen ermitteln und überwachen, die Sie im Rahmen Ihrer Richtlinienbedingungen definiert haben, z. B. Personalausweis- oder Kreditkartennummern. Sie können entweder selbst benutzerdefinierte Richtlinien und Transportregeln erstellen oder die vordefinierten DLP-Richtlinienvorlagen verwenden, die von Microsoft für den schnellen Einstieg bereitgestellt werden. Weitere Informationen zu den integrierten Richtlinienvorlagen finden Sie unter [In Exchange bereitgestellte DLP-Richtlinienvorlagen](#). Eine Richtlinienvorlage umfasst eine Reihe von Bedingungen, Regeln und Aktionen, mit denen Sie eine DLP-Richtlinie zur Untersuchung von Nachrichten erstellen und speichern können. Bei den Richtlinienvorlagen handelt es sich um Modelle, aus denen Sie Regeln auswählen oder die Sie mit eigenen Regeln anpassen können, um eine Richtlinie zu erstellen, die Ihre Anforderungen an die Verhinderung von Datenverlust erfüllt.

Ihnen stehen drei verschiedene Methoden zur Verfügung, um mit der Verwendung von DLP-Richtlinien zu beginnen:

1. **Anwenden einer von Microsoft bereitgestellt wird, die vordefinierte Vorlage:** die schnellste Möglichkeit zur Verwendung von DLP-Richtlinien zum Erstellen und implementieren einer neuen Richtlinie mit einer Vorlage ist. Auf diese Weise erstellen einen neuen Satz von Regeln Ursprung den Aufwand. Sie müssen wissen, was der Daten, die überprüft werden soll, oder die Eingabe Compliance Regulierung Sie, Adresse versucht haben. Sie müssen auch Organisationen ungewöhnlich für die Verarbeitung dieser Daten kennen. Weitere Informationen finden Sie unter [DLP-Richtlinienvorlagen im Exchange bereitgestellt](#) und [Erstellen einer DLP-Richtlinie aus einer Vorlage](#).
2. **Eine vordefinierte Richtliniendatei außerhalb Ihrer Organisation zu importieren:** Importieren von Richtlinien, die bereits erstellt wurden außerhalb Ihrer messaging-Umgebung von unabhängigen Softwarehersteller. Auf diese Weise können Sie die DLP-Lösungen entsprechend Ihren geschäftsanforderungen erweitern. Weitere Informationen finden Sie unter [Richtlinien von Microsoft-Partnern, definieren Sie Ihre eigenen DLP-Vorlagen und Informationstypen](#) und [DLP-Richtlinie aus einer Datei importieren](#).
3. **Erstellen einer benutzerdefinierten Richtlinie ohne Überprüfung vor dem Umstände:** Ihres Unternehmens möglicherweise einen eigenen Anforderungen für die Überwachung bestimmter Types von Daten, die in einem messaging-System vorhanden sind bekannt. Sie können eine benutzerdefinierte Richtlinie vollständig auf eigene erstellen, um die Überprüfung und entsprechend Ihrer eigenen eindeutigen Meldungsdaten zu starten. Sie müssen wissen, die Anforderungen und Einschränkungen der Umgebung, in der die DLP-Richtlinie erzwungen wird, um eine solche eine benutzerdefinierte Richtlinie zu erstellen. Weitere Informationen finden Sie unter [Erstellen einer benutzerdefinierten DLP-Richtlinie](#).

Nachdem Sie eine Richtlinie hinzugefügt haben, können Sie die enthaltenen Regeln prüfen und ändern, die Richtlinie inaktiv setzen oder die Richtlinie vollständig entfernen. Die Verfahren für diese Aktionen werden im Thema [Manage DLP Policies](#) beschrieben.

## Arten von vertraulichen Informationen in DLP-Richtlinien

Beim Erstellen oder Ändern von DLP-Richtlinien können Sie Regeln, die Prüfungen für vertrauliche Informationen enthalten, einschließen. Die Arten der vertraulichen Informationen im Thema [Vertrauliche Informationen Typen Inventar](#) aufgelistet sind verfügbar in Ihrer Richtlinien verwendet werden. Die Bedingungen, die Sie in einer Richtlinie, beispielsweise wie oft, die etwas gefunden werden herstellen, bevor eine Aktion oder, was diese Aktion wird werden innerhalb Ihrer neuen benutzerdefinierten Richtlinien angepasst kann, um Ihre Richtlinie bestimmte Anforderungen erfüllen. Weitere Informationen zum Erstellen von DLP

Richtlinien finden Sie unter [Erstellen einer benutzerdefinierten DLP-Richtlinie](#). Weitere Informationen zu den vollständigen Suite Transportregeln finden Sie unter [Transport Rules](#) (Exchange Server) oder [E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#).

Zu erleichtern, stellen Sie vertrauliche Informationen Regeln verwenden, Microsoft gestellt hat Richtlinienvorlagen, die bereits einige der Arten der vertraulichen Informationen enthalten. Sie können nicht hinzufügen Bedingungen für alle Arten der vertraulichen Informationen hier aufgelisteten zu Richtlinienvorlagen jedoch, da die Vorlagen entwickelt wurden, um die meisten gängige Typen von Daten im Zusammenhang mit Compliance innerhalb Ihrer Organisation konzentrieren. Weitere Informationen zu den vorhandenen Vorlagen finden Sie unter [DLP-Richtlinienvorlagen im Exchange bereitgestellt](#). Sie können zahlreiche DLP-Richtlinien für Ihre Organisation erstellen und diese aktiviert, sodass viele verschiedene Arten von Informationen untersucht werden. Sie können auch eine DLP-Richtlinie erstellen, die nicht auf eine vorhandene Vorlage basiert. Zum Erstellen einer solchen Richtlinie zu beginnen, finden Sie unter [Erstellen einer benutzerdefinierten DLP-Richtlinie](#). Weitere Informationen zu den Arten von vertraulichen Informationen finden Sie unter [Vertrauliche Informationen Typen Inventar](#).

## Richtlinientipps zur Benachrichtigung der Benutzer über die Erwartungen hinsichtlich vertraulicher Inhalte

Sie können Richtlinientipp-Benachrichtigungen verwenden, um E-Mail-Absender über mögliche Probleme mit der Richtlinientreue zu informieren, während diese eine Nachricht erstellen. Wenn Sie einen Richtlinientipp in einer DLP-Richtlinie konfigurieren, wird die Benachrichtigung nur angezeigt, wenn ein Element in der E-Mail des Absenders die in der Richtlinie festgelegten Bedingungen erfüllt. Richtlinientipps ähneln den E-Mail-Infos, die in Microsoft Exchange 2010 eingeführt wurden. Weitere Informationen finden Sie unter [Richtlinientipps](#).

## Erkennen von vertraulichen Informationen und herkömmliche Nachrichtenklassifikation

Exchange Server und Exchange Online präsentieren eine neue Methode unterstützen Sie bei der Verwaltung von Nachrichten und Anlagen Daten im Vergleich zu herkömmliche Nachrichtenklassifikation an. Ein entscheidender Faktor in die Stärke des DLP-Lösung ist die Möglichkeit, ordnungsgemäß vertrauliche Inhalte zu identifizieren, die möglicherweise nur in der Organisation, gesetzlichen Anforderungen, Geografie oder anderen geschäftsanforderungen. Exchange Server erreichen dies durch verwenden eine neue Architektur für Tiefe Inhaltsanalyse gekoppelt mit Erkennung Kriterien, die Sie über Regeln in Ihrer DLP-Richtlinien festlegen. Nutzt die Hilfe zu Datenverlusten im Exchange Server auf den richtigen Satz von Regeln für vertrauliche Informationen so konfigurieren, dass sie ein hohes Maß an Schutz bei minimalem ungeeignetes Unterbrechung der Nachrichtenübermittlung mit falsch positive und negative bieten. Diese Arten von Regeln, bezeichnet die DLP-Informationen als Erkennung von vertraulichen Informationen, Funktion im Rahmen von Transportregeln, um DLP-Funktionen zu aktivieren angeboten.

Weitere Informationen zu diesen neuen Funktionen finden Sie unter [Integrating vertrauliche Informationen Regeln mit Transportregeln](#). Der herkömmliche Klassifizierung Nachrichtenfelder können weiterhin im Exchange auf Nachrichten angewendet und diese können kombiniert werden, mit dem neuen vertrauliche Informationen entweder innerhalb einer einzelnen DLP-Richtlinie oder gleichzeitig ausgeführt werden, damit sie ausgewertet werden unabhängig voneinander in Exchange. Weitere Informationen zu der Vorversionen Nachrichtenklassifikationen in Exchange 2010 finden Sie unter [Grundlegendes zu Nachrichtenklassifikationen](#).

## Informationen zu über DLP verarbeiteten Nachrichten

Exchange-Server zum Abrufen von Informationen zu Nachrichten und DLP-Richtlinie erkannte in Ihrer Umgebung finden Sie unter [DLP-Richtlinie Erkennung von Berichten](#) und [Vorfall Erstellen von Berichten für DLP-Richtlinie erkannte](#). Daten im Zusammenhang mit DLP-Erkennung ist sehr in Delivery Reports Nachricht Tracking Tool von Exchange Server integriert.

Weitere Informationen zu Exchange Online finden Sie unter [DLP policy detection reports](#) und [Create incident reports for DLP policy detection](#).

## Installationsvoraussetzungen

Damit ist der DLP-Features verwenden, müssen Sie über Exchange Server oder Exchange Online mit mindestens einem Absender Postfach konfiguriert. Verhinderung von Datenverlust ist eine Premium-Funktion, die ein Gruppenrichtlinien-Verwaltungskonsole (Enterprise Client Access License, CAL) erforderlich sind. Weitere Informationen zu den ersten Schritten mit Exchange Server finden Sie unter [Planning and Deployment](#). Weitere Informationen zu den ersten Schritten mit Exchange Online finden Sie unter [Exchange Online](#).

## Weitere Informationen

Exchange Server

- [Messagingrichtlinien und Richtlinientreue](#)
- [DLP Procedures](#)
- [DLP policy detection reports](#)
- [Messaging Policy and Compliance Cmdlets](#)

Exchange Online

- [Sicherheit und Richtlinientreue für Exchange Online](#)
- [DLP Procedures](#)
- [DLP policy detection reports](#)

# Anwenden von DLP-Regeln zur Auswertung von Nachrichten

18.12.2018 • 8 minutes to read

Sie können in Ihren Microsoft Exchange-Richtlinien zur Verhinderung von Datenverlust (Data Loss Prevention, DLP) Regeln für vertrauliche Informationen einrichten, um ganz spezielle Daten in E-Mail-Nachrichten zu erkennen. In diesem Thema wird erklärt, wie diese Regeln angewendet werden und wie die Auswertung der Nachrichten erfolgt. Sie können Workflowunterbrechungen für Ihre E-Mail-Benutzer vermeiden und ein hohes Maß an Präzision bei Ihren DLP-Erkennungen erzielen, wenn Sie wissen, wie Ihre Regeln durchgesetzt werden. Wir verwenden hier als Beispiel die von Microsoft bereitgestellte Regel für Kreditkarteninformationen. Wenn Sie eine Transportregel oder DLP-Richtlinie aktivieren, vergleicht der Exchange-Transportregel-Agent sämtliche von Ihren Benutzern gesendeten Nachrichten mit den von Ihnen erstellten Regelsätzen.

## Halten Sie sich genau an Ihre Anforderungen

Angenommen Sie, Sie müssen auf Kreditkarteninformationen in Nachrichten anzuwenden. Aktionen, die Sie durchführen, nachdem er gefunden wird, sind nicht Gegenstand dieses Themas, aber Sie können weitere Informationen zu, die in der [E-Mail-Fluss Regelaktionen in Exchange Online](#). Mit als die meisten Sicherheit wie möglich müssen Sie sicherstellen, dass was in einer Nachricht erkannt wird tatsächlich Kreditkartendaten und nicht etwas, das eine legitime Verwendung von Gruppen von Zahlen, die lediglich Kreditkartendaten ähneln werden konnte. beispielsweise einen Reservierung Code oder eine Fahrzeug-Identifizierungsnummer.

Zu diesem Zweck, wir machen deutlich, dass die folgende Informationen als Kreditkarte klassifiziert werden sollen:

Margie's Travel,

Ich habe aktuelle Kreditkarteninformationen von Spencer erhalten.

Spencer Badillo

Visa: 4111 1111 1111 1111

Gültig bis: 2/2012

Bitte aktualisiere sein Reiseprofil.

Wir müssen auch dafür sorgen, dass die folgenden Informationen nicht als Kreditkarte klassifiziert werden sollen:

Hallo Alex

Ich erwarte, dass in Hawaii zu sein. Meine buchen Code ist 1234 1234 1234 1234, und ich werde auf 3/2018 vorhanden sein.

Bezug Lisa

Der folgende XML-Codeausschnitt zeigt, wie die oben formulierten Bedürfnisse aktuell in einer Regel für

vertrauliche Informationen definiert sind. Diese Regel wird mit Exchange geliefert und ist in eine der DLP-Richtlinienvorlagen aus dem Lieferumfang eingebettet.

```
<Entity id="50842eb7-edc8-4019-85dd-5a5c1f2bb085" patternsProximity="300" recommendedConfidence="85">
  <Pattern confidenceLevel="85">
    <IdMatch idRef="Func_credit_card" />
    <Any minMatches="1">
      <Match idRef="Keyword_cc_verification" />
      <Match idRef="Keyword_cc_name" />
      <Match idRef="Func_expiration_date" />
    </Any>
  </Pattern>
</Entity>
```

### Mustervergleich in Ihrer Lösung

Die zuvor gezeigte XML-Regeldefinition enthält einen Mustervergleich, mit dem die Wahrscheinlichkeit steigt, dass die Regel nur die wichtigen Informationen erkennt und keine vagen, nur verwandten Informationen. Weitere Informationen zum XML-Schema für DLP-Regeln und -Vorlagen finden Sie unter [Define Your Own DLP Templates and Information Types](#).

In der Kreditkartenregel gibt es einen Abschnitt des XML-Codes für Muster, der einen primären Bezeichnervergleich und einige weitere bestätigende Nachweise enthält. Diese drei Anforderungen werden hier erklärt:

1. `<IdMatch idRef="Func_credit_card" />` - Dies erfordert eine Übereinstimmung einer Funktion mit dem Titel „Kreditkarte“, die intern definiert ist. Diese Funktion umfasst ein paar Überprüfungen, nämlich folgende:
  - 2. Sie vergleicht einen regulären Ausdruck - in diesem Fall mit 16 Ziffern -, die auch Variationen enthalten können, z. B. ein Trennzeichen, sodass auch **4111 1111 1111 1111** als Übereinstimmung gilt, oder einen Bindestrich, sodass auch **4111-1111-1111-1111** als Übereinstimmung gilt.
  - 3. Sie wertet die Prüfsumme nach dem Luhn-Algorithmus gegen die 26-stellige Nummer aus, um mit hoher Wahrscheinlichkeit zu gewährleisten, dass es sich um eine Kreditkartennummer handelt.
  - 4. Sie erfordert eine zwingende Übereinstimmung, und danach wird der bestätigende Nachweis ausgewertet.
5. `<Any minMatches="1">` - Dieser Abschnitt gibt an, dass das Vorhandensein von mindesten einem der folgenden Nachweiselemente erforderlich ist.
6. Der bestätigende Nachweis kann eine Übereinstimmung bei einem der folgenden drei sein:

```
<Match idRef="Keyword_cc_verification">
<Match idRef="Keyword_cc_name">
<Match idRef="Func_expiration_date">
```

Diese drei bedeuten ganz einfach eine Liste von Schlüsselwörtern für Kreditkarten, die Namen der Kreditkarten oder die Notwendigkeit eines Ablaufdatums. Das Ablaufdatum wird intern als eine weitere Funktion definiert und ausgewertet.

### Der Prozess des Auswertens von Inhalten in Bezug auf Regeln

Die hier gezeigten fünf Schritte repräsentieren Aktionen, die Exchange durchführt, um Ihre Regel mit E-Mails zu vergleichen. Für unser Beispiel mit der Kreditkartennummer werden die nachfolgend angegebenen Schritte durchgeführt.

SCHRITT	AKTION
1. Inhalt abrufen	Spencer Badillo Visa: 4111 1111 1111 1111 Gültig bis: 2/2012
2. Analyse regulärer Ausdrücke	4111 1111 1111 1111 -> eine 16-stellige Zahl wird erkannt
3. Funktionsanalyse	4111 1111 1111 1111 -> stimmt mit Prüfsumme überein 1234 1234 1234 1234 -> stimmt nicht überein
4. Zusätzlicher Nachweis	
	Das Schlüsselwort "Visa" ist der Zahl nahe. Ein regulärer Ausdruck für das Datum (2/2012) ist der Zahl nahe.
5. Erkenntnis	
	Es ist ein regulärer Ausdruck, der mit einer Prüfsumme übereinstimmt. Weitere Nachweise erhöhen das Vertrauen.

Durch die Art, wie diese Regel von Microsoft eingerichtet wurde, wird vorausgesetzt, dass bestätigende Nachweise wie z. B. Schlüsselwörter Bestandteil des Inhalts der E-Mail-Nachricht sind, damit die Regel eine Übereinstellung erkennt. Deshalb würde für den folgenden E-Mail-Inhalt nicht erkannt werden, dass er eine Kreditkartennummer enthält:

Margie's Travel,

Ich habe aktuelle Informationen von Spencer erhalten.

Spencer Burillo

4111 1111 1111 1111

Bitte aktualisiere sein Reiseprofil.

Sie können eine benutzerdefinierte Regel einsetzen, mit der ein Muster ohne zusätzliche Nachweise definiert wird, wie das im nächsten Beispiel gezeigt wird. Damit würden Meldungen erkannt werden, die nur die Kreditkartennummer enthält und keine weiteren Nachweise.

```
<Pattern confidenceLevel="85">
    <IdMatch idRef="Func_credit_card" />
</Pattern>
</Entity>
```

Abbildung der Kreditkarte in diesem Artikel kann auch andere vertrauliche Informationen Regeln erweitert werden. Um die vollständige Liste der von Microsoft bereitgestellten Regeln im Exchange angezeigt wird, verwenden Sie das Cmdlet [Get-ClassificationRuleCollection](#), im Exchange Online PowerShell auf folgende Weise:

```
$rule_collection = Get-ClassificationRuleCollection
```

```
$rule_collection[0].SerializedClassificationRuleCollection | Set-Content oob_classifications.xml -Encoding byte
```

## Weitere Informationen

[Verhinderung von Datenverlust](#)

[Nachrichtenflussregeln \(Transportregeln\) in Exchange Online](#)

[Exchange Online PowerShell](#)

# Integrieren von Regeln für vertrauliche Informationen in Transportregeln

18.12.2018 • 5 minutes to read

In Microsoft Exchange können Sie DLP-Richtlinien erstellen, die nicht nur Regeln für herkömmliche Nachrichtenklassifikationen und vorhandene Transportregeln enthalten, sondern diese Regeln zum Schutz vertraulicher Informationen in Nachrichten auch kombinieren. Das vorhandene Transportregelframework stellt zahlreiche Funktionen für die Definition von Nachrichtenrichtlinien bereit, die das gesamte Spektrum weicher bis harter Steuerungsmöglichkeiten abdecken. Beispiele sind:

- Begrenzen der Interaktionen zwischen Empfängern und Absendern, einschließlich Interaktionen zwischen einzelnen Abteilungen innerhalb einer Organisation.
- Anwenden separater Richtlinien für die Kommunikation innerhalb und außerhalb einer Organisation.
- Vermeiden des Ein- oder Ausgangs unangemessener Inhalte in die und aus einer Organisation.
- Filtern von vertraulichen Informationen.
- Nachverfolgen oder Archivieren von Nachrichten, die von bestimmten Einzelpersonen gesendet oder empfangen werden.
- Umleiten von eingehenden und ausgehenden Nachrichten für die Untersuchung vor der Zustellung.
- Anwenden von Haftungsausschlüssen auf Nachrichten während des Transports innerhalb der Organisation.

Transportregeln können Sie Textnachrichten Richtlinien auf e-Mail-Nachrichten anwenden dieser Ablauf über die Transportpipeline im Transportdienst auf Postfachservern und auf Edge-Transport-Servern. Diese Regeln ermöglichen Systemadministratoren zum Erzwingen von Messagingrichtlinien, Nachrichten sicherer, Hilfe zum Schutz von messaging-Systemen schützen und vor unbeabsichtigten Datenverlust vermeiden. Weitere Informationen zu Transportregeln finden Sie unter [Transport Rules \(Exchange Server 2016\)](#) oder [E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#).

## Regeln für vertrauliche Informationen im Transportregelframework

Vertrauliche Informationen Regeln mit Transport Rules Framework integriert sind, durch die Einführung einer Bedingung, die Sie anpassen können: , **wenn die Nachricht enthält... Vertrauliche Informationen**. Diese Bedingung kann mit einem oder mehreren Typen von vertraulichen Informationen konfiguriert werden, die in den Nachrichten enthalten sind. Wenn mehrere DLP-Richtlinien oder Regeln in einer Richtlinie mit dieser Bedingung konfiguriert werden, wird die Richtlinie oder Regel erfüllt, wenn eine der Bedingungen entsprechen. Exchange-Richtlinienregeln untersuchen, Betreff, Textkörper und alle Anlagen einer Nachricht. Wenn die Regel auf eine dieser Nachrichtenkomponenten entspricht, werden die Regelaktionen angewendet werden.

Die Bedingung vertrauliche Informationen kann mit der bereits vorhandene Transportregeln messaging Richtlinien definiert und kombiniert werden. Wenn kombiniert, die Bedingung wird in Verbindung mit anderen Regeln und die Semantik und bietet. Beispielsweise werden zwei unterschiedliche Bedingungen zusammen mit einer Anweisung und hinzugefügt, sodass beide müssen übereinstimmen, damit die Aktion angewendet werden soll. Keines der transportregelaktionen kann aufgrund Regeln mit den entsprechenden zu vertraulichen Informationen Typ konfiguriert werden. Mehrere verschiedene Dateitypen können durch den Transportregel-Agent, überprüft, die Nachrichten zum Erzwingen von Transportregeln überprüft. Weitere Informationen zu den unterstützten Dateitypen finden, finden Sie unter [File Types, dass werden unterstützt In Transportregeln](#)

(Exchange Server) oder [Verwenden von e-Mail-Flussregeln von Nachrichtenanlagen in Office 365](#) (Exchange Online).

Die Regeln können auch im Abschnitt mit den Ausnahmen einer Regeldefinition verwendet werden. Ihre Verwendung in der Ausnahmedefinition ist unabhängig von ihrer Verwendung als Bedingung innerhalb der Regel. Auf diese Weise können Sie flexibel Regeln mit der Bedingung definieren, wobei Sie verschiedene, als Teil der Bedingung anzuwendende Typen von Informationen sowie davon abweichende Typen von Informationen in der Bedingung angeben. Dies ermöglicht beispielsweise das Anwenden von Richtlinien, die mit bestimmten Regeln für herkömmliche Nachrichtenklassifikationen übereinstimmen, aber nicht mit anderen Typen vertraulicher Informationen, bevor Aktionen ausgeführt werden, die Sie innerhalb einer Richtlinie definieren.

## Weitere Informationen

[Verhinderung von Datenverlust](#)

[Vertrauliche Informationen Typen Inventar](#)

[Transportregeln Exchange Server 2016](#)

[E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#) Exchange Online

[Erstellen einer benutzerdefinierten DLP-Richtlinie](#)

# In Exchange bereitgestellte DLP-Richtlinienvorlagen

18.12.2018 • 12 minutes to read

In Microsoft Exchange Server und Exchange Online können Data Loss Prevention (DLP) Richtlinienvorlagen als Ausgangspunkt für die Erstellung von DLP-Richtlinien, mit denen Sie Ihre bestimmte behördlichen und geschäftlichen Richtlinie Bedürfnisse. Sie können die Vorlagen, um den spezifischen Bedürfnissen von Ihrer Organisation erfüllen ändern.

## Caution

Sie sollten Ihre DLP-Richtlinien im Testmodus aktivieren, bevor Sie sie in der Produktionsumgebung ausführen. Während dieser Tests wird empfohlen, dass Sie Beispielbenutzerpostfächer konfigurieren und Testnachrichten senden, die Ihre Testrichtlinien aufrufen, um die Ergebnisse zu bestätigen. > Die Nutzung dieser Richtlinien stellt nicht die Einhaltung von Bestimmungen sicher. Nehmen Sie nach Abschluss der Testphase die erforderlichen Konfigurationsänderungen in Exchange vor, damit die Übertragung von Informationen mit den Richtlinien Ihrer Organisation übereinstimmt. Ein Beispiel: Möglicherweise müssen Sie die TLS-Verschlüsselung für die Kommunikation mit bekannten Geschäftspartnern konfigurieren oder striktere Transportregelaktionen hinzufügen, etwa einen zusätzlichen Rechteschutz für Nachrichten, die einen bestimmten Datentyp enthalten.

## Für DLP verfügbare Vorlagen

Die folgende Tabelle enthält die DLP-Richtlinienvorlagen in Exchange. Weitere Informationen zum Anpassen dieser Vorlagen zum Erstellen von DLP-Richtlinien finden Sie unter [DLP-Richtlinien verwalten](#).

VORLAGE	BESCHREIBUNG
Finanzdaten - Australien	Erkennt Informationen, die in Australien üblicherweise als Finanzdaten betrachtet werden. Dazu zählen Informationen wie Kreditkarteninformationen und SWIFT-Codes.
Australien: Health Records Act (HRIP Act)	Erkennt Informationen, die in Australien üblicherweise unter den Health Records and Information Privacy (HRIP) Act fallen. Dazu zählen Informationen wie die Medical Account-Nummer und die Steuernummer (Tax File Number).
Personenbezogene Informationen (PII-Daten) - Australien	Erkennt Informationen, die in Australien üblicherweise als personenbezogene Informationen betrachtet werden. Dazu zählen Informationen wie Steuernummern (Tax File Number) und Führerscheinnummern.
Datenschutzgesetz - Australien	Erkennt Informationen, die in Australien üblicherweise unter das Datenschutzgesetz fallen. Dazu zählen Informationen wie Führerschein- und Reisepassnummern.
Finanzdaten - Kanada	Erkennt Informationen, die in Kanada üblicherweise als Finanzdaten betrachtet werden. Dazu zählen Informationen wie Bankkontonummern und Kreditkarteninformationen.
Health Information Act (HIA) - Kanada	Erkennt Informationen, die in Kanada unter den Health Information Act (HIA) für Alberta fallen. Dazu zählen Informationen wie Reisepassnummern und Gesundheitsinformationen.

VORLAGE	BESCHREIBUNG
Kanada: Personal Health Act (PHIPA) - Ontario	Erkennt Informationen, die in Kanada unter den Personal Health Information Protection Act (PHIPA) für Ontario fallen. Dazu zählen Informationen wie Reisepassnummern und Gesundheitsinformationen.
Personal Health Information Act (PHIA) - Manitoba, Kanada	Erkennt Informationen, die in Kanada unter den Personal Health Information Act (PHIA) für Manitoba fallen. Dazu zählen Informationen wie Gesundheitsinformationen.
Personal Information Protection Act (PIPA) - Kanada	Erkennt Informationen, die in Kanada unter den Personal Information Protection Act (PIPA) für British Columbia fallen. Dazu zählen Informationen wie Reisepassnummern und Gesundheitsinformationen.
Kanada: Personal Information Protection Act (PIPEDA)	Erkennt Informationen, die in Kanada unter den Personal Information Protection and Electronic Documents Act (PIPEDA) fallen. Dazu zählen Informationen wie Reisepassnummern und Gesundheitsinformationen.
Personenbezogene Informationen (PII-Daten) - Kanada	Erkennt Informationen, die in Kanada üblicherweise als personenbezogene Informationen betrachtet werden. Dazu zählen Informationen wie Health Identification-Nummern und Sozialversicherungsnummern.
Datenschutzgesetz - Frankreich	Erkennt Informationen, die in Frankreich üblicherweise unter das Datenschutzgesetz fallen. Dazu zählen Informationen wie die Nummer der Krankenversicherungskarte.
Finanzdaten - Frankreich	Erkennt Informationen, die in Frankreich üblicherweise als Finanzdaten betrachtet werden. Dazu zählen Informationen wie Kreditkarteninformationen, Kontoinformationen und Debitkartennummern.
Frankreich: Personenbezogene Informationen (PII-Daten)	Hilft bei der Erkennung von Informationen, die in Frankreich üblicherweise als personenbezogene Informationen betrachtet werden. Dazu zählen Informationen wie Reisepassnummern.
Finanzdaten - Deutschland	Erkennt Informationen, die in Deutschland üblicherweise als Finanzdaten betrachtet werden. Dazu zählen Informationen wie EU-Debitkartennummern.
Deutschland: Personenbezogene Informationen (PII-Daten)	Hilft bei der Erkennung von Informationen, die in Deutschland üblicherweise als personenbezogene Informationen betrachtet werden. Dazu zählen Informationen wie Führerschein- und Reisepassnummern.
Finanzdaten - Israel	Erkennt Informationen, die in Israel üblicherweise als Finanzdaten betrachtet werden. Dazu zählen Informationen wie Bankkontonummern und SWIFT-Codes.
Personenbezogene Informationen (PII-Daten) - Israel	Erkennt Informationen, die in Israel üblicherweise als personenbezogene Informationen betrachtet werden. Dazu zählen Informationen wie nationale IDs.

VORLAGE	BESCHREIBUNG
Datenschutzgesetz - Israel	Erkennt Informationen, die in Israel üblicherweise unter den Datenschutz fallen. Dazu zählen Informationen wie Bankkontonummern und internationale IDs.
Finanzdaten - Japan	Erkennt Informationen, die in Japan üblicherweise als Finanzdaten betrachtet werden. Dazu zählen Informationen wie Kreditkarteninformationen, Kontoinformationen und Debitkartennummern.
Japan: Personenbezogene Informationen (PII-Daten)	Hilft bei der Erkennung von Informationen, die in Japan üblicherweise als personenbezogene Informationen betrachtet werden. Dazu zählen Informationen wie Führerschein- und Reisepassnummern.
Schutz persönlicher Informationen - Japan	Erkennt Informationen, die in Japan unter den Schutz persönlicher Informationen fallen. Dazu zählen Informationen wie Melderegistrierungsnummern.
PCI Data Security Standard (PCI DSS)	Hilft bei der Erkennung von Informationen, die dem PCI Data Security Standard (PCI DSS) unterliegen. Dazu zählen Kredit- und Debitkartennummern.
Gesetz gegen Internetkriminalität - Saudi-Arabien	Erkennt Informationen, die in Saudi-Arabien üblicherweise unter das Gesetz gegen Internetkriminalität fallen. Dazu zählen Informationen wie internationale Bankkontonummern und SWIFT-Codes.
Finanzdaten - Saudi-Arabien	Erkennt Informationen, die in Saudi-Arabien üblicherweise als Finanzdaten betrachtet werden. Dazu zählen Informationen wie internationale Bankkontonummern und SWIFT-Codes.
Personenbezogene Informationen (PII-Daten) - Saudi-Arabien	Erkennt Informationen, die in Saudi-Arabien üblicherweise als personenbezogene Informationen betrachtet werden. Dazu zählen Informationen wie nationale IDs.
Access to Medical Reports Act – Vereinigtes Königreich	Erkennt Informationen, die im Vereinigten Königreich unter den Access to Medical Reports Act fallen. Dazu zählen Informationen wie Nummern des National Health Service.
Datenschutzgesetz – Vereinigtes Königreich	Erkennt Informationen, die im Vereinigten Königreich unter das Datenschutzgesetz fallen. Dazu zählen Informationen wie Sozialversicherungsnummern.
Finanzdaten – Vereinigtes Königreich	Erkennt Informationen, die im Vereinigten Königreich üblicherweise als Finanzdaten betrachtet werden. Dazu zählen Informationen wie Kreditkarteninformationen, Kontoinformationen und Debitkartennummern.
Online-Verhaltenskodex für persönliche Informationen – U.K.	Erkennt Informationen, die im Vereinigten Königreich unter den Online-Verhaltenskodex für persönliche Informationen (Personal Information Online Code of Practice) fallen. Dazu zählen Informationen wie Gesundheitsinformationen.

VORLAGE	BESCHREIBUNG
Vereinigtes Königreich: Personenbezogene Informationen (PII)	Hilft bei der Erkennung von Informationen, die im Vereinigten Königreich üblicherweise als personenbezogene Informationen betrachtet werden. Dazu zählen Informationen wie Führerschein- und Reisepassnummern.
Richtlinien für Datenschutz und elektronische Kommunikation – UK	Erkennt Informationen, die im Vereinigten Königreich unter die Richtlinien für Datenschutz und elektronische Kommunikation (Privacy and Electronic Communications Regulations) fallen. Dazu zählen Informationen wie Finanzdaten.
Verbraucherbestimmungen der Federal Trade Commission (FTC) - USA	Erkennt Informationen, die in den USA unter die Verbraucherbestimmungen der Federal Trade Commission (FTC) fallen. Dazu zählen Informationen wie Kreditkartennummern.
USA: Finanzdaten	Hilft bei der Erkennung von Informationen, die in den USA üblicherweise als Finanzinformationen gewertet werden. Dazu zählen Kreditkarteninformationen, Kontoangaben und Debitkartennummern.
Gramm-Leach-Bliley Act (GLBA) - USA	Hilft bei der Erkennung von Informationen, die dem Gramm-Leach-Bliley Act (GLBA) unterliegen. Dazu zählen Sozialversicherungs- oder Kreditkartennummern.
USA: Health Insurance Act (HIPAA)	Erkennt Informationen, die in den USA unter den Health Insurance Portability and Accountability Act (HIPAA) fallen. Dazu zählen Informationen wie Sozialversicherungsnummern und Finanzdaten.
Patriot Act - USA	Erkennt Informationen, die in den USA üblicherweise unter den Patriot Act fallen. Dazu zählen Informationen wie Kreditkartennummern und Steueridentifikationsnummern.
USA: Personenbezogene Informationen (PII-Daten)	Hilft bei der Erkennung von Informationen, die in den USA üblicherweise als personenbezogene Informationen betrachtet werden. Dazu zählen Informationen wie Sozialversicherungs- und Führerscheinnummern.
USA: State Breach Notification Laws	Erkennt Informationen, die in den USA unter die Gesetze zur Benachrichtigung bei Datenschutzverletzungen (State Breach Notification Laws) fallen. Dazu zählen Informationen wie Sozialversicherungs- und Kreditkartennummern.
USA: State Social Security Number Confidentiality Laws	Erkennt Informationen, die in den USA unter die Gesetze zur Vertraulichkeit von Sozialversicherungsnummern (State Social Security Number Confidentiality Laws) fallen. Dazu zählen Informationen wie Sozialversicherungsnummern.

## Weitere Informationen

[Verhinderung von Datenverlust](#)

[Erstellen einer DLP-Richtlinie aus einer Vorlage](#)

[Vertrauliche Informationen Typen Inventar](#)

# Erstellen einer DLP-Richtlinie aus einer Vorlage

18.12.2018 • 7 minutes to read

In Microsoft Exchange können Sie Vorlagen für Data Loss Prevention (DLP) zur Einhaltung die messaging und Richtlinientreue Anforderungen Ihrer Organisation. Diese Vorlagen enthalten vordefinierte Sätze von Regeln, mit denen Sie Nachrichtendaten verwalten, die mehrere gemeinsamen rechtlichen und behördlichen Vorschriften zugeordnet ist. Eine Liste aller von Microsoft bereitgestellten Vorlagen finden Sie unter [DLP-Richtlinienvorlagen im Exchange bereitgestellt](#). Beispiel DLP-Vorlagen, die bereitgestellt werden, können Sie verwalten helfen:

- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standard (PCI-DSS)
- United States Personally Identifiable Information (U.S. PII)

Sie können eine dieser DLP-Vorlagen anpassen oder verwenden sie als-ist. DLP-Richtlinienvorlagen werden auf der Basis Transportregeln erstellt, die neue Bedingungen oder Prädikate und Aktionen enthalten. DLP-Richtlinien den gesamten Bereich der traditionellen Transportregeln unterstützen, und Sie können zusätzlichen Regeln hinzufügen, nachdem eine DLP-Richtlinie eingerichtet wurde. Weitere Informationen zu Vorlagen für Benutzerrechterichtlinien finden Sie unter [DLP-Richtlinienvorlagen](#). Weitere Informationen zum Transport Rule-Funktionen finden Sie unter [Transport Rules](#) (Exchange Server 2016) oder [E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#). Nachdem Sie eine Richtlinie durchsetzen gestartet haben, können Sie dazu, wie Sie auf die Ergebnisse einzuhalten, überprüfen Sie die folgenden Themen erfahren:

Exchange Server: [DLP-Richtlinie Erkennung Management](#)

Exchange Online: [DLP policy detection reports](#)

**Caution**

Sie sollten Ihre DLP-Richtlinien im Testmodus aktivieren, bevor Sie sie in der Produktionsumgebung ausführen. Während dieser Tests wird empfohlen, dass Sie Beispielbenutzerpostfächer konfigurieren und Testnachrichten senden, die Ihre Testrichtlinien aufrufen, um die Ergebnisse zu bestätigen.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 30 Minuten
- Stellen Sie sicher, dass Exchange Server eingerichtet ist, wie unter [Planning and Deployment](#)beschrieben.
- Konfigurieren Sie sowohl Administrator- als auch Benutzerkonten innerhalb Ihrer Organisation, und überprüfen Sie den grundlegenden E-Mail-Fluss.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Verhinderung von Datenverlust (Data Loss Prevention, DLP)" im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#)
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Konfigurieren einer DLP-Richtlinie aus einer Vorlage mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Verhinderung von Datenverlust**, und klicken Sie dann auf **Hinzufügen**.

## NOTE

Sie können diese Aktion auch auswählen, wenn Sie auf den Pfeil neben der **Hinzufügen** Symbol und die Option **neue DLP-Richtlinie aus Vorlage** aus dem Dropdown-Menü.

2. Füllen Sie auf der Seite **Erstellen einer neuen DLP-Richtlinie aus einer Vorlage** die folgenden Felder aus:
3. **Name:** Fügen Sie einen Namen, die diese Richtlinie von anderen unterscheidet.
4. **Beschreibung:** eine optionale Beschreibung, die Zusammenfassung dieser Richtlinie hinzufügen.
5. **Wählen Sie eine Vorlage:** Wählen Sie die geeignete Vorlage mit dem Erstellen einer neuen Richtlinie beginnen.
6. **Weitere Optionen:** Wählen Sie den Modus oder Zustand. Die neue Richtlinie ist nicht vollständig aktiviert, bis Sie angeben, dass der Fall sein sollte. Der Standardmodus für eine Richtlinie ist Test wird ohne Benachrichtigungen.
7. Klicken Sie auf **Speichern**, um die Richtlinie zu erstellen.

## NOTE

Zusätzlich zu den Regeln innerhalb einer bestimmten Vorlage kann Ihre Organisation über eine zusätzliche erwartet wird oder Unternehmensrichtlinien, die auf regulierten Daten innerhalb Ihrer messaging-Umgebung anwenden. Exchange Server vereinfacht die Basisvorlage ändern, um Aktionen hinzufügen, damit Ihre Exchange-Messagingumgebung eigene Anforderungen erfüllt.

Sie können Richtlinien ändern, indem Sie die darin enthaltenen Regeln bearbeiten, sobald die Richtlinie in der Exchange Server-Umgebung gespeichert wurde. Tätigen bestimmte Personen aus einer Richtlinie ausgenommen oder senden eine Benachrichtigung und Nachrichtenübermittlung blockieren, wenn eine Nachricht gefunden werden kann, um vertrauliche Inhalte haben, kann eine Änderung der Beispiel-Regel enthalten. Weitere Informationen zum Bearbeiten von Richtlinien und Regeln finden Sie unter [DLP-Richtlinien verwalten](#).

Sie müssen Navigieren zu der bestimmten Richtlinie Regelsatz auf der Seite **Bearbeiten DLP-Richtlinie**, und verwenden Sie die verfügbaren Tools auf der Seite zum Ändern einer DLP-Richtlinie, die Sie bereits in Exchange Server erstellt haben.

Einige Richtlinien ermöglichen das Hinzufügen von Regeln, die RMS für Nachrichten aktivieren. Sie müssen RMS auf dem Exchange-Server konfigurieren, bevor Sie die Aktionen hinzufügen, um diese Art von Regeln zu verwenden.

Sie können für alle DLP-Richtlinien die Regeln, Aktionen, Ausnahmen und den Erzwingungszeitraum ändern und

angeben, ob weitere Regeln innerhalb der Richtlinie aktiviert werden sollen. Ferner können Sie benutzerdefinierte Bedingungen erstellen.

## Weitere Informationen

[Verhinderung von Datenverlust](#)

[DLP-Richtlinienvorlagen](#)

Mit einer benutzerdefinierten Richtlinie zur Verhinderung von Datenverlust (Data Loss Prevention, DLP) können Sie Bedingungen, Regeln und Aktionen einrichten, mit denen Sie bestimmte Anforderungen Ihrer Organisation erfüllen können, die von keiner der vorhandenen DLP-Vorlagen abgedeckt werden.

Die Regelbedingungen, die in eine einzelne Richtlinie zur Verfügung stehen enthalten alle herkömmlichen Transportregeln zusätzlich zu den Arten der vertraulichen Informationen präsentiert in [Vertrauliche Informationen Typen Inventar](#). Weitere Informationen zu Transportregeln finden Sie unter [Transport Rules](#) (Exchange 2016) oder [E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#).

**Caution**

Sie sollten Ihrer DLP-Richtlinien im Testmodus aktivieren, bevor sie in Ihrer produktionsumgebung ausführen. Während dieser Tests wird empfohlen, dass Sie Benutzerpostfächer Beispiel konfigurieren, und senden Sie Testnachrichten, die Ihrer Richtlinien Test aufrufen, um das Ergebnis zu bestätigen. Weitere Informationen zu testen finden Sie unter [Test Mail Flow Regel](#).

Weitere Verwaltungsaufgaben im Zusammenhang mit einer benutzerdefinierten DLP-Richtlinie zu erstellen finden Sie unter [DLP Procedures](#)(Exchange Server) oder [DLP Procedures](#) (Exchange Online).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 60 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Verhinderung von Datenverlust (Data Loss Prevention, DLP)" im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#).
- Um eine neue benutzerdefinierte DLP-Richtlinie zu erstellen, müssen Sie die installationsanweisungen für Exchange Server ausführen. Weitere Informationen zur Bereitstellung finden Sie unter [Planning and Deployment](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### NOTE

Aufgrund der Unterschiede in Kundenansprüche und Inhalte match Anforderungen, Microsoft Support kann bei der Bereitstellung von benutzerdefinierten Definitionen übereinstimmenden Inhalts nicht behilflich sein; definieren z. B. benutzerdefinierte Klassifikationen und/oder reguläre Muster ("RegEx"). Testen und Debuggen, Office 365-Kunden müssen für benutzerdefinierten Inhalt übereinstimmenden Entwicklung basieren auf dem internen IT-Ressourcen, oder Sie können eine externe consulting Ressource wie beispielsweise Microsoft Consulting Services (MCS). Support-Mitarbeiter können eingeschränkten Unterstützung für das Feature bereitstellen, jedoch nicht bereitstellen Garantien, dass alle benutzerdefinierter Inhalte übereinstimmenden Entwicklung Anforderungen oder Verpflichtungen des Kunden erfüllen wird. Als Beispiel für den Typ der Unterstützung der bereitgestellt werden kann, können Beispiel Muster für reguläre Ausdrücke zu Testzwecken bereitgestellt werden. Oder Unterstützung bei der Problembehandlung eines vorhandenen RegEx-Musters, die nicht wie erwartet mit einem einzelnen bestimmten Content Beispiel auslöst unterstützen kann.

Weitere Informationen über das .NET Regex-Modul die für die Verarbeitung von Text verwendet wird, finden Sie unter <https://docs.microsoft.com/dotnet/standard/base-types/regular-expressions>.

# Erstellen einer benutzerdefinierten DLP-Richtlinie

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen einer benutzerdefinierten DLP-Richtlinie ohne vorhandene Regeln mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue** > **Verhinderung von Datenverlust**. Alle vorhandenen Richtlinien, die Sie konfiguriert haben, werden in einer Liste angezeigt.
2. Klicken Sie auf den Pfeil neben der **Hinzufügen**  Symbol, und wählen Sie **neue benutzerdefinierte Richtlinie**.

### IMPORTANT

Wenn Sie auf **Hinzufügen** klicken  Symbol nicht auf den Pfeil, erstellen Sie eine neue Richtlinie auf einer Vorlage basiert. Weitere Informationen zur Verwendung von Vorlagen finden Sie unter [Erstellen einer DLP-Richtlinie aus einer Vorlage](#).

3. Füllen Sie auf der Seite **Neue benutzerdefinierte Richtlinie** die folgenden Felder aus:
4. **Name**: Fügen Sie einen Namen, die diese Richtlinie von anderen unterscheidet.
5. **Beschreibung**: eine optionale Beschreibung, die Zusammenfassung dieser Richtlinie hinzufügen.
6. **Wählen Sie einen Status**: Wählen Sie den Modus oder Status für diese Richtlinie. Die neue Richtlinie ist nicht vollständig aktiviert, bis Sie angeben, dass der Fall sein sollte. Der Standardmodus für eine Richtlinie ist Test wird ohne Benachrichtigungen.
7. Klicken Sie auf **Speichern**, um das Erstellen der Referenzinformationen der neuen Richtlinie zu beenden. Die Richtlinie wird der Liste der von Ihnen konfigurierten Richtlinien hinzugefügt, obwohl es noch keine Regeln oder Aktionen gibt, die mit dieser neuen benutzerdefinierten Richtlinie verknüpft sind.
8. Doppelklicken Sie auf die Richtlinie, die Sie gerade erstellt haben, oder wählen Sie sie aus, und klicken Sie auf **Bearbeiten** .
9. Klicken Sie auf der Seite **DLP-Richtlinie bearbeiten** auf **Regeln**.

Klicken Sie auf **Hinzufügen**  eine neue leere Regel hinzufügen. Sie können mithilfe von alle herkömmlichen Transportregeln zusätzlich zu den Arten der vertraulichen Informationen zu ermöglichen.

Damit Sie die Übersicht behalten, sollten Sie jedem Bestandteil Ihrer Richtlinie oder Regel einen eindeutigen Namen geben, wenn Sie eine eigene Zeichenfolge bereitstellen können. Es stehen Ihnen mehrere zusätzliche Optionen zur Verfügung:

10. Klicken Sie auf den Pfeil neben der **Hinzufügen**  Symbol, um eine Regel zur Benachrichtigung des Absenders oder das Hochladen von Außerkraftsetzungen hinzuzufügen.
11. Um eine Regel entfernen möchten, markieren Sie die Regel, und klicken Sie auf **Löschen** .

12. Klicken Sie auf **Weitere Optionen**  zusätzliche Bedingungen und Aktionen für diese Regel Time-Grenze Grenzen eines Erzwingung oder Effekte auf anderen Regeln in dieser Richtlinie einschließlich hinzufügen.
13. Klicken Sie auf **Speichern**, um die Bearbeitung der Richtlinie zu beenden und Ihre Änderungen zu speichern.

DLP-Richtlinienvorlagen sind ein des Features für Microsoft Exchange, die Ihnen helfen können entwerfen und ein robustes und Richtlinientreue System für die messaging-Umgebung anwenden. Weitere Informationen zu Compliance-Features finden Sie unter [Messaging Policy and Compliance](#) (Exchange 2016) oder [Sicherheit und Richtlinientreue für Exchange Online](#).

## Weitere Informationen

[Verhinderung von Datenverlust](#)

[Transportregeln Exchange 2016](#)

[E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#) Exchange Online

[Integrieren von Regeln für vertrauliche Informationen in Transportregeln](#)

# Richtlinientipps

18.12.2018 • 13 minutes to read

Sie helfen, Microsoft Outlook, Outlook Web App (OWA) und OWA für Geräte Ihrer Organisation zu verhindern, dass e-Mail-Benutzer am Senden von vertraulichen Informationen fälschlicherweise Erstellen von Data Loss Prevention (DLP)-Richtlinien, die Richtlinientipp-Benachrichtigung enthalten Nachrichten. Ähnlich wie bei e-Mail-Infos, die in Microsoft Exchange Server 2010 eingeführt wurden, werden Richtlinientipp-Benachrichtigung angezeigt, für die Benutzer in Outlook während sie eine e-Mail-Nachricht verfassen. Richtlinie Tipp Benachrichtigungen angezeigt nur wenn etwas über die e-Mail-Nachricht des Absenders scheint zu einer DLP-Richtlinie verletzen, die Sie eingerichtet haben und dass Richtlinie enthält eine Regel, um den Absender benachrichtigen, wenn die, die Sie einrichten erfüllt werden. Sehen Sie sich dieses Video an, um mehr zu erfahren.

Tipps zu Richtlinien für Ihr e-Mail-Absender angezeigt wird, müssen Ihre Regeln die Aktion **Absender mit Richtlinientipp benachrichtigen** enthalten. Sie können dies in der Regel-Editor aus der Exchange-Verwaltungskonsole hinzufügen. Weitere Informationen finden Sie unter [Verwalten von richtlinientipps](#).

Der Transportregel-Agent, der DLP-Richtlinien erzwingt, unterscheidet bei der Auswertung von Nachrichten und den in Ihren Richtlinien enthaltenen Bedingungen nicht zwischen E-Mail-Anlagen, Nachrichtentext oder Betreffzeile. Beispiel: Ein Benutzer erstellt eine E-Mail-Nachricht, die eine Kreditkartennummer im Nachrichtentext enthält. Anschließend versucht der Benutzer, die Nachricht an einen Empfänger außerhalb der Organisation zu senden. In einem solchen Fall kann dem Benutzer in Outlook oder Outlook Web App eine Richtlinientipp-Benachrichtigung angezeigt werden, in welcher der Benutzer an die in Ihrem Unternehmen geltenden Beschränkungen für die Weitergabe solcher Informationen erinnert wird. Diese Art der Benachrichtigung wird jedoch nur angezeigt, wenn Sie eine DLP-Richtlinie konfiguriert haben, mit der die beschriebenen Beispielhandlungen eingeschränkt werden - in diesem Fall das Hinzufügen eines externen E-Mail-Alias zur Kopfzeile einer Nachricht mit Kreditkarteninformationen. Es gibt zahlreiche verschiedene Bedingungen, Aktionen und Ausnahmen, die Sie beim Erstellen von DLP-Richtlinien auswählen können. Auf diese Weise können Sie die Richtlinien zur Verhinderung von Datenverlust in einer Weise anpassen, die genau auf die Anforderungen Ihres Unternehmens zugeschnitten ist.

Verwenden von Aktion Absender benachrichtigen oder eine Außerkraftsetzung Aktion innerhalb einer Regel jederzeit wird empfohlen, dass Sie die Bedingung, die die Nachricht gesendet wurde auch innerhalb Ihrer Organisation enthalten. Hierzu können Sie mit dem Gruppenrichtlinienobjekt-Regeleditor So fügen Sie die folgende Bedingung hinzu: **der Absender befindet... > innerhalb der Organisation**. Weitere Informationen zum Ändern der vorhandener DLP-Richtlinien unter [DLP-Richtlinien verwalten](#). Dies ist eine empfohlene optimale Methode, da die Aktion Absender benachrichtigen im Rahmen Ihres Unternehmens Message-Creation Erfahrung angewendet wird. Bezeichnet die Aktion Absender sind die Autoren von Nachrichten in Ihrem Unternehmen erläutert. Die Benutzerinteraktion präsentiert von Richtlinientipps kann nicht von den Benutzern für eingehende Nachrichten ergriffen werden und wird ignoriert, wenn der Absender außerhalb Ihrer Organisation befindet. Sie können DLP-Richtlinien zum Scannen eingehender Nachrichten, und führen Sie eine Vielzahl von Aktionen anwenden, jedoch nicht, wenn Sie dies tun, Aktion Absender benachrichtigen hinzufügen.

Wenn E-Mail-Absender in Ihrer Organisation beim Verfassen einer Nachricht mithilfe von Richtlinientipp-Benachrichtigungen in Echtzeit auf die in Ihrer Organisation geltenden Erwartungen und Standards hingewiesen werden, sind weniger Verstöße gegen Standards zu erwarten, die Ihre Organisation umsetzen möchte.

**NOTE**

- Exchange Online: DLP ist eine Premium-Funktion, die ein Exchange Online – Plan 2-Abonnement erforderlich sind. Weitere Informationen finden Sie unter [Exchange Online-Lizenzierung](#).
- Exchange Server: DLP ist eine Premium-Funktion, die eine Exchange Enterprise Client Access License (CAL) erforderlich sind. Weitere Informationen zu Clientzugriffslizenzen und Terminalserverlizenzerzung finden Sie unter [Exchange Server-Lizenzierung](#).
- Wenn Ihre Organisation Exchange Server oder Exchange Online verwendet wird, stehen Richtlinientipps Personen senden von e-Mail in Outlook 2013, Outlook Web App oder OWA for Devices. Wenn Ihre Organisation derzeit Exchange Server verwendet wird, sind Richtlinientipps nur zum Senden von e-Mail in Outlook 2013 Personen zur Verfügung.

## Standardtext für Richtlinientipps und Regeloptionen

Sie haben einen Bereich der möglichen Optionen, wenn Sie DLP-Richtlinien Benachrichtigungsregeln Absender hinzufügen. Beim Hinzufügen einer Regel zum Absender benachrichtigen, mit der **Absender mit Richtlinientipp benachrichtigen** -Aktion innerhalb einer DLP-Richtlinie, Sie können auswählen, wie restriktiv sein. In der folgenden Tabelle die Benachrichtigungsoptionen sind verfügbar. Allgemeine Informationen zur Bearbeitung von Richtlinien finden Sie unter [DLP-Richtlinien verwalten](#). Informationen zum Erstellen von Richtlinientipps finden Sie unter [Verwalten von richtlinientipps](#).

BENACHRICHTIGUNGSREGEL	BEDEUTUNG	STANDARDTEXT EINER RICHTLINIENTIPP-BENACHRICHTIGUNG, DIE BENUTZERN IN OUTLOOK ANGEZEIGT WIRD
<b>Nur benachrichtigen</b>	Ähnlich wie E-Mail-Infos erzeugt diese Einstellung eine Richtlinientipp-Informationsmeldung zu einer Richtlinienverletzung. Ein Absender kann über ein Optionsdialogfeld zu Richtlinientipps in Outlook die Anzeige dieser Art von Tipps verhindern.	Diese Nachricht enthält möglicherweise vertrauliche Inhalte. Alle Empfänger müssen autorisiert sein, diese Inhalte zu empfangen.
<b>Nachricht zurückweisen</b>	Die Nachricht wird erst zugestellt, wenn die Bedingung nicht länger erfüllt ist. Der Absender kann über eine bereitgestellte Option angeben, dass die E-Mail-Nachricht keine vertraulichen Inhalte umfasst. Dies wird auch als Außerkraftsetzung eines falsch positiven Ergebnisses bezeichnet. Wenn der Benutzer dies angibt, lässt Outlook es zu, dass die Nachricht den Postausgang verlässt, damit der Benutzerbericht überprüft werden kann, Exchange verhindert jedoch, dass die Nachricht gesendet wird.	Diese Nachricht enthält möglicherweise vertrauliche Inhalte. Ihre Organisation lässt das Senden dieser Nachricht erst zu, wenn dieser Inhalt entfernt wurde.

BENACHRICHTIGUNGSREGEL	BEDEUTUNG	STANDARDTEXT EINER RICHTLINIENTIPP-BENACHRICHTIGUNG, DIE BENUTZERN IN OUTLOOK ANGEZEIGT WIRD
<b>Zurückweisen, sofern keine Außerkraftsetzung als falsch positiv vorliegt</b>	Das Ergebnis dieser Benachrichtigungsregel ähnelt dem der Benachrichtigungsregel <b>Nachricht zurückweisen</b> . Wenn Sie jedoch diese Option auswählen, lässt Exchange das Senden der Nachricht an den beabsichtigten Empfänger zu, statt die Nachricht zu blockieren.	<b>Bevor der Absender eine Option zum Überschreiben auswählt:</b> Diese Meldung kann vertrauliche Inhalte enthalten. Der Organisation werden nicht zulässig, diese Nachricht gesendet werden, bis dieser Inhalt entfernt wird. <b>Nach dem Absender wählt eine Option für die Außerkraftsetzung:</b> Ihr Feedback wird an den Administrator gesendet werden, wenn die Nachricht gesendet wird.
<b>Zurückweisen, sofern keine implizite Außerkraftsetzung vorliegt</b>	Die Nachricht wird erst zugestellt, wenn die Bedingung nicht länger erfüllt ist oder der Absender eine Außerkraftsetzung auswählt. Dem Absender wird eine Option angezeigt, die das Außerkraftsetzen der Richtlinie ermöglicht.	<b>Bevor der Absender eine Option zum Überschreiben auswählt:</b> Diese Meldung kann vertrauliche Inhalte enthalten. Der Organisation werden nicht zulässig, diese Nachricht gesendet werden, bis dieser Inhalt entfernt wird. <b>Nach dem Absender wählt eine Option für die Außerkraftsetzung:</b> Sie haben Ihrer Organisation geltenden Richtlinien für vertrauliche Inhalte in dieser Nachricht überschrieben. Ihre Aktion wird von Ihrer Organisation gilt, überwacht werden.
<b>Ablehnen, sofern keine explizite Außerkraftsetzung vorliegt</b>	Das Ergebnis dieser Benachrichtigungsregel ähnelt dem der Benachrichtigungsregel <b>Zurückweisen, sofern keine implizite Außerkraftsetzung vorliegt</b> , in diesem Fall müssen die Absender jedoch eine Begründung für die Richtlinienaußerkraftsetzung angeben.	<b>Bevor der Absender eine Option zum Überschreiben auswählt:</b> Diese Meldung kann vertrauliche Inhalte enthalten. Der Organisation werden nicht zulässig, diese Nachricht gesendet werden, bis dieser Inhalt entfernt wird. <b>Nach dem Absender wählt eine Option für die Außerkraftsetzung:</b> Sie haben Ihrer Organisation geltenden Richtlinien für vertrauliche Inhalte in dieser Nachricht überschrieben. Ihre Aktion wird von Ihrer Organisation gilt, überwacht werden.

## Anpassen der Richtlinientipp-Benachrichtigungen

Wählen Sie zum Anpassen des Texts einer Richtlinientipp-Benachrichtigung, die E-Mail-Absender in ihrem E-Mail-Programm sehen, auf der Seite „Verhinderung von Datenverlust“ die Option **Richtlinientipps verwalten** aus. Damit Ihr benutzerdefinierter Text angezeigt wird, muss eine DLP-Richtlinie die Aktion **Absender mit Richtlinientipp benachrichtigen** enthalten. Fügen Sie die Aktion mithilfe des DLP-Regel-Editors einer Regel hinzu.

Verfahren zur Erläuterung der Erstellung eigener Richtlinientipps finden Sie unter [Richtlinientipps verwalten](#). Der benutzerdefinierte Text, den Sie erstellen, kann den in der vorherigen Tabelle gezeigten Standardtext ersetzen.

AKTIONEN UND EINSTELLUNGEN FÜR RICHTLINIENTIPP-BENACHRICHTIGUNGEN	BEDEUTUNG
<b>Absender benachrichtigen</b>	Der Text wird nur angezeigt, wenn eine Aktion <b>Absender benachrichtigen, aber Senden zulassen</b> initiiert wird.
<b>Außenkraftsetzen durch Absender zulassen</b>	Der Text wird nur angezeigt, wenn folgende Aktionen initiiert werden: <b>Nachricht blockieren, wenn es sich nicht um ein falsch positives Ergebnis handelt, Nachricht blockieren, aber Außenkraftsetzen und Senden durch Absender zulassen.</b>
<b>Nachricht blockieren</b>	Dieser Text wird nur angezeigt, wenn eine Aktion <b>Nachricht blockieren</b> initiiert wird.
<b>Link zur URL zur Richtlinientreue</b>	Die Compliance-URL ist ein Link zu einer Webseite, auf der Sie Ihre Compliance- und Außenkraftsetzungsrichtlinien erklären können. Dieser Link wird im Richtlinientipp angezeigt, wenn ein Benutzer klickt auf den Link <b>Weitere Details</b> klickt.

## Weitere Informationen

[Verhinderung von Datenverlust](#)

[Verwalten von DLP-Richtlinien](#)

[Richtlinientipps verwalten](#)

# Richtlinientipps verwalten

18.12.2018 • 17 minutes to read

Richtlinientipps sind informative Hinweise, die E-Mail-Absendern beim Verfassen einer Nachricht angezeigt werden. Der Zweck von Richtlinientipps ist es, Benutzern zu vermitteln, dass sie möglicherweise Unternehmenspraktiken oder -richtlinien verletzen, die Sie mit den von Ihnen eingerichteten DLP-Richtlinien (Data Loss Prevention, Verhinderung von Datenverlust) durchsetzen möchten. Die folgenden Verfahren helfen Ihnen, mit dem Einsatz von Richtlinientipps zu beginnen. Schauen Sie dieses Video, um mehr zu erfahren.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 30 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Verhinderung von Datenverlust (Data Loss Prevention, DLP)" im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#).
- Richtlinientipps werden E-Mail-Absendern angezeigt, wenn die folgenden Bedingungen erfüllt sind:
  1. Das Clientprogramm für Nachrichten des Absenders ist Microsoft Outlook 2013. Wenn in Ihrer Organisation Exchange 2013 SP1 bereitgestellt wird oder Exchange Online zum Einsatz kommt, werden Richtlinientipps sowohl in Outlook Web App als auch in OWA für Geräte angezeigt.
  2. Eine Transportregel ist vorhanden, die Benachrichtigungen zu Richtlinientipps aufruft. Sie können eine solche Transportregel erstellen, indem Sie eine DLP-Richtlinie konfigurieren, die die Aktion **Absender mit Richtlinientipp benachrichtigen** enthält.
  3. Der Inhalt eines Nachrichtenkopfs, eines Nachrichtentexts oder einer Nachrichtenanlage, der bzw. die vom Transport-Agent überprüft wird, erfüllt die Bedingungen, die in den DLP-Richtlinien oder -Regeln festgelegt sind, die auch Benachrichtigungsregeln für Richtlinientipps enthalten. Der Richtlinientipp wird also Endbenutzern nur angezeigt, wenn sie etwas tun, das zum Auslösen der zughörigen Regel führt.
- Der standardmäßige Benachrichtigungstext für Richtlinientipps, der im System implementiert ist, wird angezeigt, wenn Sie nicht mit dem Feature für die Einstellungen von Richtlinientipps den Text von Richtlinientipps anpassen. Weitere Informationen zum Standardtext finden Sie unter [Richtlinientipps](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen oder Ändern eines nur als Benachrichtigung dienenden Richtlinientipps

Dieses Verfahren führt zu einer Informationszwecken Richtlinieninfo an eine e-Mail-Absender angezeigt wird,

wenn die einer bestimmten Regel erfüllt werden. In Microsoft Outlook kann der Absender verhindern, dass dieser Tipp mithilfe einer Richtlinientipp Optionsdialogfeld angezeigt. Um benutzerdefinierte Text für Richtlinientipps zu konfigurieren, finden Sie unter **Erstellen benutzerdefinierter Benachrichtigungstext** weiter unten in diesem Artikel.

#### Konfigurieren von nur als Benachrichtigung dienenden Richtlinientipps mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Verhinderung von Datenverlust**.
  2. Doppelklicken Sie auf eine der Richtlinien, die in der Richtlinienliste oder markieren Sie ein Element, und wählen Sie **Bearbeiten**.
  3. Wählen Sie auf der Seite **DLP-Richtlinie bearbeiten** die Option **Regeln**.
  4. Klicken Sie zum Hinzufügen von Richtlinientipps zu einer vorhandenen Regel markieren Sie die Regel, und wählen Sie **Bearbeiten**.
- Wählen Sie **Hinzufügen** aus, um eine neue leere Regel hinzuzufügen, die Sie vollständig anpassen können, und wählen Sie dann auf **neue Regel erstellen**.
5. Wählen Sie unter **Diese Regel anwenden** die Option **Wenn die Nachricht vertrauliche Informationen enthält**. Diese Bedingung ist erforderlich.
  6. Wählen Sie **Hinzufügen**, wählen Sie die Arten der vertraulichen Informationen, wählen Sie **Hinzufügen**, wählen Sie **OK** aus und wählen Sie dann auf **OK**.
  7. Wählen Sie im Feld **Folgendes ausführen** die Option **Absender mit Richtlinientipp benachrichtigen**, wählen Sie dann eine Option aus der Dropdownliste zum **Auswählen, ob die Nachricht blockiert ist oder gesendet werden kann** aus, und wählen Sie dann **OK**.
  8. Wenn Sie weitere Bedingungen oder Aktionen hinzufügen möchten, wählen Sie unten im Fenster **Weitere Optionen**.

#### NOTE

Es können nur die folgenden Bedingungen verwendet werden: > **SentTo (Der Empfänger ist)** > **SentToScope (Der Empfänger befindet sich)** > **From (Der Absender ist)** > **FromMemberOf (Der Absender ist Mitglied von)** > **FromScope (Der Absender befindet sich in)** > Die folgenden Aktionen können nicht verwendet werden:  
> **RejectMessageReasonText (Nachricht ablehnen und Erklärung einschließen)** >  
**RejectMessageEnhancedStatusCode (Nachricht ablehnen mit erweitertem Statuscode)** > **DeletedMessage (Löschen der Nachricht ohne Benachrichtigung)**

9. Wählen Sie in der Liste **Wählen Sie einen Modus für diese Regel** aus, ob die Regel erzwungen werden soll. Es wird empfohlen, zuerst Testen der Regel.
10. Wählen Sie **Speichern**, um die Bearbeitung der Regel zu beenden und Ihre Änderungen zu speichern.

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie folgende Schritt aus, um zu überprüfen, ob Sie erfolgreich einen Richtlinientipp erstellt haben, mit dem ein Absender nur informiert wird:

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Verhinderung von Datenverlust**.
2. Wählen Sie die Richtlinie aus, von der Sie erwarten, dass sie eine Benachrichtigung enthält.
3. Wählen Sie **Bearbeiten** und dann **Regeln**.

4. Wählen Sie die Regel aus, von der Sie erwarten, dass sie eine Benachrichtigung enthält.
5. Überprüfen Sie, ob die Aktion **Absender benachrichtigen** im unteren Teil der Regelzusammenfassung angezeigt wird.

## Erstellen oder Ändern eines Richtlinientipps zum Blockieren von Nachrichten

Dieses Verfahren Ergebnisse in ein Richtlinientipp angezeigt wird, an eine e-Mail-Absender, die eine Meldung weist darauf hin abgelehnt, und es wird nicht übermittelt werden, bis die problematische Bedingung nicht mehr vorhanden ist. Der Absender wird bereitgestellt, mit der Option um anzugeben, dass ihre e-Mail-Nachricht nicht die problematische Bedingung enthält. Dies ist auch bekannt als eine falsch Positive überschreiben. Wenn der Absender angegeben, kann die Nachricht im Ordner Postausgang verlassen, und des Benutzers Bericht überwacht werden kann. Allerdings blockiert Exchange die Nachricht gesendet werden.

### Konfigurieren von Richtlinientipps zum Blockieren von Nachrichten mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Verhinderung von Datenverlust**.
2. Doppelklicken Sie auf eine der Richtlinien, die in der Richtlinienliste oder markieren Sie ein Element, und wählen Sie **Bearbeiten**.
3. Wählen Sie auf der Seite **DLP-Richtlinie bearbeiten** die Option **Regeln**.
4. Klicken Sie zum Hinzufügen von Richtlinientipps zu einer vorhandenen Regel markieren Sie die Regel, und wählen Sie **Bearbeiten**.
5. Wählen Sie **Hinzufügen** aus, um eine neue leere Regel hinzuzufügen, die Sie vollständig anpassen können,
6. Um eine Aktion hinzuzufügen, die ein Richtlinientipp angezeigt wird, wählen Sie **Weitere Optionen**, und wählen Sie dann die Schaltfläche **Aktion hinzufügen** aus.
7. Wählen Sie in der Dropdownliste **Absender mit Richtlinientipp benachrichtigen** aus, und wählen Sie dann **Nachricht blockieren** aus.
8. Wählen Sie **OK** und dann **Speichern**, um die Bearbeitung der Regel zu beenden und Ihre Änderungen zu speichern.

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie folgende Schritte aus, um zu überprüfen, ob Sie erfolgreich einen Richtlinientipp zum Ablehnen von Nachrichten erstellt haben:

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Verhinderung von Datenverlust**.
2. Wählen Sie einmal aus, um die Richtlinie zu markieren, von der Sie annehmen, dass sie eine Benachrichtigungsmeldung enthält.
3. Wählen Sie **Bearbeiten** und dann **Regeln**.
4. Wählen Sie einmal aus, um die Regel zu markieren, von der Sie annehmen, dass sie eine Benachrichtigungsmeldung enthält.
5. Überprüfen Sie, ob die Aktion **Absender benachrichtigen, dass die Nachricht nicht gesendet werden kann** im unteren Teil der Regelzusammenfassung angezeigt wird.

# Erstellen oder Ändern eines Richtlinientipps zum Blockieren von Nachrichten, sofern keine Außerkraftsetzung erfolgt

Es gibt vier Optionen für Richtlinientipps, mit denen Nachrichten abgelehnt werden können oder mit denen verhindert werden kann, dass Nachrichten den Postausgang des Absenders verlassen. Weitere Informationen zu diesen Optionen finden Sie unter [Richtlinientipps](#).

## Konfigurieren von Richtlinientipps zum Blockieren von Nachrichten, sofern keine Außerkraftsetzung erfolgt, mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Verhinderung von Datenverlust**.
  2. Double-Wert auswählen eine der Richtlinien, die in der Richtlinienliste oder markieren Sie ein Element, und wählen Sie **Bearbeiten** .
  3. Wählen Sie auf der Seite **DLP-Richtlinie bearbeiten** die Option **Regeln**.
  4. Klicken Sie zum Hinzufügen von Richtlinientipps zu einer vorhandenen Regel markieren Sie die Regel, und wählen Sie **Bearbeiten** .
- Wählen Sie **Hinzufügen** aus, um eine neue leere Regel hinzuzufügen, die Sie vollständig anpassen können,  und wählen Sie dann auf **Weitere Optionen**.
5. Zum Hinzufügen einer Aktion, durch die ein Richtlinientipp angezeigt wird, wählen Sie die Schaltfläche **Aktion hinzufügen**.
  6. Wählen Sie in der Dropdownliste **Absender mit Richtlinientipp benachrichtigen** aus, und wählen Sie dann **Die Nachricht blockieren, dem Absender aber Außerkraftsetzen und Senden gestatten** aus.
  7. Wählen Sie **OK** und dann **Speichern**, um die Bearbeitung der Regel zu beenden und Ihre Änderungen zu speichern.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie folgende Schritte aus, um zu überprüfen, ob Sie erfolgreich einen Richtlinientipp zum Ablehnen von Nachrichten, sofern keine Außerkraftsetzung erfolgt, erstellt haben:

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Verhinderung von Datenverlust**.
2. Wählen Sie einmal aus, um die Richtlinie zu markieren, von der Sie annehmen, dass sie eine Benachrichtigungsmeldung enthält.
3. Wählen Sie **Bearbeiten**  und dann **Regeln**.
4. Wählen Sie einmal aus, um die Regel zu markieren, von der Sie annehmen, dass sie eine Benachrichtigungsmeldung enthält.
5. Überprüfen Sie, ob die Aktion **Die Nachricht blockieren, dem Absender aber Außerkraftsetzen und Senden gestatten** im unteren Teil der Regelzusammenfassung angezeigt wird.

# Erstellen von benutzerdefiniertem Benachrichtigungstext für Richtlinientipps

Mithilfe dieses optionalen Verfahrens können Sie den Benachrichtigungstext für Richtlinientipps anpassen, der E-Mail-Absendern in ihrem E-Mail-Programm angezeigt wird. Wenn Sie dieses Verfahren durchführen, wird der benutzerdefinierte Benachrichtigungstext für Richtlinientipps erst angezeigt, wenn Sie zudem eine DLP-Richtlinienregel mit einer Aktion konfigurieren, die die Anzeige der Benachrichtigung auslöst. Bedenken Sie, dass

es standardmäßige Systembenachrichtigungen für Richtlinientipps gibt, die angezeigt werden können, wenn Sie den Benachrichtigungstext für Richtlinientipps nicht anpassen. Weitere Informationen zum Standardtext finden Sie unter [Richtlinientipps](#).

## **Erstellen und Verwalten von benutzerdefiniertem Benachrichtigungstext für Richtlinientipps mithilfe der Exchange-Verwaltungskonsole**

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Verhinderung von Datenverlust**.
2. Wählen Sie **Einstellungen für Richtlinientipps**.
3. Wählen Sie zum Hinzufügen eines neuen Richtlinientipps mit Ihrer eigenen benutzerdefinierten Meldung **Hinzufügen**. Weitere Informationen zu den verfügbaren Optionen Aktion finden Sie unter [Tipps zu Richtlinien](#).  
Um einen vorhandenen Richtlinientipp zu ändern, markieren Sie den Tipp, und wählen Sie **Bearbeiten**
- Um einen vorhandenen Richtlinientipp zu löschen, markieren Sie es, und wählen Sie **Löschen** und bestätigen Sie die Aktion.
4. Wählen Sie **Speichern**, um die Bearbeitung des Richtlinientipps zu beenden und Ihre Änderungen zu speichern.
5. Wählen Sie **Schließen**, um die Verwaltung der Richtlinientipps zu beenden und die Änderungen zu speichern.

## **Verwenden Sie zum Erstellen von benutzerdefinierten Benachrichtigungstext Exchange Online PowerShell**

Im folgenden Beispiel wird ein neuer englischer Richtlinientipp erstellt, der das Senden einer Nachricht verhindert. Der Text dieser benutzerdefinierten Richtlinieninfo wird in den folgenden Wert geändert: "This message appears to contain restricted content and will not be delivered."

```
New-PolicyTipConfig -Name en\Reject -Value "This message appears to contain restricted content and will not be delivered."
```

Weitere Informationen zu DLP-Cmdlets finden Sie unter [Messaging Policy and Compliance Cmdlets](#).

## **Verwenden Sie Exchange Online PowerShell, um benutzerdefinierte Benachrichtigungstext ändern**

Im folgenden Beispiel wird ein vorhandener englischer Richtlinientipp, der nur der Benachrichtigung dient, geändert. Der Text dieses benutzerdefinierten Richtlinientipps wird in "Sending bank account numbers in email is not recommended" geändert.

```
Set-PolicyTipConfig en\NotifyOnly "Sending bank account numbers in email is not recommended."
```

Weitere Informationen zu DLP-Cmdlets finden Sie unter [Messaging Policy and Compliance Cmdlets](#).

## **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Führen Sie folgende Schritte aus, um zu überprüfen, ob Sie erfolgreich einen benutzerdefinierten Text für Richtlinientipps erstellt haben:

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Verhinderung von Datenverlust**.
2. Wählen Sie **Einstellungen für Richtlinientipps**.
3. Wählen Sie **Aktualisieren**.

4. Überprüfen Sie, ob die Aktion, das Gebietsschema und der Text für das Gebietsschema in der Liste angezeigt werden.

## Weitere Informationen

[Verhinderung von Datenverlust](#)

[Richtlinientipps](#)

[Transportregeln Exchange 2016](#)

[Nachrichtenflussregeln \(Transportregeln\) in Exchange Online](#)

[Exchange 2010 E-Mail-Info](#)

# Exchange-Überwachungsberichte

18.12.2018 • 12 minutes to read

Verwenden Sie die Überwachungsprotokollierung um Konfigurationsprobleme zu beheben, indem Sie bestimmte Änderungen durch Administratoren und als Hilfe beim erfüllen von behördlichen, Compliance und Aufbewahrung für eventuelle Anforderungen nachverfolgen. Exchange Online bietet zwei Arten von Überwachungsprotokollierung:

- Administrator audit-Protokollierung Datensätze Aktion basierend auf einer Exchange Online PowerShell-Cmdlets, von einem Administrator durchgeführt. Dadurch können Sie behandeln von Konfigurationsproblemen bei oder die Ursache des sicherheitsbezogene oder Compliance-bezogene Probleme zu identifizieren. In Exchange Online Aktionen von Microsoft-Administratoren und delegierte Administratoren, ausgeführt werden ebenfalls aufgezeichnet.
- Bei der Postfachüberwachungsprotokollierung werden alle Postfachzugriffe durch Administratoren, delegierte Benutzer oder den Postfachbesitzer aufgezeichnet. Dadurch können Sie feststellen, wer auf ein Postfach zugegriffen hat und welche Aktionen ausgeführt wurden.

## Exportieren von Überwachungsprotokollen

In der Exchange-Verwaltungskonsole (EAC) können Sie auf der Seite **Verwaltung der Richtlinientreue > Überwachung** nach Einträgen aus dem Administratorüberwachungsprotokoll und aus dem Postfachüberwachungsprotokoll suchen und diese exportieren.

- **Exportieren des administratorüberwachungsprotokolls:** Maßnahmen, die von einem Administrator, die auf ein Exchange Online PowerShell-Cmdlet basieren, die mit dem Verb **Get**, **Search**-beginnen nicht ausgeführt oder der Administrator-Überwachungsprotokolleinträge **Test** angemeldet ist Melden Sie sich. Das Cmdlet, das ausgeführt wurde, die Parameter und Werte weitergeleitet, woraufhin mit dem Cmdlet, wenn der Vorgang erfolgreich war, einschließen Überwachungsprotokolleinträge Sie können Suchen nach und Einträge aus dem Administrator-Überwachungsprotokoll exportieren. Wenn Sie die Suchergebnisse exportieren, Microsoft Exchange in einer XML-Datei gespeichert und fügt diese an eine e-Mail-Nachricht. Weitere Informationen finden Sie unter:
  - [Durchsuchen der Rollengruppenänderungen oder Administratorüberwachungsprotokolle](#)
  - [Anzeige und Export des externen Administratorüberwachungsprotokolls](#)

### NOTE

Standardmäßig werden die Einträge im Administrator-Überwachungsprotokoll 90 Tage lang aufbewahrt. Einträge, die älter als 90 Tage sind, werden gelöscht. In cloudbasierten Organisationen lässt sich diese Einstellung nicht ändern. In lokalen Exchange-Organisationen jedoch kann sie mithilfe des Cmdlets **Set-AdminAuditLog** geändert werden.

- **Postfachüberwachungsprotokolle exportieren:** Wenn postfachüberwachungsprotokollierung Protokollierung für ein Postfach aktiviert ist, werden Microsoft Exchange speichert einen Datensatz des ausgeführten Aktionen auf Postfachdaten von nicht-Besitzer im postfachüberwachungsprotokoll, das in einem ausgeblendeten Ordner im Postfach überwacht gespeichert ist. Mailbox Audit Logging können auch konfigurieren werden, um Besitzer Aktionen zu protokollieren. Einträge in diesem Protokoll weisen darauf hin, die das Postfach zugegriffen werden muss und wann die Aktionen ausgeführt, und gibt an, ob die Aktion erfolgreich war. Bei der Suche nach Einträge in die Überwachungsliste Postfach melden und zu

exportieren, speichert Microsoft Exchange, die Suche führt zu einer XML-Datei und fügt diese an eine e-Mail-Nachricht. Weitere Informationen finden Sie unter [postfachüberwachungsprotokolle exportieren](#).

## Ausführen von Überwachungsberichten

Wenn Sie in der Exchange-Verwaltungskonsole auf der Seite **Überwachung** einen der folgenden Berichte ausführen, werden die Ergebnisse im Detailbereich des Berichts angezeigt.

- **Führen Sie einen nicht-Besitzer Postfach Access-Bericht:** mit diesem Bericht können Sie Postfächer finden, die von einem Benutzer als Person zugegriffen wurde, die Besitzer des Postfachs ist. Weitere Informationen finden Sie unter [Ausführen von einem nicht-Besitzer Postfach Access-Bericht](#).
- **Führen Sie ein Administrator-rollengruppenbericht:** mit diesem Bericht können Sie um nach Änderungen an administratorrollengruppen zu suchen. Weitere Informationen finden Sie unter [Durchsuchen der rollengruppenänderungen oder Administrator Überwachungsprotokolle](#).
- **Führen Sie eine Compliance - Discovery und Haltebericht:** mit diesem Bericht können Sie Postfächer finden, die auf halten, oder von Compliance-Archiv entfernt wurden. Weitere Informationen finden Sie unter:
  - [In-Situ-Speicher und Beweissicherungsverfahren](#)
  - [Compliance-eDiscovery](#)
- **Führen Sie einen pro Postfach Rechtsstreitigkeiten Haltebericht:** mit diesem Bericht können Sie Postfächer finden, die auf halten oder von Aufbewahrung für eventuelle Rechtsstreitigkeiten entfernt wurden. Weitere Informationen finden Sie unter.
  - [Ausführen eines Berichts zu Beweissicherungsverfahren pro Postfach](#)
  - [Aktivieren des Beweissicherungsverfahrens für ein Postfach](#)
- **Führen Sie die Überwachungsprotokollbericht Admin:** mit diesem Bericht können Sie die Einträge des administratorüberwachungsprotokolls anzeigen. Anstelle von Exportieren des administratorüberwachungsprotokolls, die in einer e-Mail-Nachricht empfangen bis zu 24 Stunden dauern kann, können Sie diesen Bericht in der Exchange-Verwaltungskonsole ausführen. In diesem Bericht werden konfigurationsänderungen durch Administratoren in Ihrer Organisation. Bis zu 5.000 Einträge werden auf mehreren Seiten angezeigt. Um die Suche einzuschränken, können Sie einen Datumsbereich angeben. Weitere Informationen finden Sie unter:
  - [Anzeigen des Administratorüberwachungsprotokolls](#)
  - [Administratorüberwachungsprotokollierung](#)
- **Führen Sie die Überwachungsprotokollbericht externer Administrator:** Dieser Bericht ist nur verfügbar in Exchange Online und Exchange Online Protection. Aktionen von Microsoft-Administratoren ausgeführt oder delegierte Administratoren das Administrator-Überwachungsprotokoll angemeldet sind. Verwenden Sie die Überwachungsprotokollbericht externer Administrator suchen und Anzeigen der Aktionen, die Administratoren außerhalb Ihrer Organisation für die Konfiguration des Exchange Online-Organisation ausgeführt. Weitere Informationen finden Sie unter [anzeigen und exportieren das externer Administrator Audit melden](#).

## Konfigurieren der Überwachungsprotokollierung

Sie müssen zunächst die Überwachungsprotokollierung für die Organisation konfigurieren, um Überwachungsberichte auszuführen und Überwachungsprotokolle exportieren zu können.

### **Aktivieren der Postfachüberwachungsprotokollierung**

Die Postfachüberwachungsprotokollierung muss für jedes Postfach aktiviert werden, für das ein Bericht zum Postfachzugriff durch Nicht-Besitzer ausgeführt werden soll. Wenn die Postfachüberwachungsprotokollierung für ein Postfach nicht aktiviert ist, erhalten Sie beim Ausführen eines Berichts sowie beim Exportieren des Postfachüberwachungsprotokolls keine Ergebnisse für das Postfach.

Um die postfachüberwachungsprotokollierung für ein einzelnes Postfach zu aktivieren, führen Sie den folgenden Befehl in Exchange Online PowerShell.

```
Set-Mailbox <Identity> -AuditEnabled $true
```

Führen Sie folgende Befehle aus, um die Postfachüberwachung für alle Benutzerpostfächer in Ihrer Organisation zu aktivieren.

```
$UserMailboxes = Get-mailbox -Filter {(RecipientTypeDetails -eq 'UserMailbox')}  
$UserMailboxes | ForEach {Set-Mailbox $_.Identity -AuditEnabled $true}
```

Weitere Informationen dazu, wie Sie konfigurieren, welche Aktionen protokolliert werden sollen, finden Sie in den folgenden Artikeln:

- **Exchange Server:** [Aktivieren oder Deaktivieren der postfachüberwachungsprotokollierung für ein Postfach](#)
- **Exchange Online:** [Aktivieren der Überwachung in Office 365 Postfach](#)

### Gewähren des Benutzerzugriffs auf Überwachungsberichte

Standardmäßig können Administratoren in der Exchange-Verwaltungskonsole auf alle Berichte der Seite Überwachung zugreifen und diese ausführen. Anderen Benutzern (beispielsweise aus der Datensatzverwaltung oder aus der Rechtsabteilung) müssen die notwendigen Berechtigungen jedoch erst zugewiesen werden.

Die einfachste Möglichkeit, Benutzerzugriff gewähren ist so fügen sie der Rollengruppe "Datensatzverwaltung" hinzu. Exchange Online PowerShell können auch um ein Benutzerzugriff auf die Seite **Überwachung** in der Exchange-Verwaltungskonsole zu ermöglichen, von dem Benutzer die Rolle für Überwachungsprotokolle zuweisen.

#### Hinzufügen eines Benutzers zur Rollengruppe "Datensatzverwaltung"

1. Navigieren Sie zu **Berechtigungen > Administratorrollen**.
2. In der Liste mit Rollengruppen, klicken Sie auf **Verwaltung**, und klicken Sie dann auf **Bearbeiten**
3. Klicken Sie auf **Hinzufügen**, klicken Sie unter **Mitglieder** .
4. Wählen Sie den Benutzer, klicken Sie im Dialogfeld **Elemente auswählen**. Sie können für einen Benutzer eingeben ganz oder teilweise einen Anzeigennamen ein, und klicken Sie dann auf **Suche** suchen . Sie können auch die Liste sortieren, indem Sie auf die Spaltenüberschriften **Feldnamen** oder **Anzeigennamen**.
5. Klicken Sie auf **Hinzufügen** , und klicken Sie dann auf **OK**, um zur rollengruppenseite zurückzukehren.
6. Klicken Sie auf **Speichern**, um die Änderungen an der Rollengruppe zu speichern.

Im Detailbereich wird der Benutzer unter Mitglieder aufgeführt, und er kann in der Exchange-Verwaltungskonsole auf die Seite Überwachung zugreifen, Überwachungsberichte ausführen und Überwachungsprotokolle exportieren.

#### Zuweisen der Rolle für Überwachungsprotokolle zu einem Benutzer

Führen Sie den folgenden Befehl aus, um einem Benutzer die Rolle für Überwachungsprotokolle zuzuweisen.

```
New-ManagementRoleAssignment -Role "Audit Logs" -User <Identity>
```

Auf diese Weise kann der Benutzer in der Exchange-Verwaltungskonsole die Optionen **Verwaltung der Richtlinientreue** > **Überwachung** auswählen, um einen Bericht auszuführen. Zudem kann der Benutzer auch das Postfachüberwachungsprotokoll exportieren und das Administratorüberwachungsprotokoll exportieren und anzeigen.

#### **NOTE**

Wenn Sie einem Benutzer zwar das Ausführen von Überwachungsberichten, aber nicht das Exportieren von Überwachungsprotokollen ermöglichen möchten, weisen Sie mithilfe des vorherigen Befehls die Rolle mit Leserechten für Überwachungsprotokolle zu.

### **Konfigurieren von Outlook Web App, um XML-Anlagen zuzulassen**

Wenn Sie das Postfachüberwachungsprotokoll oder das Administratorüberwachungsprotokoll exportieren, wird das Überwachungsprotokoll (XML-Datei) an eine E-Mail angefügt. Jedoch blockiert Outlook Web App standardmäßig XML-Anlagen. Wenn Sie mit Outlook Web App auf exportierte Überwachungsprotokolle zugreifen möchten, muss Outlook Web App für das Zulassen von XML-Anlagen konfiguriert werden.

Führen Sie den folgenden Befehl aus, um XML-Anlagen in Outlook Web App zuzulassen.

```
Set-OwaMailboxPolicy -Identity Default -AllowedFileTypes  
.rmsg','.xlsx','.xlsm','.xlsb','.tiff','.pptx','.pptm','.ppsx','.ppsm','.docx','.docm','.zip','.xls','.wmv',  
.wma','.wav','.vsd','.txt','.tif','.rtf','.pub','.ppt','.png','.pdf','.one','.mp3','.jpg','.gif','.doc','.bmp',  
.avi','.xml'
```

# Exportieren von Postfachüberwachungsprotokollen

18.12.2018 • 13 minutes to read

Bei aktivierter Postfachüberwachung für ein Postfach werden im Postfachüberwachungsprotokoll Informationen protokolliert, wenn ein Benutzer, bei dem es sich nicht um den Besitzer des Postfachs handelt, auf das Postfach zugreift. Jeder Protokolleintrag enthält Angaben zur zugreifenden Person und zur Zugriffszeit, zu den Aktionen, die der Nicht-Besitzer ausgeführt hat, sowie zum Status der Aktion. Einträge im Postfachüberwachungsprotokoll werden standardmäßig für 90 Tage beibehalten. Mithilfe des Postfachüberwachungsprotokolls können Sie feststellen, ob auf ein Postfach von einer Person zugegriffen wurde, bei der es sich nicht um den Besitzer des Postfachs handelt.

Wenn Sie Einträge aus Postfachüberwachungsprotokollen exportieren, speichert Microsoft Exchange die Einträge in einer XML-Datei und fügt diese einer E-Mail an die angegebenen Empfänger an.

## Bevor Sie beginnen

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: Die Zeiten sind unterschiedlich. In Exchange Online wird das Postfachüberwachungsprotokoll binnen weniger Tage gesendet, nachdem Sie es exportiert haben.
- In Exchange Online müssen Sie die Remote Windows PowerShell verwenden, um viele der in diesem Thema aufgeführten Prozeduren auszuführen. Details finden Sie unter [Connect to Exchange Online Using Remote PowerShell](#).
- Für die Verfahren in diesem Thema sind bestimmte Berechtigungen erforderlich. Informationen zu den Berechtigungen finden Sie in den einzelnen Verfahren.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der Postfachüberwachungsprotokollierung

Zum Exportieren und Anzeigen von Postfachüberwachungsprotokollen muss zunächst die Postfachüberwachungsprotokollierung für jedes Postfach aktiviert werden, das Sie überwachen möchten. Außerdem müssen Sie Outlook Web App so konfigurieren, dass XML-Anlagen zugelassen werden. Nur dann können Sie mit Outlook Web App auf das Überwachungsprotokoll zugreifen.

### Schritt 1: Aktivieren der Postfachüberwachungsprotokollierung

Die Postfachüberwachungsprotokollierung muss für jedes Postfach aktiviert werden, für das ein Bericht zum Postfachzugriff durch Nicht-Besitzer ausgeführt werden soll. Ist die Postfachüberwachungsprotokollierung für ein Postfach nicht aktiviert, erhalten Sie keine Ergebnisse für dieses Postfach, wenn Sie das Postfachüberwachungsprotokoll exportieren.

Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Postfachüberwachungsprotokollierung" im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#).

Um die Postfachüberwachungsprotokollierung für ein einzelnes Postfach zu aktivieren, führen Sie den Befehl in Exchange Online PowerShell aus.

```
Set-Mailbox <Identity> -AuditEnabled $true
```

Führen Sie folgende Befehle aus, um die Postfachüberwachungsprotokollierung für alle Benutzerpostfächer in Ihrer Organisation zu aktivieren.

```
$UserMailboxes = Get-mailbox -Filter { (RecipientTypeDetails -eq 'UserMailbox') }
```

```
$UserMailboxes | ForEach { Set-Mailbox $_.Identity -AuditEnabled $true }
```

## Schritt 2: Konfigurieren von Outlook Web App, um XML-Anlagen zuzulassen

Beim Exportieren des Postfachüberwachungsprotokolls wird das Überwachungsprotokoll, das eine XML-Datei ist, an eine E-Mail angefügt. XML-Anlagen werden von Outlook Web App jedoch standardmäßig blockiert. Damit Sie auf das exportierte Überwachungsprotokoll zugreifen können, müssen Sie Microsoft Outlook verwenden oder Outlook Web App so konfigurieren, dass XML-Anlagen akzeptiert werden.

Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Outlook Web App-Postfachrichtlinien" im Thema [Client Access Permissions](#).

Führen Sie die folgenden Verfahren zum XML-Anlagen in Outlook Web App zuzulassen. Verwenden Sie in Exchange Server den Wert `Default` für den Parameter *Identity*.

1. Führen Sie den folgenden Befehl aus, um XML zur Liste der zulässigen Dateitypen in Outlook Web App hinzuzufügen.

```
Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -AllowedFileTypes @{'add=''.xml'}
```

2. Führen Sie den folgenden Befehl aus, um XML aus der Liste der blockierten Dateitypen in Outlook Web App zu entfernen.

```
Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -BlockedFileTypes @{'remove=''.xml'}
```

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie wie folgt vor, um zu überprüfen, ob die Postfachüberwachungsprotokollierung erfolgreich konfiguriert wurde:

1. Führen Sie den folgenden Befehl aus, um sich zu vergewissern, dass die Überwachungsprotokollierung für Postfächer aktiviert ist.

```
Get-Mailbox | Format-List Name,AuditEnabled
```

Der Wert `True` für die `_AuditEnabled_`-Eigenschaft überprüft, ob Überwachungsprotokollierung aktiviert ist. A value of `True` for the `_AuditEnabled_` property verifies that audit logging is enabled.

2. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass XML-Anlagen in Outlook Web App zulässig sind.

```
Get-OwaMailboxPolicy | Select-Object -ExpandProperty AllowedFileTypes
```

<span data-ttu-id="27114-150">Überprüfen Sie, ob `xml` in der Liste der zulässigen Dateitypen enthalten ist.</span><span class="sxs-lookup"><span data-stu-id="27114-150">Verify that `xml` is included in the list of allowed file types.</span></span>

3. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass XML-Anlagen aus der Liste für blockierte Dateien in Outlook Web App entfernt werden.

```
Get-OwaMailboxPolicy | Select-Object -ExpandProperty BlockedFileTypes
```

<span data-ttu-id="27114-152">Überprüfen Sie, ob `xml` ist nicht in der Liste der blockierten Dateitypen enthalten.</span><span class="sxs-lookup"><span data-stu-id="27114-152">Verify that `xml` isn't included in the list of blocked file types.</span></span>

## Exportieren des Postfachüberwachungsprotokolls

Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Leserechten administratorüberwachungsprotokollierung" im Thema [Shell Infrastructure Permissions](#).

1. Wechseln Sie in Exchange Admin Center (EAC) zu **Verwaltung der Richtlinientreue > Überwachung**.
2. Klicken Sie auf **Postfachüberwachungsprotokolle exportieren**.
3. Konfigurieren Sie die folgenden Suchkriterien zum Exportieren der Einträge aus dem Postfachüberwachungsprotokoll:
  - **Anfangs- und Enddatum:** Wählen Sie den Datumsbereich für die Einträge in die exportierte Datei eingeschlossen.
  - **Protokollieren, zu das Überwachungsprotokoll durchsucht Postfächer:** Wählen Sie die Postfächer abgerufen überwachen Protokolleinträge für.
  - **Typ des nicht-Besitzer-Zugriffs:** Wählen Sie eine der folgenden Optionen, um den Typ des nicht-Besitzer-Zugriffs abzurufenden Einträge für definieren:
  - **Alle nicht-Besitzer:** Suchen nach Zugriffen durch Administratoren und delegierte Benutzer in Ihrer Organisation sowie durch Microsoft-datencenteradministratoren in Exchange Online.
  - **Externe Benutzer:** Suchen nach Zugriffen durch Microsoft-datencenteradministratoren.
  - **Administratoren und delegierte Benutzer:** Suchen nach Zugriffen durch Administratoren und delegierte Benutzer in Ihrer Organisation.
  - **Administratoren:** Suchen nach Zugriffen durch Administratoren in Ihrer Organisation.
  - **Empfänger:** Wählen Sie die Benutzer zum Senden des postfachüberwachungsprotokolls an.
4. Klicken Sie auf **Exportieren**.

Microsoft Exchange ruft aus dem Postfachüberwachungsprotokoll die Einträge ab, die den Suchkriterien entsprechen, speichert die Einträge in einer Datei namens " SearchResult.xml ", und fügt die XML-Datei dann an eine E-Mail an, die an die von Ihnen angegebenen Empfänger gesendet wird.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Melden Sie sich an dem Postfach an, an das das Postfachüberwachungsprotokoll gesendet wurde. Wenn das Überwachungsprotokoll erfolgreich exportiert wurde, erhalten Sie eine von Exchange gesendete Nachricht. In Exchange Online dauert es möglicherweise ein paar Tage, bis Sie diese Nachricht erhalten. Das Postfachüberwachungsprotokoll "SearchResult.xml" wird an diese Nachricht angefügt. Wenn Sie Outlook Web App ordnungsgemäß konfiguriert haben, um XML-Anlagen zuzulassen, können Sie die angefügte XML-Datei herunterladen.

## Anzeigen des Postfachüberwachungsprotokolls

Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Leserechten administratorüberwachungsprotokollierung" im Thema [Shell Infrastructure Permissions](#).

So speichern Sie die Datei "SearchResult.xml" und zeigen sie an

1. Melden Sie sich an dem Postfach an, an das das Postfachüberwachungsprotokoll gesendet wurde.
2. Öffnen Sie im Posteingang die von Microsoft Exchange gesendete Nachricht mit der XML-Dateianlage. Der Text der E-Mail enthält die Suchkriterien.
3. Klicken Sie auf die Anlage, und laden Sie die XML-Datei herunter.
4. Öffnen Sie die Datei "SearchResult.xml" in Microsoft Excel.

## Weitere Informationen

- **Einträge im postfachüberwachungsprotokoll:** das folgende Beispiel zeigt einen Eintrag aus dem postfachüberwachungsprotokoll in der Datei "SearchResult.xml" enthalten. Jeder Eintrag vorangestellt ist die \*\* <Ereignis> \*\* XML-Tag und endet mit dem \*\* </Event> \*\* XML-Tag. Dieser Eintrag zeigt an, dass der Administrator die Nachricht mit dem Betreff "Benachrichtigung über Rechtsstreitigkeiten Archiv" aus dem Ordner wiederherstellbare Elemente in das Postfach von David auf 30 April 2010 gelöscht.

```
<Event MailboxGuid="6d4fbdae-e3ae-4530-8d0b-f62a14687939"
Owner="PPLNSL-dom\ david50001-1363917750"
LastAccessed="2010-04-30T11:01:55.140625-07:00"
Operation="HardDelete"
OperationResult="Succeeded"
LogonType="Admin"
FolderId="0000000073098C3277988F4CB882F5B82EBF64610100A7C317F68C24304BBD18ABE1F185E79B00000026BD4F0000"
FolderPathName="\Recoverable Items\Deletions"
ClientInfoString="Client=OWA;Action=ViaProxy"
ClientIPAddress="10.196.241.168"
InternalLogonType="Owner"
MailboxOwnerUPN="david@contoso.com"
MailboxOwnerId="S-1-5-21-290112810-296651436-1966561949-1151"
CrossMailboxOperation="false"
LogonUserDN="Administrator"
LogonUserId="S-1-5-21-290112810-296651436-1966561949-1149">
<SourceItems>

<ItemId="0000000073098C3277988F4CB882F5B82EBF64610700A7C317F68C24304BBD18ABE1F185E79B00000026BD4F0000A7
C317F68C24304BBD18ABE1F185E79B00000026BD540"
Subject="Notification of litigation hold"
FolderPathName="\Recoverable Items\Deletions" />
</SourceItems>
</Event>
```

- **Hilfreiche Felder im Postfach Überwachungsprotokoll:** Hier finden Sie eine Beschreibung der

hilfreiche Felder im postfachüberwachungsprotokoll. Sie helfen Ihnen bestimmte Informationen zu jeder Instanz von Access nicht-Besitzer eines Postfachs zu identifizieren.

FELD	BESCHREIBUNG
Owner	Der Besitzer des Postfachs, auf das von einem Nicht-Besitzer zugegriffen wurde.
LastAccessed	Das Datum und die Uhrzeit des Postfachzugriffs.
Operation	Die vom Nicht-Besitzer ausgeführte Aktion. Weitere Informationen finden Sie unter <a href="#">Run a Non-Owner Mailbox Access Report</a> im Abschnitt "Was wird im Postfachüberwachungsprotokoll protokolliert?".
OperationResult	Gibt an, ob die vom Nicht-Besitzer ausgeführte Aktion erfolgreich war.
LogonType	Der Typ des Nicht-Besitzer-Zugriffs. Hierzu zählen Zugriffe durch Administratoren, durch delegierte Benutzer und durch externe Benutzer.
FolderPathName	Der Name des Ordners mit der Nachricht, die von der Aktion des Nicht-Besitzers betroffen war.
ClientInfoString	Informationen zum E-Mail-Client, mit dem der Nicht-Besitzer auf das Postfach zugegriffen hat.
ClientIPAddress	Die IP-Adresse des Computers, mit dem der Nicht-Besitzer auf das Postfach zugegriffen hat.
InternalLogonType	Der Anmeldetyp des Kontos, mit dem der Nicht-Besitzer auf das Postfach zugegriffen hat.
MailboxOwnerUPN	Die E-Mail-Adresse des Postfachbesitzers.
LogonUserDN	Der Anzeigename des Nicht-Besitzers.
Subject	Die Betreffzeile der E-Mail, die von der Aktion des Nicht-Besitzers betroffen war.

[When mailbox auditing is enabled for a mailbox, Microsoft Exchange logs information in the mailbox audit log whenever a user other than the owner accesses the mailbox. Each log entry includes information about who accessed the mailbox and when, the actions performed by the non-owner, and whether the action was successful. Entries in the mailbox audit log are retained for 90 days by default. You can use the mailbox audit log to determine if a user other than the owner has accessed a mailbox. When you export entries from mailbox audit logs, Microsoft Exchange saves the entries in an XML file and attaches it to an email message sent to the specified recipients.](#Introduction.md)

# Ausführen eines Berichts zum Postfachzugriff durch Nicht-Besitzer

18.12.2018 • 10 minutes to read

Nicht-Besitzer Postfach Access-Bericht in der Exchange-Verwaltungskonsole (EAC) Listet die Postfächer, die von einem Benutzer als Person zugegriffen wurde, die Besitzer des Postfachs ist. Wenn ein Postfach mit einer nicht-Besitzer zugegriffen wird, protokolliert Microsoft Exchange Informationen über diese Aktion in einer postfachüberwachungsprotokolls, die als e-Mail-Nachricht in einem ausgeblendeten Ordner im Postfach überwacht gespeichert ist. Einträge aus dieses Protokoll als Suchergebnisse angezeigt, und eine Liste der Postfächer, die mit einem nicht-Besitzer, wer auf das Postfach zugegriffen und wann durchgeföhrten Aktionen mit nicht-Besitzer, zugegriffen und gibt an, ob die Aktion erfolgreich war. Standardmäßig werden die Einträge im postfachüberwachungsprotokoll 90 Tage lang aufbewahrt.

Wenn Sie die Postfachüberwachungsprotokollierung für ein Postfach aktivieren, werden bestimmte Aktionen von Nicht-Besitzern protokolliert. Zu diesen Nicht-Besitzern zählen neben Administratoren auch so genannte delegierte Benutzer, denen Berechtigungen für ein Postfach zugewiesen wurden. Die Suche kann auch auf Benutzer innerhalb oder außerhalb der Organisation eingegrenzt werden.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Postfachüberwachungsprotokollierung" im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren der Postfachüberwachungsprotokollierung

Die Postfachüberwachungsprotokollierung muss für jedes Postfach aktiviert werden, für das ein Bericht zum Postfachzugriff durch Nicht-Besitzer ausgeführt werden soll. Ist die Postfachüberwachungsprotokollierung nicht aktiviert, erhalten Sie beim Ausführen eines Berichts keine Ergebnisse.

Um die postfachüberwachungsprotokollierung für ein einzelnes Postfach zu aktivieren, führen Sie den folgenden Befehl in Exchange Online PowerShell.

```
Set-Mailbox <Identity> -AuditEnabled $true
```

Führen Sie beispielsweise den folgenden Befehl aus, um die Postfachüberwachung für einen Benutzer mit dem Namen Florence Flipo zu aktivieren.

```
Set-Mailbox "Florence Flipo" -AuditEnabled $true
```

Führen Sie folgende Befehle aus, um die Postfachüberwachung für alle Benutzerpostfächer in Ihrer Organisation zu aktivieren.

```
$UserMailboxes = Get-mailbox -Filter { (RecipientTypeDetails -eq 'UserMailbox') }
```

```
$UserMailboxes | ForEach {Set-Mailbox $_.Identity -AuditEnabled $true}
```

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie den folgenden Befehl aus, um sich zu vergewissern, dass Sie die Postfachüberwachungsprotokollierung erfolgreich konfiguriert haben.

```
Get-Mailbox | Format-List Name,AuditEnabled
```

Der Wert `True` für die `AuditEnabled`-Eigenschaft überprüft, ob Überwachungsprotokollierung aktiviert ist.

## Ausführen eines Berichts zum Postfachzugriff durch Nicht-Besitzer

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Überwachung**.

2. Klicken Sie auf **Bericht für Nicht-Besitzer-Postfachzugriff ausführen**.

Standardmäßig wird der Bericht zu Nicht-Besitzer-Zugriffen auf Postfächer in der Organisation für den Zeitraum der letzten zwei Wochen ausgeführt. Für die in den Suchergebnissen aufgeführten Postfächer wurde die Postfachüberwachungsprotokollierung aktiviert.

3. Wählen Sie zum Anzeigen von Nicht-Besitzer-Zugriffen für ein bestimmtes Postfach das Postfach in der Liste der Postfächer aus. Sehen Sie sich die Suchergebnisse im Detailbereich an.

#### TIP

Eingrenzen der Suchergebnisse? Wählen Sie das Startdatum und/oder das Enddatum sowie bestimmte Postfächer aus, die durchsucht werden sollen. Klicken Sie auf **Suchen**, um den Bericht erneut auszuführen.

#### Suchen nach bestimmten Typen von Nicht-Besitzer-Zugriff

Sie können auch den Typ des Nicht-Besitzer-Zugriffs (auch Anmeldetyp genannt) angeben, nach dem gesucht werden soll. Sie haben folgende Möglichkeiten:

- **Alle nicht-Besitzer:** Suchen nach Zugriffen durch Administratoren und delegierte Benutzer in Ihrer Organisation. Enthält außerdem Zugriffsbenutzer außerhalb Ihrer Organisation.
- **Externe Benutzer:** Suchen nach Zugriffen durch Benutzer außerhalb Ihrer Organisation.
- **Administratoren und delegierte Benutzer:** Suchen nach Zugriffen durch Administratoren und delegierte Benutzer in Ihrer Organisation.
- **Administratoren:** Suchen nach Zugriffen durch Administratoren in Ihrer Organisation.

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie erfolgreich einen nicht-Besitzer Postfach Access-Bericht ausgeführt haben, überprüfen

Sie im Ergebnisbereich Suche. Postfächer, denen Sie den Bericht für ausgeführt haben, werden in diesem Bereich angezeigt. Wenn keine Ergebnisse für ein bestimmtes Postfach vorhanden sind, ist es Zugriff durch nicht-Besitzer oder nicht-Besitzer-Zugriffs innerhalb des angegebenen Datumsbereichs stattgefunden noch nicht vorhanden wurde nicht möglich. Wie oben beschrieben werden Sie sicher, dass die Überwachungsprotokollierung aktiviert wurde für die Postfächer, den, die Sie suchen, für den Zugriff möchten, durch nicht-Besitzer.

## Was wird im Postfachüberwachungsprotokoll protokolliert?

Wenn Sie einen Bericht für Nicht-Besitzer-Postfachzugriff ausführen, werden Einträge aus dem Postfachüberwachungsprotokoll in den Suchergebnissen der Exchange-Verwaltungskonsole angezeigt. Jeder Berichtseintrag enthält folgende Informationen:

- Angaben zur zugreifenden Person und zur Zugriffszeit
- Die Aktionen, die durch den Nicht-Besitzer ausgeführt wurden
- Die betroffene Nachricht und der Speicherort des entsprechenden Ordners
- Den Status der Aktion

Die folgende Tabelle enthält die Aktionen postfachüberwachungsprotokollierung für nicht-Besitzer auf, die vom Postfach protokolliert werden können. Gibt an ein **Ja**, in der Tabelle **No** gibt an, dass eine Aktion kann nicht protokolliert werden, dass die Aktion für diese Anmeldetyp protokolliert werden kann. Ein Sternchen ( \* ) gibt an, dass die Aktion standardmäßig protokolliert wird, wenn die postfachüberwachungsprotokollierung für das Postfach aktiviert ist. Wenn Sie Aktionen verfolgen, die standardmäßig protokolliert werden nicht möchten, müssen Sie PowerShell verwenden, um die Protokollierung dieser Aktionen zu aktivieren.

### NOTE

Ein Administrator, dem Vollzugriff für ein Benutzerpostfach gewährt wurde, gilt als delegierter Benutzer.

ACTION	BESCHREIBUNG	ADMINISTRATOR	DELEGIERTER BENUTZER
<b>Kopieren</b>	Eine Nachricht wurde in einen anderen Ordner kopiert.	Ja	Nein
<b>Erstellen</b>	Ein Element wird im Postfachordner „Kalender“, „Kontakte“, „Aufgaben“ oder „Notizen“ erstellt. Beispielsweise wird eine neue Besprechungsanfrage erstellt. Die Erstellung von Nachrichten oder Ordnern wird nicht überwacht.	Ja*	Ja*
<b>„Folderbind“</b>	Auf einen Postfachordner wurde zugegriffen.	Ja*	Ja
<b>Dauerhaft löschen</b>	Eine Nachricht wurde endgültig aus dem Ordner „Wiederherstellbare Elemente“ gelöscht.	Ja*	Ja*

ACTION	BESCHREIBUNG	ADMINISTRATOR	DELEGIERTER BENUTZER
<b>"Messagebind"</b>	Eine Nachricht wurde im Vorschaufenster angezeigt oder geöffnet.	Ja	Nein
<b>Verschieben</b>	Eine Nachricht wurde in einen anderen Ordner verschoben.	Ja*	Ja
<b>In Ordner "Gelöschte Objekte" verschieben</b>	Eine Nachricht wurde in den Ordner "Gelöschte Objekte" verschoben.	Ja*	Ja
<b>Senden als</b>	Eine Nachricht wurde mithilfe der SendAs-Berechtigung gesendet. Das bedeutet, dass ein anderer Benutzer die Nachricht so gesendet hat, dass sie vom Postfachbesitzer zu kommen scheint.	Ja*	Ja*
<b>Senden im Auftrag von</b>	Eine Nachricht wurde mithilfe der SendOnBehalf-Berechtigung gesendet. Das bedeutet, dass ein anderer Benutzer die Nachricht im Namen des Postfachbesitzers gesendet hat. Für den Empfänger ist in der Nachricht angegeben, in wessen Namen die Nachricht gesendet wurde und wer die Nachricht tatsächlich gesendet hat.	Ja*	Ja
<b>Vorläufig löschen</b>	Eine Nachricht wurde aus dem Ordner "Gelöschte Objekte" gelöscht.	Ja*	Ja*
<b>Aktualisieren</b>	Eine Nachricht wurde geändert.	Ja*	Ja*

**NOTE**

\*Wird standardmäßig überwacht, wenn die Überwachung für ein Postfach aktiviert ist.

# Ausführen eines Berichts zu Beweissicherungsverfahren pro Postfach

18.12.2018 • 4 minutes to read

Wenn Ihre Organisation in ein Rechtsverfahren involviert ist, müssen Sie möglicherweise Schritte unternehmen, um relevante Daten zu sichern - beispielsweise E-Mails, die als Beweis dienen können. In einer solchen Situation können Sie alle von bestimmten Personen gesendeten und empfangenen E-Mails bzw. alle in Ihrer Organisation gesendeten und empfangenen E-Mails mithilfe der Beweissicherung für einen bestimmten Zeitraum aufzubewahren. Weitere Informationen dazu, was passiert, wenn ein Postfach einem Beweissicherungsverfahren unterliegt, sowie zur Aktivierung und Deaktivierung der Beweissicherung für ein Postfach finden Sie im Abschnitt "Postfachfunktionen" unter [Verwalten von Benutzerpostfächern](#).

Verwenden Sie den Bericht für die Beweissicherung, um die folgenden Typen von Änderungen nachzuverfolgen, die innerhalb eines bestimmten Zeitraums an einem Postfach vorgenommen wurden:

- Das Beweissicherungsverfahren wurde aktiviert.
- Das Beweissicherungsverfahren wurde deaktiviert.

Der Bericht enthält für jede dieser Änderungen den Benutzer, der die Änderung vorgenommen hat, und die Zeit (Uhrzeit und Datum), zu der die Änderung vorgenommen wurde.

## Was sollten Sie wissen, bevor Sie beginnen?

- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Leserechten administratorüberwachungsprotokollierung" im Thema [Shell Infrastructure Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen eines Berichts für die Beweissicherung über die Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Überwachung**.
2. Klicken Sie auf **Bericht zu Beweissicherungsverfahren pro Postfach ausführen**.

Microsoft Exchange führt den Bericht für alle für die Beweissicherung relevanten Änderungen aus, die in den vergangenen zwei Wochen an allen Postfächern vorgenommen wurden.

3. Um die Änderungen für ein bestimmtes Postfach anzuzeigen, wählen Sie im Suchergebnisbereich das Postfach aus. Sehen Sie sich die Suchergebnisse im Detailbereich an.

**TIP**

Eingrenzen der Suchergebnisse? Wählen Sie das Startdatum und/oder das Enddatum sowie bestimmte Postfächer aus, die durchsucht werden sollen. Klicken Sie auf **Suchen**, um den Bericht erneut auszuführen.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum Bestätigen, dass Sie einen Bericht zur Beweissicherung erfolgreich erstellt haben, werden Postfächer, bei denen im Datumsbereich für die Beweissicherung relevante Änderungen erfolgt sind, im Suchergebnisbereich angezeigt. Wenn es keine Ergebnisse gibt, sind im Datumsbereich keine für die Beweissicherung relevante Änderungen erfolgt oder neueste Änderungen noch nicht wirksam.

**NOTE**

Wenn ein Postfach der Beweissicherung unterliegt, kann es bis zu 60 Minuten dauern, bis diese wirksam wird.

# Durchsuchen der rollengruppenänderungen oder Administrator von Überwachungsprotokollen in Exchange Online

18.12.2018 • 14 minutes to read

Sie können die administratorüberwachungsprotokolle, um zu ermitteln, die die Organisation und Empfängerkonfiguration geändert suchen. Dies kann hilfreich sein, wenn Sie versuchen, eine verfolgen die Ursache des unerwartetes Verhalten, um ein böswilliger Administrator zu identifizieren oder um sicherzustellen, dass die Compliance-Bestimmungen eingehalten werden. Weitere Informationen zu Administrator audit-Protokollierung, finden Sie unter [administratorüberwachungsprotokollierung](#).

Wenn Sie das postfachüberwachungsprotokoll suchen möchten, finden Sie unter [Mailbox Audit Logging](#).

## TIP

In Exchange Online können Sie die Exchange-Verwaltungskonsole verwenden, um Einträge aus dem Administrator-Überwachungsprotokoll anzeigen zu lassen. Weitere Informationen finden Sie unter [Anzeigen des Administratorüberwachungsprotokolls](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: Weniger als 5 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Überwachungsprotokollierung durch Administratoren mit Leserechten" im Thema [Exchange and Shell Infrastructure Permissions](#).
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ausführen des Berichts mit Änderungen an Verwaltungsrollengruppen über die Exchange-Verwaltungskonsole

Wenn Sie möchten wissen, welche Änderungen Management Role Gruppenmitgliedschaft Rollengruppen in Ihrer Organisation vorgenommen wurden, können Sie den Bericht Rollengruppe Administrator im Exchange Administrationscenter (EAC). Den Administrator Rollengruppe Bericht können Sie eine Liste mit Rollengruppen anzeigen, die in einem angegebenen Zeitraum geändert wurden. Sie können auch bestimmte Rollengruppen auswählen, Änderungen für anzeigen möchten.

1. Wählen Sie in der Exchange-Verwaltungskonsole **Verwaltung der Richtlinientreue > Überwachung** aus, und klicken Sie anschließend auf **Administrator-Rollengruppenbericht ausführen**.
2. Wählen Sie über die Felder **Startdatum** und **Enddatum** einen Datumsbereich aus.
3. Klicken Sie auf **Rollengruppen auswählen**, und wählen Sie anschließend die Rollengruppen aus, deren Änderungen Sie prüfen möchten, oder lassen Sie dieses Feld leer, um in allen Rollengruppen nach Änderungen zu suchen.
4. Klicken Sie auf **Suchen**.

Wenn anhand der angegebenen Kriterien Änderungen ermittelt werden, wird im Bereich Ergebnisse eine Liste der Änderungen angezeigt. Beim Klicken auf eine Rollengruppe werden die Änderungen an der Rollengruppe im Detailbereich angezeigt.

## Exportieren des Administratorüberwachungsprotokolls mithilfe der Exchange-Verwaltungskonsole

Um eine XML-Datei mit den an Ihrer Organisation vorgenommenen Änderungen zu erstellen, können Sie in der Exchange-Verwaltungskonsole den Bericht "Administratorüberwachungsprotokoll" verwenden. Anhand dieses Berichts kann ein Datumsbereich für die Suche nach Überwachungsprotokolleinträgen mit Änderungen angegeben werden, die von bestimmten Benutzern vorgenommen wurden. Die XML-Datei wird anschließend als E-Mail-Anlage an einen Empfänger gesendet. Die maximale Größe der XML-Datei beträgt 10 MB.

### NOTE

In der Standardeinstellung zulassen nicht Outlook im Web (vormals Outlook Web App) Sie zum Öffnen von XML-Anlagen. Sie können entweder Konfigurieren von Outlook im Web zum anzuzeigende XML-Anlagen zuzulassen, oder Sie können einen anderen e-Mail-Client verwenden, um die Anlage (beispielsweise Microsoft Outlook) anzuzeigen. Informationen zum Konfigurieren von Outlook im Web, damit Sie XML-Anlagen anzeigen können, finden Sie unter [anzeigen oder Konfigurieren von Outlook auf die Eigenschaften der Web-Postfachrichtlinie in Exchange Online](#).

1. Wählen Sie in der Exchange-Verwaltungskonsole **Verwaltung der Richtlinientreue > Überwachung** aus, und klicken Sie anschließend auf **Administratorüberwachungsprotokoll exportieren**.
2. Wählen Sie über die Felder **Startdatum** und **Enddatum** einen Datumsbereich aus.
3. Klicken Sie im Feld **Überwachungsbericht senden an** auf **Benutzer auswählen**, und wählen Sie anschließend den Empfänger aus, an den der Bericht gesendet werden soll.
4. Klicken Sie auf **Exportieren**.

Wenn anhand der angegebenen Kriterien Protokolleinträge ermittelt werden, wird eine XML-Datei erstellt und als E-Mail-Anlage an den angegebenen Empfänger gesendet.

## Verwenden Sie Exchange Online PowerShell zum Suchen nach Überwachungsprotokolleinträgen

Exchange Online PowerShell können Sie um nach Überwachungsprotokolleinträgen zu suchen, die die Kriterien erfüllen, die Sie angeben. Eine Liste der Suchkriterien finden Sie unter [administratorüberwachungsprotokollierung](#). Dieses Verfahren verwendet das Cmdlet **Search-AdminAuditLog** und zeigt Suchergebnisse im Exchange Online PowerShell. Sie können dieses Cmdlet verwenden, wenn Sie benötigen, um eine Gruppe von Ergebnissen zurückzugeben, die auf das Cmdlet " **New-AdminAuditLogSearch**" oder in der Exchange-Verwaltungskonsole Überwachungsberichte Berichte festgelegten Beschränkungen überschreitet.

Wenn Sie Audit Log-Suchergebnisse in eine e-Mail-Anlage an einen Empfänger senden möchten, finden Sie weiter unten in diesem Thema **Verwenden von Exchange Online PowerShell zu suchenden Audit Einträgen protokolliert werden, und sendet Ergebnisse an einen Empfänger**.

Verwenden Sie die folgende Syntax, um das Überwachungsprotokoll anhand angegebener Kriterien zu durchsuchen.

```
Search-AdminAuditLog - Cmdlets <cmdlet 1, cmdlet 2, ...> -Parameters <parameter 1, parameter 2, ...> -  
StartDate <start date> -EndDate <end date> -UserIds <user IDs> -ObjectIds <object IDs> -IsSuccess <$True |  
$False >
```

#### NOTE

Standardmäßig gibt das Cmdlet **Search-AdminAuditLog** bis zu 1.000 Protokolleinträge zurück. Verwenden des Parameters *ResultSize* bis zu 250.000 Protokolleinträge angeben. Oder verwenden Sie den Wert **Unlimited** alle Einträge zurückgegeben.

In diesem Beispiel wird eine Suche nach allen Überwachungsprotokolleinträgen ausgeführt, welche die folgenden Kriterien erfüllen:

- **Startdatum:** 04/08/2018
- **Enddatum:** 03/10/2018
- **Benutzer-IDs:** Davids, Chrisd, Kima
- **Cmdlets:** Set-Mailbox
- **Parameter:** ProhibitSendQuota, ProhibitSendReceiveQuota, IssueWarningQuota, MaxSendSize, MaxReceiveSize

```
Search-AdminAuditLog -Cmdlets Set-Mailbox -Parameters  
ProhibitSendQuota,ProhibitSendReceiveQuota,IssueWarningQuota,MaxSendSize,MaxReceiveSize -StartDate 08/04/2018  
-EndDate 10/03/2018 -UserIds davids,chrisd,kima
```

In diesem Beispiel werden Änderungen an einem bestimmten Postfach ermittelt. Dies ist bei der Problembehebung nützlich, oder wenn Sie Informationen für eine Untersuchung bereitstellen müssen. Die folgenden Kriterien werden verwendet:

- **Startdatum:** 05/01/2018
- **Enddatum:** 03/10/2018
- **Objekt-ID:** contoso.com/Users/DavidS

```
Search-AdminAuditLog -StartDate 05/01/2018 -EndDate 10/03/2018 -ObjectID contoso.com/Users/DavidS
```

Wenn Ihre Suchanfragen viele Protokolleinträge zurückgeben, wird empfohlen, dass Sie das Verfahren in **Use Exchange Online PowerShell zu suchenden Audit Einträgen protokolliert werden, und Senden der Ergebnisse an einen Empfänger** weiter unten in diesem Thema verwenden. Das Verfahren unter, dass im Abschnitt eine XML-Datei als e-Mail-Anlage an die Empfänger gesendet geben Sie, sodass Sie leichter Extrahieren der Daten, die Ihnen interessiert sind.

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Search-AdminAuditLog](#).

#### Anzeigen der Details von Überwachungsprotokolleinträgen

Das Cmdlet **Search-AdminAuditLog** gibt die im Abschnitt "Inhalte von Überwachungsprotokollen" unter [Administratorüberwachungsprotokollierung](#) beschriebenen Felder zurück. Zwei der zurückgegebenen Felder, **CmdletParameters** und **ModifiedProperties**, enthalten zusätzliche Informationen, die standardmäßig nicht angezeigt werden.

Um die Inhalte der **Felder CmdletParameters und geänderte Eigenschaften** Felder anzuzeigen, verwenden Sie die folgenden Schritte aus. Oder Sie können das Verfahren weiter unten in diesem Thema in [Use Exchange Online PowerShell zu suchenden Audit Einträge protokolliert werden, und Senden der Ergebnisse an einen Empfänger](#) verwenden, um eine XML-Datei zu erstellen.

In dieser Vorgehensweise werden die folgenden Konzepte verwendet:

- [Arrays](#)
- [User-Defined Variables](#)

1. Legen Sie die Suchkriterien fest, führen Sie das Cmdlet **Search-AdminAuditLog** aus, und speichern Sie die Ergebnisse über den folgenden Befehl in einer Variablen.

```
$Results = Search-AdminAuditLog <search criteria>
```

2. Jede Überwachungsprotokolleintrag wird als Array-Elements in der Variablen gespeichert `$Results`. Arrayelement können Sie auswählen, indem Sie den arrayelementindex angeben. Array-Element Indizes beginnen bei Null (0) für das erste Arrayelement. Zum Abrufen des 5. Arrayelement einen Index von 4, das ist, verwenden Sie beispielsweise den folgenden Befehl.

```
$Results[4]
```

3. Der oben stehende Befehl gibt den im Arrayelement 4 gespeicherten Protokolleintrag zurück. Zum Anzeigen der Felder **CmdletParameters** und **ModifiedProperties** für diesen Protokolleintrag verwenden Sie die folgenden Befehle.

```
$Results[4].CmdletParameters  
$Results[4].ModifiedProperties
```

4. Um die Inhalte der Felder **CmdletParameters** und **ModifiedProperties** in einem anderen Protokolleintrag anzuzeigen, ändern Sie den Arrayelementindex.

## Verwenden von Exchange Online PowerShell zum Suchen nach Überwachungsprotokolleinträgen und Senden der Ergebnisse an einen Empfänger

Exchange Online PowerShell können Sie um Überwachungsprotokoll zu suchen, die Einträge, die die Kriterien erfüllen, die Sie angeben, die und senden Sie die Ergebnisse an einen Empfänger Sie, als Anlage zu einer XML-Datei angeben. Die Ergebnisse werden innerhalb von 15 Minuten an den Empfänger gesendet. Eine Liste der Suchkriterien finden Sie unter [Administratorüberwachungsprotokollierung](#).

#### NOTE

In der Standardeinstellung zulassen nicht Outlook im Web (vormals Outlook Web App) Sie zum Öffnen von XML-Anlagen. Sie können entweder Konfigurieren von Outlook im Web zum anzuzeigende XML-Anlagen zuzulassen, oder Sie können einen anderen e-Mail-Client verwenden, um die Anlage (beispielsweise Microsoft Outlook) anzuzeigen. Informationen zum Konfigurieren von Outlook im Web, damit Sie XML-Anlagen anzeigen können, finden Sie unter [anzeigen oder Konfigurieren von Outlook auf die Eigenschaften der Web-Postfachrichtlinie in Exchange Online](#).

Verwenden Sie die folgende Syntax, um das Überwachungsprotokoll anhand angegebener Kriterien zu durchsuchen.

```
New-AdminAuditLogSearch -Cmdlets <cmdlet1, cmdlet2, ...> -Parameters <parameter1, parameter2, ...> -StartDate <start date> -EndDate <end date> -UserIds <user IDs> -ObjectIds <object IDs> -IsSuccess <$true | $false > -StatusMailRecipients <recipient1, recipient2, ...> -Name <string to include in subject>
```

In diesem Beispiel wird eine Suche nach allen Überwachungsprotokolleinträgen ausgeführt, welche die folgenden Kriterien erfüllen:

- **Startdatum:** 04/08/2018
- **Enddatum:** 03/10/2018
- **Benutzer-IDs** davids, chrisd, kima
- **Cmdlets: Set-Mailbox**
- **Parameter:** *ProhibitSendQuota, ProhibitSendReceiveQuota, IssueWarningQuota, MaxSendSize, MaxReceiveSize*

Der Befehl sendet die Ergebnisse in einer Nachricht mit der Betreffzeile "Mailbox limit changes" an die SMTP-Adresse "davids@contoso.com".

```
New-AdminAuditLogSearch -Cmdlets Set-Mailbox -Parameters  
ProhibitSendQuota,ProhibitSendReceiveQuota,IssueWarningQuota,MaxSendSize,MaxReceiveSize -StartDate 08/04/2018  
-EndDate 10/03/2018 -UserIds davids,chrisd,kima -StatusMailRecipients davids@contoso.com -Name "Mailbox limit  
changes"
```

#### NOTE

Für den vom Cmdlet **New-AdminAuditLogSearch** generierten Bericht gilt eine Höchstgröße von 10 MB. Wenn bei der Suche ein Bericht mit einer Größe von mehr als 10 MB zurückgegeben wird, ändern Sie die angegebenen Suchkriterien. Verringern Sie z. B. den Datumsbereich, und führen Sie mehrere Berichte aus (für je einen Abschnitt des ursprünglichen Datumsbereichs).

Weitere Informationen zum Format der XML-Datei finden Sie unter [Administrator Audit Log Structure](#).

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-AdminAuditLogSearch](#).

# Anzeigen des Administratorüberwachungsprotokolls

18.12.2018 • 5 minutes to read

In Exchange Online können Sie die Exchange-Verwaltungskonsole (EAC) zum Suchen und Einträge in das Administrator-Überwachungsprotokoll anzeigen. Das Administrator-Überwachungsprotokoll aufgezeichnet bestimmte Aktionen, basierend auf Exchange Online PowerShell-Cmdlets, die von Administratoren und Benutzer, die mit administrative Berechtigungen zugewiesen wurden. Einträge in das Administrator-Überwachungsprotokoll bieten Ihnen Informationen über welche Cmdlet ausgeführt wurde, welche Parameter verwendet wurden, die das Cmdlet ausgeführt wurde und welche Objekte betroffen waren.

## NOTE

Administrator auditing Protokollierung ist standardmäßig aktiviert. > Das Administrator-Überwachungsprotokoll aufzeichnen keine Aktionen, die auf ein Exchange Online PowerShell-Cmdlet basiert, die mit dem Verb **Get**, **Search** oder **Test** beginnt. > Überwachungsprotokolleinträge werden 90 Tage lang aufbewahrt. Wenn ein Eintrag älter als 90 Tage ist, wird es gelöscht.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berichte anzeigen" im Thema [Feature Permissions in EOP](#).
- Wie bereits erwähnt, ist die Administratorüberwachungsprotokollierung standardmäßig aktiviert. Führen Sie zur Sicherstellung, dass die Administratorüberwachungsprotokollierung aktiviert wurde, folgenden Befehl aus:

```
Get-AdminAuditLogConfig | Format-List AdminAuditLogEnabled
```

In Exchange Server, können Sie Administrator Audit logging, falls es deaktiviert ist, indem Sie den folgenden Befehl ausführen.

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
```

In Exchange Online Protection und Exchange Online ist die Administratorüberwachungsprotokollierung immer aktiviert und kann nicht deaktiviert werden.

- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Anzeigen des Administratorüberwachungsprotokolls mithilfe der

## Exchange-Verwaltungskonsole

1. Wählen Sie in der Exchange-Verwaltungskonsole **Verwaltung der Compliance > Überwachung** aus, und klicken Sie anschließend auf **Administratorüberwachungsprotokoll-Bericht ausführen**.
2. Legen Sie **Startdatum** und **Enddatum** fest, und klicken Sie dann auf **Suchen**. Sämtliche Konfigurationsänderungen, die im angegebenen Zeitraum erfolgt sind, werden angezeigt und können anhand der folgenden Informationen sortiert werden:
  - **Datum:** Datum und Uhrzeit, die die Konfigurationsänderung vorgenommen wurde. Datum und Uhrzeit werden in koordinierter Weltzeit (UTC)-Format gespeichert.
  - **Cmdlet:** der Name des Cmdlets, die verwendet wurde, auf die Konfigurationsänderung erfolgt.
  - **Benutzer:** der Name des Benutzerkontos des Benutzers, der die Konfigurationsänderung vorgenommen hat.Es können bis zu 5000 Einträge auf mehreren Seiten angezeigt werden. Geben Sie einen kürzeren Datumsbereich ein, wenn Sie Ihre Ergebnisse eingrenzen möchten. Wenn Sie ein einzelnes Suchergebnis auswählen, werden im Detailbereich die folgenden weiteren Informationen angezeigt:
  - **Objekt geändert:** das Objekt, das vom Cmdlet geändert wurde.
  - **Parameter (Parameter: Wert):** die Cmdlet-Parameter, die verwendet wurden, und einen beliebigen Wert mit dem Parameter angegeben.
3. Wenn Sie einen bestimmten Überwachungsprotokolleintrag drucken möchten, klicken Sie im Detailbereich auf die Schaltfläche **Drucken**.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Wenn Sie einen Administrator-Überwachungsprotokollbericht erfolgreich ausgeführt haben, werden im angegebenen Datumsbereich erfolgte Konfigurationsänderungen im Suchergebnisbereich angezeigt. Wenn keine Ergebnisse vorhanden sind, ändern Sie den Datumsbereich, und führen Sie den Bericht erneut aus.

### NOTE

Wenn eine Änderung in Ihrer Organisation erfolgt, kann es bis zu 15 Minuten dauern, bis diese in den Suchergebnissen des Überwachungsprotokolls angezeigt wird. Wenn eine Änderung nicht im Administratorüberwachungsprotokoll aufgeführt wird, warten Sie einige Minuten, und führen Sie dann die Suche erneut aus.

# Anzeige und Export des externen Administratorüberwachungsprotokolls

18.12.2018 • 9 minutes to read

In Exchange Online Aktionen von Microsoft durchgeführt, und die Administrator-Überwachungsprotokoll delegierte Administratoren angemeldet sind. Sie können die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell zum Suchen und Anzeigen von Überwachungsprotokolleinträgen um zu ermitteln, ob externe Administratoren für alle Aktionen ausgeführt oder die Konfiguration Ihrer Exchange Online-Organisation geändert. Sie können auch Exchange Online PowerShell verwenden, um diese Überwachungsprotokolleinträgen zu exportieren.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Dies hängt davon ab, ob Sie die Einträge aus dem Administratorüberwachungsprotokoll anzeigen oder exportieren. Lesen Sie für jedes Verfahren nach, wie viel Zeit für dessen Abschluss veranschlagt wird.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Überwachungsprotokollierung durch Administratoren mit Leserechten" im Thema [Exchange and Shell Infrastructure Permissions](#).
- Beim Exportieren des Administratorüberwachungsprotokolls wird das Überwachungsprotokoll, das eine XML-Datei ist, an eine E-Mail angefügt, die an die angegebenen Empfänger gesendet wird. XML-Anlagen werden von Outlook Web App jedoch standardmäßig blockiert. Wenn Sie mit Outlook Web App auf exportierte Überwachungsprotokolle zugreifen möchten, muss Outlook Web App für das Zulassen von XML-Anlagen konfiguriert werden. Führen Sie den folgenden Befehl aus, um XML-Anlagen in Outlook Web App zuzulassen.

```
Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -AllowedFileTypes  
.rpmsg','.xlsx','.xlsm','.xlsb','.tiff','.pptx','.pptm','.ppsx','.ppsm','.docx','.docm','.zip','.xls',  
.wmv','.wma','.wav','.vsd','.txt','.tif','.rtf','.pub','.ppt','.png','.pdf','.one','.mp3','.jpg','.gif',  
.doc','.bmp','.avi','.xml'
```

- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## In der EAC das externe Administratorüberwachungsprotokoll anzeigen

Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten

1. Wählen Sie **Verwaltung der Richtlinientreue > Überwachung** aus, und klicken Sie anschließend auf **Externes Administratorüberwachungsprotokoll anzeigen**. Sämtliche Konfigurationsänderungen, die von Microsoft-Datencenteradministratoren und delegierten Administratoren im angegebenen Zeitraum

vorgenommen wurden, werden angezeigt und können anhand der folgenden Informationen sortiert werden:

- **Datum:** Datum und Uhrzeit, die die Konfigurationsänderung vorgenommen wurde. Datum und Uhrzeit werden in koordinierter Weltzeit (UTC)-Format gespeichert.
- **Cmdlet:** der Name des Cmdlets, die verwendet wurde, auf die Konfigurationsänderung erfolgt.

Wenn Sie ein einzelnes Suchergebnis auswählen, werden im Detailbereich die folgenden Informationen angezeigt:

- Datum und Uhrzeit der Cmdlet-Ausführung.
  - Der Benutzer, von dem das Cmdlet ausgeführt wurde. Bei allen Einträgen im externen Administratorüberwachungsprotokoll wird der Benutzer als **Administrator** angegeben, was auf einen Microsoft-Datencenteradministrator oder einen externen Administrator hinweist.
  - Die verwendeten Cmdlet-Parameter und der mit dem Parameter angegebene beliebige Wert im Format **Parameter:Wert**.
2. Wenn Sie einen bestimmten Eintrag im Überwachungsprotokoll drucken möchten, wählen Sie ihn im Suchergebnisbereich aus, und klicken Sie im Detailbereich auf **Drucken**.
  3. Um die Suche einzuschränken, legen Sie die Dropdownmenüs **Anfangsdatum** und **Enddatum** fest, und klicken Sie dann auf **Suchen**.

## Verwenden von Exchange Online PowerShell Einträge in die Überwachungsprotokollbericht externer Administrator anzeigen

Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten

Sie können das Cmdlet **Search-AdminAuditLog** mit dem Parameter *ExternalAccess* anzeigen Einträge aus der Administrator audit Log für Aktionen, die von Microsoft-datencenteradministratoren durchgeführt und als Administratoren delegierte.

Dieser Befehl gibt alle Einträge im Administratorüberwachungsprotokoll für Cmdlets zurück, die von externen Administratoren ausgeführt wurden.

```
Search-AdminAuditLog -ExternalAccess $true
```

Dieser Befehl gibt alle Einträge im Administratorüberwachungsprotokoll für Cmdlets zurück, die von externen Administratoren zwischen dem 17. September 2013 und dem 2. Oktober 2013 ausgeführt wurden.

```
Search-AdminAuditLog -ExternalAccess $true -StartDate 09/17/2013 -EndDate 10/02/2013
```

Weitere Informationen finden Sie unter [Search-AdminAuditLog](#).

## Exportieren des administratorüberwachungsprotokolls mithilfe von Exchange Online PowerShell

Geschätzte Zeit bis zum Abschließen des Vorgangs: Ungefähr 24 Stunden

Sie können das Cmdlet **New-AdminAuditLogSearch** mit dem Parameter *ExternalAccess* verwenden, um Einträge aus dem Administratorüberwachungsprotokoll zu exportieren, die sich auf Aktionen beziehen, die von Microsoft-Datencenteradministratoren oder delegierten Administratoren vorgenommen wurden. Microsoft Exchange ruft Einträge im Administratorüberwachungsprotokoll ab, die von Administratoren durchgeführt wurden, und speichert sie in einer Datei mit dem Namen SearchResult.xml. Diese XML-Datei wird einer E-Mail-

Nachricht angefügt, die innerhalb von 24 Stunden an die angegebenen Empfänger gesendet wird.

Der folgende Befehl gibt Administrator-Überwachungsprotokolleinträge für Cmdlets zurück, die von externen Administratoren zwischen dem 25. September 2013 und dem 24. Oktober 2013 ausgeführt wurden. Die Suchergebnisse werden an die SMTP-Adressen admin@contoso.com und pilarp@contoso.com mit dem Text "External admin audit log" (Externes Administratorüberwachungsprotokoll) in der Betreffzeile der Nachricht gesendet.

```
New-AdminAuditLogSearch -ExternalAccess $true -EndDate 10/24/2013 -StartDate 07/25/2013 -StatusMailRecipients admin@contoso.com,pilarp@contoso.com -Name "External admin audit log"
```

#### NOTE

Wenn der Parameter *ExternalAccess* verwendet werden, nur Einträge für Aktionen, die von Microsoft Datacenter Administrator durchgeführt oder delegierte Administratoren in das Überwachungsprotokoll, das exportiert wird enthalten sind. Wenn Sie keinen den *ExternalAccess* -Parameter angeben, wird das Überwachungsprotokoll Einträge für die Administratoren in Ihrer Organisation und von externen Administratoren ausgeführten Aktionen enthalten.

Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der Befehl für den Export der Einträge im Administratorüberwachungsprotokoll, die von externen Administratoren durchgeführt wurden, erfolgreich war, und um Informationen über die aktuellen Suchen im Administratorüberwachungsprotokoll anzuzeigen:

```
Get-AuditLogSearch | Format-List
```

## Weitere Informationen

- In Office 365 können Sie die Möglichkeit, bestimmte Verwaltungsaufgaben an einen autorisierten Partner von Microsoft delegieren. Diese Administratoraufgaben enthalten erstellen oder Bearbeiten von Benutzern, Zurücksetzen von Benutzerkennwörtern, Verwalten von Benutzerlizenzen, Verwalten von Domänen und anderen Benutzern in Ihrer Organisation Administratorberechtigungen zuweisen. Wenn Sie einen Partner dieser Rolle übernehmen autorisieren, wird der Partner als einem delegierten Administrator bezeichnet. Die Aufgaben, die von einem delegierten Administrator durchgeführt werden im administratorüberwachungsprotokoll protokolliert. Wie oben beschrieben, von delegierten Administratoren ausgeführten Aktionen angezeigt werden, indem Sie die Überwachungsprotokollbericht externer Administrator ausführen oder mit dem **New-AdminAuditLogSearch** -Cmdlet mit dem Parameter *ExternalAccess* exportiert werden können.
- Das Administrator-Überwachungsprotokoll aufzeichnet bestimmte Aktionen, basierend auf Exchange Online PowerShell-Cmdlets, die von Administratoren und Benutzer, die mit administrative Berechtigungen zugewiesen wurden. Von externen Administratoren ausgeführten Aktionen werden ebenfalls protokolliert. Einträge im administratorüberwachungsprotokoll bieten Ihnen Informationen über das Cmdlet ausgeführt wurde, welche Parameter verwendet wurden, und welche Objekte betroffen waren.
- Das Administrator-Überwachungsprotokoll aufzeichnen keine Aktionen, die basierend auf einem Exchange Online PowerShell-Cmdlets, die mit dem Verb **Get**, **Search**oder **Test**beginnt.
- Die Überwachungsprotokolleinträge werden 90 Tage lang aufbewahrt. Wenn ein Eintrag älter als 90 Tage ist, wird er gelöscht.

# Messaging-Datensatzverwaltung

18.12.2018 • 14 minutes to read

Benutzer senden und empfangen jeden Tag E-Mails. Wenn diese große Menge an E-Mails, die jeden Tag verfasst und empfangen werden, nicht verwaltet wird, kann dies Benutzer belasten, ihre Produktivität beeinträchtigen und zu Risiken für Ihre Organisation führen. Daher ist die Verwaltung des E-Mail-Lebenszyklus eine entscheidende Komponente für die meisten Organisationen.

Messaging-datensatzverwaltung (MRM) ist die Datensätze-Technologie in Exchange Server und Exchange-Online, die Organisationen e-Mail-Lebenszyklus verwalten und Reduzieren der rechtlichen Risiken im Zusammenhang mit e-Mail-helfen. Bereitstellen von MRM helfen Ihrer Organisation auf verschiedene Weise:

- **Business-Anforderungen erfüllen:** abhängig von Ihrer Organisation die messaging-Richtlinien, müssen Sie möglicherweise wichtige e-Mail-Nachrichten für einen bestimmten Zeitraum aufzubewahren. Beispielsweise kann dem Postfach eines Benutzers im Zusammenhang mit der Unternehmensstrategie, Transaktionen, Produktentwicklung oder Interaktion mit Kunden wichtige Nachrichten enthalten.
- **Rechtliche Hinweise und behördliche Anforderungen erfüllen:** viele Organisationen verfügen über eine rechtliche oder behördliche Voraussetzung zum Speichern von Nachrichten für einen bestimmten Zeitraum und Entfernen von Nachrichten, die älter sind als dieses Zeitraums. Speichern von Nachrichten, die länger als notwendig kann Ihre Organisation rechtlichen oder finanziellen Risiken erhöhen.
- **Erhöhen Sie die Produktivität der Benutzer:** Wenn diesbezüglich, kann die Lautstärke werdende von e-Mail in die Postfächer der Benutzer auch ihre Produktivität auswirken. Beispielsweise zwar Newsletter-Abonnements und automatische Benachrichtigung Informationszwecken Wert aufweisen können beim Empfang sind, Benutzer möglicherweise nicht entfernen sie nach dem Lesen (oft sie sind niemals gelesen). Viele der folgenden Nachrichtentypen keinen Wert für die Beibehaltungsdauer jenseits binnen weniger Tage. Entfernen von Nachrichten mit MRM kann Informationen in den Postfächern der Benutzer, steigert die Produktivität der Übersichtlichkeit helfen.
- **Speicherverwaltung verbessern:** aufgrund von den Diensten für kostenlose Consumer-e-Mail-gesteuerte rechnen, viele Benutzer alte Nachrichten für einen längeren Zeitraum beizubehalten oder nie entfernt werden. Verwalten von großen Postfächern ist in zunehmendem ein Standardverfahren, und Benutzer sollten nicht so ändern Sie ihre Arbeitsgewohnheiten basierend auf strengen Postfachkontingente gezwungen sein. Allerdings Beibehaltung Nachrichten jenseits des Zeitraums, der für das Unternehmen erforderlich ist, rechtliche oder behördliche Gründe auch Speicher Kosten erhöht.

Mit MRM können Sie die Richtlinie für die Datensatzverwaltung implementieren, mit der die Anforderungen Ihrer Organisation am besten erfüllt werden. Wenn Sie sich mit MRM und Compliance-Archiven vertraut machen, sind Sie in der Lage, Ihre Ziele beim Verwalten des Postfachspeichers zu erreichen und Vorschriften im Hinblick auf die Nachrichtenaufbewahrung einzuhalten.

Möchten Sie wissen, welche Verwaltungsaufgaben es im Zusammenhang mit MRM gibt? Weitere Informationen finden Sie unter [Messaging Records Management Procedures](#).

## MRM in Exchange Server und Exchange Online

In Exchange Server und Exchange Online wird durch die Verwendung von Aufbewahrungstags und Aufbewahrungsrichtlinien MRM erreicht. Aufbewahrungstags werden verwendet, um die Einstellungen für die Aufbewahrung für eine gesamte Postfach und Postfach-Standardordner wie Posteingang und gelöschte Objekte gelten. Sie können auch erstellen und Bereitstellen von Aufbewahrungstags, mit denen Outlook 2010 und höher und Outlook Web App-Benutzer können auf Ordner oder einzelne Nachrichten anzuwenden. Nachdem sie erstellt

haben, Sie aufbewahrungstags für eine Aufbewahrungsrichtlinie hinzufügen und wenden Sie die Richtlinie für Benutzer. Assistenten für verwaltete Ordner verarbeitet Postfächer und beibehaltungseinstellungen in der Aufbewahrungsrichtlinie des Benutzers angewendet. Weitere Informationen zu Aufbewahrungsrichtlinien finden Sie unter [aufbewahrungstags und Aufbewahrungsrichtlinien](#).

Wenn eine Nachricht den im jeweiligen Aufbewahrungstag angegebenen Aufbewahrungszeitraum erreicht, führt der Assistent für verwaltete Ordner die im Tag festgelegte Aufbewahrungsaktion aus. Nachrichten können dann endgültig gelöscht werden oder wiederherstellbar bleiben. Wenn für den Benutzer ein Archiv bereitgestellt wurde, können Sie mit Aufbewahrungstags auch Elemente in das Compliance-Archiv des Benutzers verschieben.

## MRM-Strategien

Mithilfe von Aufbewahrungsrichtlinien können Sie grundlegende Einstellungen für die Aufbewahrung von Nachrichten für ein vollständiges Postfach und für bestimmte Standardordner durchsetzen. Es gibt verschiedene Strategien für die MRM-Bereitstellung. Die gängigsten werden im Folgenden dargestellt:

**Entfernen Sie alle Nachrichten nach einem angegebenen Zeitraum:** In dieser Strategie implementieren Sie eine einzelne MRM-Richtlinie, die alle Nachrichten nach einem bestimmten Zeitraum entfernt. In dieser Strategie besteht keine Klassifikation von Nachrichten. Sie können diese Richtlinie implementieren, durch eine einzelne Richtlinie Standardtag (DPT) für das Postfach erstellen. Dies sicherstellen nicht jedoch, dass Nachrichten für den angegebenen Zeitraum aufbewahrt werden. Benutzer können weiterhin Nachrichten löschen, bevor Aufbewahrungsdauer erreicht ist.

**Verschieben von Nachrichten in archivpostfächern:** In dieser Strategie implementieren Sie MRM-Richtlinien, die Elemente in das Archivpostfach des Benutzers zu verschieben. Ein Archivpostfach bietet zusätzlichen Speicher für Benutzer zum Aufrechterhalten der alten und Inhalte selten zugegriffen. Aufbewahrungstags, die Elemente zu verschieben, sind auch bekannt als archivrichtlinien. Sie können in die gleiche Aufbewahrungsrichtlinie ein Standardrichtlinientag und persönliche Tags zum Verschieben von Elementen, und ein Standardrichtlinientag, Aufbewahrungsrichtlinientags und persönliche Tags zum Löschen von Elementen kombinieren. Weitere Informationen zu Archivierungsrichtlinien finden Sie unter:

- [Exchange Server 2016: Compliance - Archivierung](#)
- [Exchange Online: Archivieren von Postfächern in Exchange Online](#)

### NOTE

In einer Exchange-Hybridbereitstellung können Sie ein cloudbasiertes Archivpostfach für ein lokales primäres Postfach aktivieren. Beim Zuweisen einer Archivrichtlinie zu einem lokalen Postfach werden die Elemente zum cloudbasierten Archiv verschoben. Wenn ein Element in das Archivpostfach verschoben wird, wird im lokalen Postfach keine Kopie davon beibehalten. Wenn das lokale Postfach ausgesetzt wird, werden Elemente anhand einer Archivrichtlinie weiterhin in das cloudbasierte Archivpostfach verschoben, in dem sie so lange aufbewahrt werden, wie dies durch die In-Situ-Speicherung festgelegt wurde.

**Entfernen von Nachrichten auf Grundlage der Speicherort des Ordners:** In dieser Strategie implementieren Sie basierte auf e-Mail-Speicherort MRM-Richtlinien. Beispielsweise können Sie angeben, dass Nachrichten im Posteingang ein Jahr aufbewahrt werden und Nachrichten in den Junk-e-Mail-Ordner 60 Tage lang aufbewahrt werden. Sie können diese Richtlinie implementieren, indem Sie mit einer Kombination von aufbewahrungsrichtlinientags (Aufbewahrungsrichtlinientags), für jeden Standardordner, den Sie konfigurieren möchten, und ein Standardrichtlinientag für das gesamte Postfach. Die DPT gilt für alle benutzerdefinierten Ordnern und alle Standardordnern, die ein Berichtskopf angewendet haben.

#### **NOTE**

In Exchange Server können Sie Aufbewahrungsrichtlinientags für die Ordner Kalender und Aufgaben erstellen. Wenn Sie nicht, dass die Elemente in diese Ordner oder andere Standardordnern abläuft möchten, können Sie eine deaktivierte aufbewahrungstag für den standardmäßigen Ordner erstellen.

**Benutzer können Nachrichten klassifizieren:** In dieser Strategie implementieren Sie MRM-Richtlinien, die eine Einstellung für geplante Archivierung für alle Nachrichten, aber Benutzer basierte auf geschäftlichen oder gesetzlichen Anforderungen angemessen klassifizieren zulassen enthalten. In diesem Fall Benutzer werden ein wichtiger Bestandteil Ihrer Strategie für die Verwaltung – häufig über das beste Verständnis der Wert für eine Nachricht die Beibehaltungsdauer verfügen.

Benutzer können unterschiedliche Aufbewahrungseinstellungen auf Nachrichten anwenden, die für einen längeren oder kürzeren Zeitraum aufbewahrt werden müssen. Sie können diese Richtlinie mit einer Kombination der folgenden Tags implementieren:

- Ein Standardrichtlinientag für das Postfach
- Persönliche Tags, die Benutzer auf benutzerdefinierte Ordner oder einzelne Nachrichten anwenden können
- (Optional) Zusätzliche Aufbewahrungsrichtlinientags, um für Elemente in bestimmten Standardordnern ein Aufbewahrungslimit festzulegen

Beispielsweise können Sie eine Aufbewahrungsrichtlinie mit persönlichen Tags verwenden, die einen kürzeren Aufbewahrungszeitraum festlegen (z. B. 2 Tage, 1 Woche oder 1 Monat), sowie mit persönlichen Tags, in denen ein längerer Aufbewahrungszeitraum (z. B. 1 Jahr, 2 Jahre, 5 Jahre) definiert ist. Die Benutzer können persönliche Tags mit kürzeren Aufbewahrungszeiträumen auf Elemente wie Newsletterabonnements anwenden, die innerhalb von Tagen nach dem Empfang ihren Nutzen verlieren. Mithilfe von Tags mit längeren Zeiträumen können dagegen Elemente aufbewahrt werden, die einen großen geschäftlichen Nutzen aufweisen. Sie können den Vorgang auch mithilfe von Posteingangsregeln in Outlook automatisieren, um ein persönliches Tag auf Nachrichten anzuwenden, die die Regelbedingungen erfüllen.

**Beibehalten von Nachrichten für eDiscovery-Zwecken:** In dieser Strategie implementieren Sie MRM-Richtlinien, die Nachrichten aus Postfächern entfernen, nachdem einem angegebenen Zeitraum, sondern auch behalten sie im Ordner "wiederherstellbare Elemente" aus Gründen der [Compliance - eDiscovery](#), auch wenn die Nachrichten wurden vom Benutzer oder von einem anderen Prozess gelöscht.

Sie können diese Anforderung mithilfe einer Kombination von Aufbewahrungsrichtlinien und [Compliance-Archiv und Aufbewahrung für eventuelle Rechtsstreitigkeiten](#) oder Aufbewahrung für eventuelle Rechtsstreitigkeiten erfüllen. Aufbewahrungsrichtlinien werden Nachrichten aus dem Postfach nach einem bestimmten Zeitraum entfernen. Eine zeitbasierten Compliance-Archiv oder die Aufbewahrung für eventuelle Rechtsstreitigkeiten behält Nachrichten, die vor diesem Zeitraum geändert oder gelöscht. Beispielsweise können, um Nachrichten sieben Jahren beibehalten werden, Sie erstellen eine Aufbewahrungsrichtlinie mit einer DPT, die Nachrichten in sieben Jahren löscht und Aufbewahrung für eventuelle Rechtsstreitigkeiten, um Nachrichten sieben Jahren zu speichern. Nach sieben Jahren werden Nachrichten, die vom Benutzer entfernt werden nicht gelöscht. Nachrichten von Benutzern gelöscht werden, bevor die sieben Jahre werden im Ordner "wiederherstellbare Elemente" sieben Jahre aufbewahrt werden. Weitere Informationen zu diesen Ordner finden Sie unter [Recoverable Items Folder](#).

Optional können Sie es Benutzern mit Aufbewahrungsrichtlinientags und persönlichen Tags ermöglichen, ihre Postfächer zu bereinigen. Jedoch bleiben die gelöschten Nachrichten im In-Situ-Speicher und im Beweissicherungsverfahren erhalten, bis der Aufbewahrungszeitraum beendet ist.

**NOTE**

Ein zeitbasierter In-Situ-Speicher oder ein Beweissicherungsverfahren ist mit der sogenannten rollierenden gesetzlichen Aufbewahrungspflicht in Exchange 2010 vergleichbar (bitte beachten Sie, dass dies nicht der offizielle Begriff ist). Zur Implementierung der gesetzlichen Aufbewahrungspflicht wurde der Aufbewahrungszeitraum für gelöschte Elemente für eine Postfachdatenbank oder einzelne Postfächer konfiguriert. Bei der Aufbewahrung gelöschter Elemente werden gelöschte und geänderte Elemente jedoch basierend auf dem Löschdatum beibehalten. Der In-Situ-Speicher und das Beweissicherungsverfahren bewahren Elemente basierend auf dem Datum des Empfangs oder der Erstellung auf. Dadurch wird sichergestellt, dass Nachrichten mindestens für den angegebenen Zeitraum beibehalten werden.

## Weitere Informationen

[Zeichnet Management Terminologie 2013 im Exchange Messaging](#)

[Aufbewahrungstags und Aufbewahrungsrichtlinien](#)

# Aufbewahrungstags und Aufbewahrungsrichtlinien

18.12.2018 • 31 minutes to read

In Microsoft Exchange Server und Exchange Online unterstützt Messaging-datensatzverwaltung (MRM) zum Verwalten von e-Mail-Lebenszyklus und Reduzieren der rechtlichen Risiken im Zusammenhang mit E-mail und anderen Organisationen. MRM macht es einfacher, die Einhaltung von Unternehmensrichtlinien, behördlichen Vorschriften oder rechtlichen Anforderungen und zum Entfernen der Inhalte, die nicht zulässigen hat benötigte Nachrichten beizubehalten oder geschäftlichen Nutzen.

Sehen Sie sich dieses [video](#) für einen schnellen Überblick über Gewusst wie: Anwenden von aufbewahrungstags und eine Aufbewahrungsrichtlinie auf ein Postfach in Exchange Online.

## Strategie für die Messaging-Datensatzverwaltung

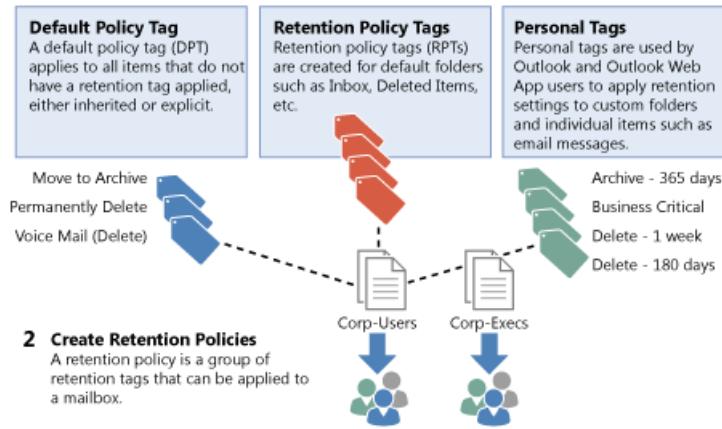
In Exchange Server und Exchange Online MRM erfolgt mithilfe von aufbewahrungstags und Aufbewahrungsrichtlinien. Vor dem im Zusammenhang mit Details zu den einzelnen diese Archivierungsfunktionen ist es wichtig, um zu erfahren, wie die Features in der gesamten MRM-Strategie verwendet werden. Diese Strategie basiert auf:

- Zuweisen von Aufbewahrungsrichtlinientags zu Standardordnern, beispielsweise dem Posteingang und dem Ordner für gelöschte Elemente.
- Anwenden von Standardrichtlinientags auf Postfächer, um die Aufbewahrung aller nicht markierten Elementen zu verwalten.
- Möglichkeit für Benutzer, benutzerdefinierten Ordnern und einzelnen Elementen persönliche Tags zuzuweisen.
- Trennen der MRM-Funktionalität von den Verwaltungs- und Archivierungsvorgängen, die Benutzer für ihren Posteingang durchführen. Benutzer müssen Nachrichten nicht anhand von Aufbewahrungsanforderungen in verwalteten Ordner ablegen. Einzelne Nachrichten können ein anderes Aufbewahrungstag aufweisen als die Ordner, in denen sie enthalten sind.

Die folgende Abbildung zeigt die Aufgaben im Zusammenhang mit der Implementierung dieser Strategie.

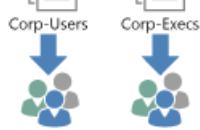
## 1 Create Retention Tags

Retention tags are used to apply retention settings to messages and folders. There are three types of retention tags:



## 2 Create Retention Policies

A retention policy is a group of retention tags that can be applied to a mailbox.



## 3 Link Retention Tags to Retention Policies

A retention policy can have one DPT to move items to the archive, one DPT to delete items, one DPT to delete voice mail messages, one RPT for each supported default folder, and any number of personal tags.

## 4 Apply Retention Policies

Retention policies are applied to mailbox users. Different sets of users can have different retention policies.



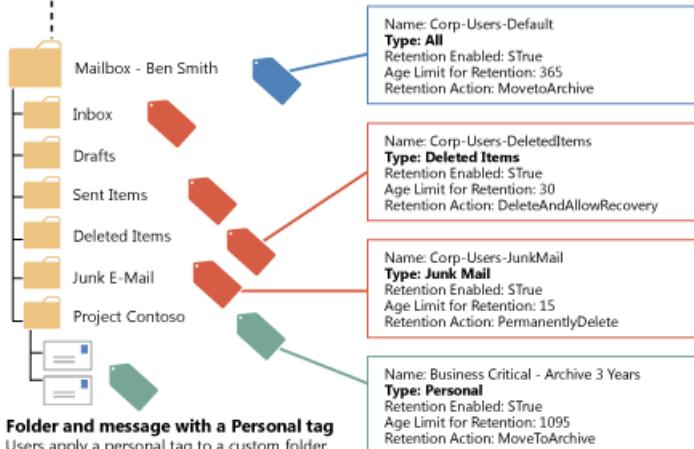
## 5 The Managed Folder Assistant Processes Mailboxes

The Managed Folder Assistant, a process that runs on Mailbox servers, processes mailboxes, applies retention settings to mailbox items, and takes the specified retention action.



## 6 Mailbox Processed

After a mailbox is processed, the DPT and RPTs are applied to the mailbox and default folders, and personal tags become available in Outlook and Outlook Web App. Retention action is taken on messages based on tag settings.



## Folder and message with a Personal tag

Users apply a personal tag to a custom folder. Items in folders can have a different personal tag applied.

# Aufbewahrungstags

Wie in der vorherigen Abbildung dargestellt, werden aufbewahrungstags verwendet, Ordnern und einzelnen Elementen wie E-mail-Nachrichten und Voicemail-Einstellungen für die Aufbewahrung zuweisen. Diese Einstellungen angeben, wie lange eine Nachricht verbleibt in einem Postfach und die Aktion, die ausgeführt werden soll, wenn die Meldung die angegebenen Aufbewahrungszeitraum erreicht. Wenn eine Nachricht den Aufbewahrungszeitraum erreicht, hat des Benutzers Compliance-Archiv verschoben oder gelöscht.

new tag applied automatically to entire mailbox (default)

\*Name:

DPT - Delete 7 Years

Retention action:

- Delete and Allow Recovery
- Permanently Delete
- Move to Archive

Retention action specifies the action that will be taken on an item

The tag type determines where and how a retention tag applies

Retention period:

- Never
- When the item reaches the following age (in days):

2555

Retention period specifies when the selected action will be taken

Comment:

Delete all items after 7 years (2555 days)

save

cancel

Mithilfe von Aufbewahrungstags können Benutzer ihre eigenen Postfachordner und einzelne Elemente für die Aufbewahrung kennzeichnen. Die Benutzer müssen Elemente nicht länger in verwalteten Ordner archivieren, die von einem Administrator auf Grundlage der Anforderungen für die Nachrichtenaufbewahrung bereitgestellt werden.

### Typen von Aufbewahrungstags

Aufbewahrungstags werden in die folgenden drei Typen unterteilt, je nachdem, wer sie anwenden kann und wo in einem Postfach sie angewendet werden können.

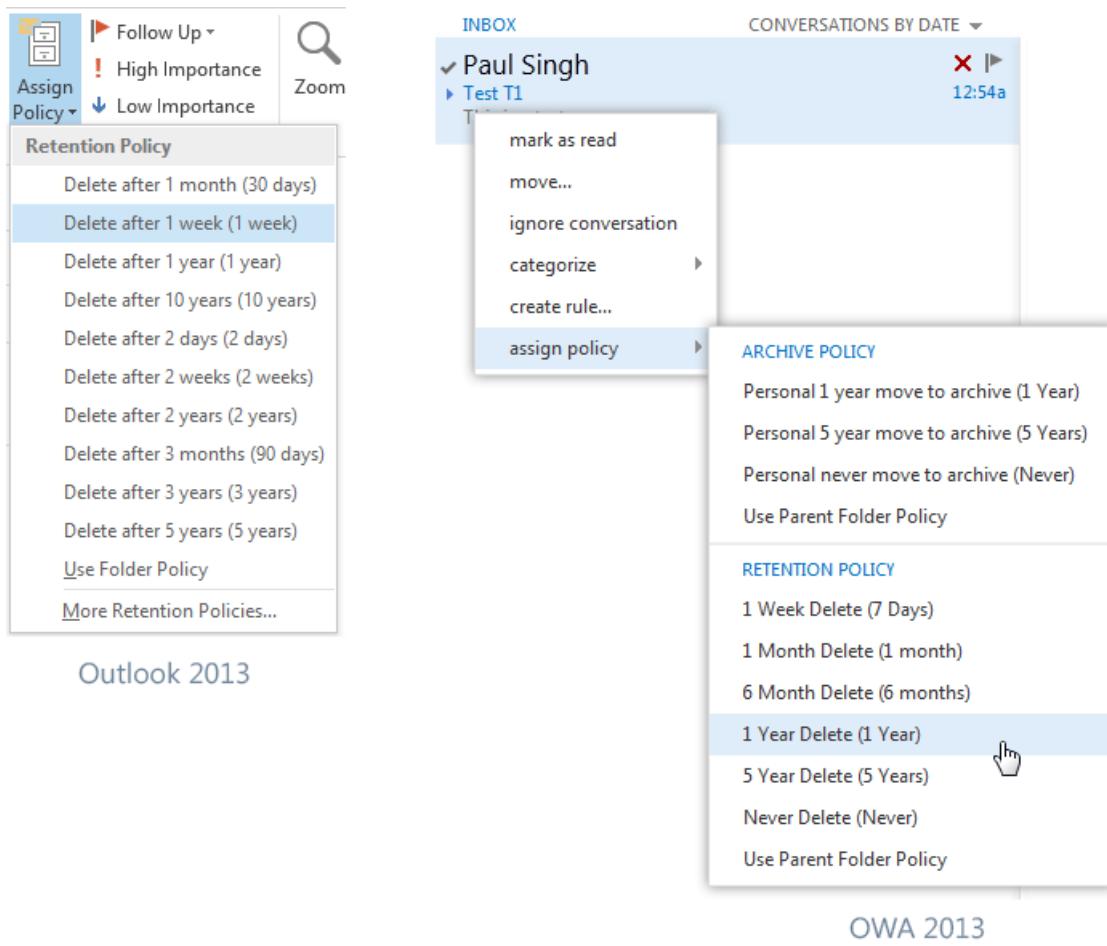
TYP DES AUFBEWAHRUNGSTAGS	ANGEWENDET...	ANGEWENDET VON...	VERFÜGBARE AKTIONEN...	DETAILS

TYP DES AUFBEWAHRUNGSTAGS	ANGEWENDET...	ANGEWENDET VON...	VERFÜGBARE AKTIONEN...	DETAILS
Standardrichtlinientag	Automatisch auf das gesamte Postfach Ein Standardrichtlinientag wird auf nicht gekennzeichnete Elemente angewendet, d. h. Elemente, auf die Aufbewahrungstags weder direkt noch durch Vererbung über den Ordner angewendet wurden.	Administrator	In Archiv verschieben Löschen und Wiederherstellung zulassen Permanent löschen	Benutzer können auf ein Postfach angewendete Standardrichtlinientags nicht ändern.
Aufbewahrungsrichtlinientag	Automatisch auf einen Standardordner Standardordner sind Ordner, die in allen Postfächern automatisch erstellt werden. Beispiel: <b>Posteingang, Gelöschte Elemente und Gesendete Elemente.</b> Eine Liste der unterstützten Standardorder finden Sie unter <a href="#">Standardordner, die Aufbewahrungsrichtlinientags unterstützen.</a>	Administrator	Löschen und Wiederherstellung zulassen Permanent löschen	Benutzer können auf einen Standardordner angewendete Standardrichtlinientags nicht ändern.

TYP DES AUFBEWAHRUNGSTAGS	ANGEWENDET...	ANGEWENDET VON...	VERFÜGBARE AKTIONEN...	DETAILS
Persönliches Tag	Manuell auf Elemente und Ordner Benutzer können die Kennzeichnung mithilfe von Posteingangsregeln automatisieren, um eine Nachricht entweder in einen Ordner zu verschieben, der über ein bestimmtes Tag verfügt, oder um ein persönliches Tag auf die Nachricht anzuwenden.	Benutzer	In Archiv verschieben Löschen und Wiederherstellung zulassen Permanent löschen	Persönliche Tags ermöglichen Benutzern zu bestimmen, wie lange ein Element beibehalten werden soll. Beispiel: Das Postfach kann über ein Standardrichtlinientag verfügen, damit Elemente nach sieben Jahren gelöscht werden. Benutzer können jedoch eine Ausnahme für Elemente wie beispielsweise Newsletter oder automatische Benachrichtigungen erstellen, indem sie ein persönliches Tag anwenden, sodass diese Elemente nach drei Tagen gelöscht werden.

### Weitere Informationen zu persönlichen Tags

Persönliche Tags sind als Teil ihrer Aufbewahrungsrichtlinie für Outlook 2010 und Outlook Web App-Benutzer verfügbar. In Outlook 2010 und Outlook Web App mit der Aktion **in Archiv verschieben** persönliche Tags als **Archivrichtlinie** und persönliche Tags mit den Aktionen **Löschen und Wiederherstellung zulassen** oder **Endgültig löschen** angezeigt als \*\*Aufbewahrungsrichtlinie \*\*, wie in der folgenden Abbildung dargestellt.



Benutzer können persönliche Tags auf von ihnen erstellte Ordner oder auf einzelnen Elementen anwenden. Nachrichten, auf die persönlichen Tags angewendet sind, werden immer auf der Basis der Einstellungen der persönlichen Tags verarbeitet. Benutzer können ein persönliches Tag auf eine Nachricht anwenden, sodass diese früher oder später verschoben oder gelöscht wird, als durch das Standardrichtlinientag oder die Aufbewahrungsrichtlinientags angegeben ist, die auf das Postfach dieses Benutzers angewendet wurden. Sie können außerdem persönliche Tags erstellen, in denen die Aufbewahrung deaktiviert ist. Hierdurch ist es Benutzern möglich, Elemente so zu kennzeichnen, dass diese nie in ein Archiv verschoben werden oder nie ablaufen.

#### NOTE

Benutzer können Archivrichtlinien auf Standardordner, auf von Benutzern erstellte Ordner oder Unterordner und auf einzelne Elemente anwenden. Benutzer können eine Aufbewahrungsrichtlinie auf von Benutzern erstellte Ordner oder Unterordner und auf einzelne Elemente (was auch Unterordner und Elemente in einem Unterordner einschließt), jedoch nicht auf Standardordner anwenden.

Benutzer können auch im Exchange Administrationscenter (EAC) verwenden, um zusätzliche Persönliche Tags auszuwählen, die mit ihrer Aufbewahrungsrichtlinie verknüpft sind. Den ausgewählten Tags verfügbar, klicken Sie dann in Outlook 2010 und Outlook Web App. Damit Benutzer aus der Exchange-Verwaltungskonsole zusätzliche Tags auswählen können, müssen Sie die [MyRetentionPolicies Rolle](#) des Benutzers rollenzuweisungsrichtlinie hinzufügen. Weitere Informationen zu rollenzuweisungsrichtlinien für Benutzer finden Sie unter [Understanding Management Rollenzuweisungsrichtlinien](#). Wenn Sie Benutzer zusätzliche Persönliche Tags auswählen können, werden alle persönlichen Tags in Ihrer Exchange-Organisation zur Verfügung.

## NOTE

Persönliche Tags sind ein Premium-Feature. Für Postfächer mit Richtlinien, die diese Tags enthalten (oder diese Tags aufweisen, weil Benutzer die Tags zu ihrem Postfach hinzugefügt haben), ist eine Exchange Enterprise-Clientzugriffs Lizenz (CAL) erforderlich.

## Aufbewahrungszeitraum

Wenn Sie einen Aufbewahrungstag aktivieren, müssen Sie einen Aufbewahrungszeitraum für das Tag angeben. Dieser Zeitraum gibt die Anzahl der Tage an, die eine Nachricht aufbewahrt wird, nachdem sie im Postfach des Benutzers eingegangen ist.

Der Aufbewahrungszeitraum für nicht wiederkehrende Elemente (z. B. E-Mail-Nachrichten) wird anders berechnet als für Elemente mit Enddatum oder für Serienelemente (z. B. Besprechungen und Aufgaben). Informationen zum Berechnen des Aufbewahrungszeitraums für verschiedene Elementtypen finden Sie unter [Berechnung von Aufbewahrungszeiträumen](#).

Sie können auch Aufbewahrungstags mit deaktivierter Aufbewahrung erstellen oder die Tags nach der Erstellung deaktivieren. Da Nachrichten mit deaktiviertem Tag nicht verarbeitet werden, findet keine Aufbewahrungsaktion statt. Daher können Benutzer ein deaktiviertes persönliches Tag als **Nie verschieben-** oder **Nie löschen**-Tag verwenden, um ein Standardrichtlinientag oder ein Aufbewahrungsrichtlinientag außer Kraft zu setzen, das ansonsten auf die Nachricht angewendet werden würde.

## Aufbewahrungsaktionen

Beim Erstellen oder Konfigurieren eines Aufbewahrungstags können Sie eine der folgenden Aufbewahrungsaktionen auswählen, die ausgeführt werden, wenn für ein Element das Ende des Aufbewahrungszeitraums erreicht ist:

AUFBEWAHRUNGSAKTION	AKTION...	MIT AUSNAHME DER...
<b>In Archiv verschieben<sup>1</sup></b>	Verschiebt die Nachricht in das Archivpostfach des Benutzers Nur verfügbar für Standardrichtlinientags und persönliche Tags Weitere Informationen zur Archivierung finden Sie unter: <a href="#">In-Situ-Archivierung</a> <a href="#">Archivieren von Postfächern in Exchange Online</a>	Wenn der Benutzer nicht über ein Archivpostfach verfügt, wird keine Aktion durchgeführt.
<b>Löschen und Wiederherstellung zulassen</b>	Emuliert das Verhalten, wenn der Benutzer den Ordner "Gelöschte Elemente" leert. Elemente sind in den <a href="#">Ordner "wiederherstellbare Elemente"</a> im Postfach verschoben und erhalten bleiben, bis die Aufbewahrungszeit für gelöschte. Ermöglicht dem Benutzer, die zweite Möglichkeit, das Element mithilfe des Dialogfelds <b>Gelöschte Elemente wiederherstellen</b> wiederherstellen im Feld in Outlook oder Outlook Web App	Wenn Sie die Aufbewahrungszeit für gelöschte Elemente auf Null Tage festgelegt haben, werden die Elemente dauerhaft gelöscht. Weitere Informationen hierzu finden Sie unter <a href="#">ändern wie lange dauerhaft gelöscht Elemente für ein Exchange Online-Postfach aufbewahrt werden</a> .

AUFBEWARUNGSAKTION	AKTION...	MIT AUSNAHME DER...
<b>Endgültig löschen</b>	Nachrichten werden dauerhaft gelöscht. Nachrichten können nicht wiederhergestellt werden, nachdem sie dauerhaft gelöscht wurden.	Wenn für das Postfach <a href="#">In-Situ-Speicher und Beweissicherungsverfahren</a> oder das Beweissicherungsverfahren aktiviert wurde, werden Elemente im Ordner "Wiederherstellbare Elemente" basierend auf den entsprechenden Parametern beibehalten. <a href="#">Compliance-eDiscovery</a> gibt diese Elemente weiterhin in den Suchergebnissen zurück.
<b>Markieren Sie als nach dem Aufbewahrungslimit</b>	Markiert die Nachricht als abgelaufen. In Outlook 2010 oder höher und Outlook Web App werden abgelaufene Elemente mit der Benachrichtigung Auskunft über 'dieses Element ist abgelaufen' und "dieses Element läuft in 0 Tagen" angezeigt. In Outlook 2007 werden als abgelaufen gekennzeichnete Elementen mithilfe von durchgestrichenen Text angezeigt.	N/V

#### NOTE

<sup>1</sup> in einer Exchange-hybridbereitstellung, können Sie eine Cloud-basierten Archivpostfach für eine lokale Hauptpostfach aktivieren. Wenn Sie eine Richtlinie für die Archivierung auf ein lokales Postfach zuweisen, werden die Elemente in der cloudbasierten Archiv verschoben. Wenn ein Element in das Archivpostfach verschoben wurde, wird nicht im lokalen Postfach eine Kopie davon beibehalten. Wenn das lokale Postfach in die Warteschleife gestellt wird, werden weiterhin auf ein Archivrichtlinie Elemente in das Cloud-basierten Archivpostfach verschoben, in dem sie für die Dauer, die durch den Haltestatus angegebenen beibehalten werden.

Weitere Informationen zum Erstellen von Aufbewahrungstags finden Sie unter [Erstellen einer Aufbewahrungsrichtlinie](#).

## Aufbewahrungsrichtlinien

Zur Anwendung von mindestens einem Aufbewahrungstag auf ein Postfach müssen Sie die Tags zu einer Aufbewahrungsrichtlinie hinzufügen und anschließend die Richtlinie auf das Postfach anwenden. Ein Postfach kann nur eine Aufbewahrungsrichtlinie aufweisen. Aufbewahrungstags können jederzeit mit einer Aufbewahrungsrichtlinie verknüpft bzw. eine derartige Verknüpfung kann jederzeit aufgehoben werden. Die Änderungen werden dann für alle Postfächer automatisch wirksam, auf die die Richtlinie angewendet wird.

Eine Aufbewahrungsrichtlinie kann die folgenden Aufbewahrungstags aufweisen:

AUFBEWARUNGSTAGTYP	TAGS IN EINER RICHTLINIE
Standardrichtlinientag	Ein Standardrichtlinientag mit der Aktion <b>In Archiv verschieben</b> Ein Standardrichtlinientag mit der Aktion <b>Löschen und Wiederherstellung zulassen</b> oder <b>Endgültig löschen</b> Ein Standardrichtlinientag für Voicemailnachrichten mit der Aktion <b>Löschen und Wiederherstellung zulassen</b> oder <b>Endgültig löschen</b>

AUFBEWAHRUNGSTAGTYP	TAGS IN EINER RICHTLINIE
Aufbewahrungsrichtlinientags	<p>Ein Aufbewahrungsrichtlinientag für jeden unterstützten Standardordner</p> <p>&gt; [!NOTE]&gt; Sie können nicht mehr als ein Aufbewahrungsrichtlinientag für einen bestimmten Standardordner (z. B. <b>Gelöschte Elemente</b>) mit derselben Aufbewahrungsrichtlinie verknüpfen.</p>
Persönliche Tags	<p>Eine beliebige Anzahl von persönlichen Tags</p> <p>&gt; [!TIP]&gt; Viele persönliche Tags in einer Richtlinie können für Benutzer verwirrend sein. Es wird empfohlen, einer Aufbewahrungsrichtlinie nicht mehr als 10 persönliche Tags hinzuzufügen.</p>

#### NOTE

Auch wenn Sie eine Aufbewahrungsrichtlinie nicht zwingend mit Aufbewahrungstags verknüpfen müssen; wird ein solches Szenario trotzdem nicht empfohlen. Wenn keine Aufbewahrungstags mit Postfächern mit Aufbewahrungsrichtlinien verknüpft sind, kann dies dazu führen, dass die Postfachelemente niemals ablaufen.

Eine Aufbewahrungsrichtlinie kann sowohl Archivtags (Tags, mit denen Elemente in das persönliche Archivpostfach verschoben werden) als auch Löschungstags (Tags, die Elemente löschen) enthalten. Auf ein Postfachelement können ebenfalls beide Arten von Tags angewendet werden. Archivpostfächer verfügen über keine separate Aufbewahrungsrichtlinie. Dieselbe Aufbewahrungsrichtlinie wird auf das primäre und das Archivpostfach angewendet.

Bei der Planung von Aufbewahrungsrichtlinien zu erstellen, müssen Sie berücksichtigen, ob sie Archiv und Löschung-Tags enthalten werden. Wie bereits erwähnt, kann eine Aufbewahrungsrichtlinie ein standardrichtlinientag Aktion, die die Aktion **in Archiv verschieben** verwendet und eine DPT, die **entweder die löschen und Wiederherstellung zulassen** oder **Endgültig löschen** -Aktion verwendet haben. Die Standardrichtlinientag mit der Aktion **in Archiv verschieben** benötigen eine niedrigere Aufbewahrungszeitraum als die DPT mit einer Aktion löschen. Beispielsweise können Sie ein Standardrichtlinientag mit der Aktion **in Archiv verschieben** Verschieben von Elementen in das Archivpostfach in zwei Jahre und ein Standardrichtlinientag mit einer Aktion Löschen verwenden, um Elemente aus dem Postfach in sieben Jahren zu entfernen. Elemente in Primär- und archivpostfächer werden nach sieben Jahren gelöscht.

Eine Liste der Verwaltungsaufgaben im Zusammenhang mit den Aufbewahrungsrichtlinien finden Sie unter [Messaging Records Management Procedures](#).

#### Standardaufbewahrungsrichtlinie

Exchange-Setup erstellt die Aufbewahrungsrichtlinie **MRM-Standardrichtlinie**. Der MRM-Standardrichtlinie wird automatisch in neuen Postfächer in Exchange Online angewendet. In Exchange Server wird die Richtlinie automatisch angewendet, wenn Sie ein Archiv für den neuen Benutzer erstellen, und geben Sie an einer Aufbewahrungsrichtlinie

Sie können Tags modifizieren, die in der MRM-Standardrichtlinie enthalten sind, z. B., indem Sie die Verfallszeit für die Aufbewahrung oder die Aufbewahrungsaktion ändern, ein Tag deaktivieren oder die Richtlinie ändern, indem Sie Tags zu ihr hinzufügen oder aus ihr entfernen. Die aktualisierte Richtlinie wird ab der nächsten Verarbeitung von Postfächern durch den [Assistent für verwaltete Ordner](#) auf die Postfächer angewendet.

Genauere Informationen, darunter eine Liste von mit der Richtlinie verknüpften Aufbewahrungs-Tags finden Sie unter [Standardaufbewahrungsrichtlinie in Exchange Online und Exchange Server](#).

# Assistent für verwaltete Ordner

Der Assistent für verwaltete Ordner, ein auf Postfachservern ausgeführter Postfach-Assistent, verarbeitet Postfächer, auf die eine Aufbewahrungsrichtlinie angewendet wird.

Der Assistent für verwaltete Ordner wendet die Aufbewahrungsrichtlinie an, indem die Elemente im Postfach untersucht werden und somit ermittelt wird, ob diese aufbewahrt werden müssen. Elemente, die der Aufbewahrung unterliegen, werden dann mit den entsprechenden Aufbewahrungstags versehen, und die angegebene Aufbewahrungsaktion wird für Elemente ausgeführt, deren Aufbewahrungslimit überschritten wurde.

Der Assistent für verwaltete Ordner ist ein einschränkungsbasierter Assistent. Einschränkungsbasierte Assistenten werden immer ausgeführt und müssen nicht eingeplant werden. Die Systemressourcen, die von ihnen beansprucht werden können, sind eingeschränkt. Sie können den Assistenten für verwaltete Ordner so konfigurieren, dass dieser alle Postfächer auf dem Postfachserver innerhalb eines bestimmten Zeitraums verarbeitet (auch als Arbeitszyklus bezeichnet). Zusätzlich aktualisiert der Assistent in einem angegebenen Intervall (auch als Arbeitszyklusprüfzeitpunkt bezeichnet) die Liste der zu verarbeitenden Postfächer. Während der Aktualisierung fügt der Assistent neu erstellte oder verschobene Postfächer zur Warteschlange hinzu. Er weist vorhandenen Postfächern auch neue Prioritäten zu, die aufgrund von Fehlern nicht erfolgreich verarbeitet wurden und verschiebt sie in der Warteschlange nach vorne, damit Sie im gleichen Arbeitszyklus verarbeitet werden können.

Sie können auch das Cmdlet [Start-ManagedFolderAssistant](#) verwenden, um den Assistenten für die Verarbeitung eines Postfachs manuell auszulösen. Weitere Informationen finden Sie unter [Konfigurieren des Assistenten für verwaltete Ordner](#).

## NOTE

Der Assistent für verwaltete Ordner führt keine Aktion für Nachrichten aus, die nicht der Aufbewahrung unterliegen, was durch Deaktivieren des Aufbewahrungstags angegeben wird. Sie können ein Aufbewahrungstag auch deaktivieren, um die Verarbeitung von Elementen mit diesem Tag temporär einzustellen.

## Verschieben von Elementen zwischen Ordnern

Ein Postfachelement, das von einem Ordner in einen anderen verschoben wird, erbt ggf. alle Tags, die auf den Zielordner angewendet wurden. Wenn ein Element in einen Ordner verschoben wird, dem kein Tag zugewiesen wurde, wird das Standardrichtlinientag angewendet. Wenn dem Element ein Tag explizit zugewiesen wurde, hat dieses Tag immer Vorrang gegenüber allen Tags auf Ordnerebene sowie gegenüber dem Standardtag.

## Anwenden eines Aufbewahrungstags auf einen Ordner im Archiv

Wenn der Benutzer ein persönliches Tag auf einen Ordner im Archiv anwendet und im primären Postfach ein Ordner mit dem gleichen Namen, aber einem anderen Tag existiert, wird das Tag für diesen Ordner im Archiv so geändert, dass es mit dem im primären Postfach übereinstimmt. Dadurch wird Verwechslungen bei Elementen in einem Ordner im Archiv vorgebeugt, die ein anderes Ablaufverhalten aufweisen als der gleiche Ordner im primären Postfach des Benutzers. Beispiel: Der Benutzer besitzt im primären Postfach einen Ordner mit dem Namen "Project Contoso" und dem Tag Löschen - 3 Jahre. Außerdem enthält auch das Archivpostfach einen Ordner mit dem Namen "Project Contoso". Der Benutzer wendet ein persönliches Löschen - 1 Jahr-Tag an, um Elemente im Ordner nach 1 Jahr zu löschen. Wenn das Postfach erneut verarbeitet wird, wird der Ordner auf das Tag "Löschen - 3 Jahre" zurückgesetzt.

## Entfernen oder Löschen eines Aufbewahrungstags aus einer Aufbewahrungsrichtlinie

Wenn ein Aufbewahrungstag aus der auf ein Postfach angewendeten Aufbewahrungsrichtlinie entfernt wird, steht das Tag nicht mehr für den Benutzer zur Verfügung und kann nicht auf Elemente im Postfach angewendet werden.

Vorhandene Elemente, auf die dieses Tag angewendet wurde, werden weiterhin anhand dieser Einstellungen vom Assistenten für verwaltete Ordner verwaltet, und alle im Tag angegebenen Aufbewahrungsaktionen werden auf diese Nachrichten angewendet.

Wenn Sie das Tag jedoch löschen, wird die in Active Directory gespeicherte Definition entfernt. Das führt dazu, dass der Assistent für verwaltete Ordner alle Elemente in einem Postfach verarbeitet und diejenigen mit einem neuen Tag versieht, auf die das entfernte Tag angewendet wurde. Je nach Anzahl von Postfächern und Nachrichten kann dieser Prozess erhebliche Ressourcen auf allen Postfachservern in Anspruch nehmen, die Postfächer mit Aufbewahrungsrichtlinien enthalten, in denen das entfernte Tag enthalten war.

#### **IMPORTANT**

Wenn ein Aufbewahrungstag aus einer Aufbewahrungsrichtlinie entfernt wird, verlieren ggf. alle vorhandenen Postfachelemente, auf die das Tag angewendet wurde, ihre Gültigkeit weiterhin laut den Einstellungen im Tag. Wenn Sie verhindern möchten, dass die Einstellungen des Tags weiterhin auf Elemente angewendet werden, sollten Sie das Tag löschen. Indem Sie ein Tag löschen, entfernen Sie es aus allen Aufbewahrungsrichtlinien, in denen es enthalten ist.

#### **Deaktivieren eines Aufbewahrungstags**

Wenn Sie einen Aufbewahrungstag deaktivieren, ignoriert der Assistent für verwaltete Ordner Elemente, auf die dieses Tag angewendet wurde. Elemente mit einem Aufbewahrungstag, für das die Aufbewahrung deaktiviert ist, werden in Abhängigkeit von der angegebenen Aufbewahrungsaktion entweder nie verschoben oder nie gelöscht. Da diese Elemente weiterhin als mit einem Tag markierte Elemente angesehen werden, wird auf sie nicht das Standardrichtlinientag angewendet. Wenn Sie beispielsweise eine Problembehandlung für Einstellungen von Aufbewahrungstags durchführen möchten, können Sie einen Aufbewahrungstag vorübergehend deaktivieren, um zu verhindern, dass der Assistent für verwaltete Ordner Nachrichten mit diesem Tag verarbeitet.

#### **NOTE**

Die Aufbewahrungszeit für einen Aufbewahrungstag deaktiviert wird dem Benutzer **nie** angezeigt. Wenn ein Benutzer ein Element glaubt, dass es nie gelöscht werden soll, aktivieren das Tag später unbeabsichtigten Löschens von Elementen möglicherweise den Benutzer nicht löschen möchten. Dies gilt auch für Tags mit der Aktion **in Archiv verschieben**.

## Anhalten der Aufbewahrungszeit

Wenn Benutzer vorübergehend abwesend sind und keinen Zugriff auf ihre e-Mail-Nachrichten, können Einstellungen für die Aufbewahrung auf neue Nachrichten angewendet werden, bevor sie erneut zu arbeiten, oder greifen Sie auf ihre e-Mails. Je nach der Aufbewahrungsrichtlinie werden Nachrichten gelöscht oder in der Benutzer Persönliche Archiv verschoben. Sie können vorübergehend Aufbewahrung unterbrechen, die die Verarbeitung eines Postfachs für einen bestimmten Zeitraum durch Platzieren des Postfachs zur Aufbewahrung von Richtlinien enthalten. Beim Platzieren eines Postfachs zur Aufbewahrung von halten, Sie können auch angeben, ein Aufbewahrung Kommentar, der den Postfachbenutzer (oder einen anderen Benutzer autorisiert, das Postfach zugegriffen hat) über die Aufbewahrung informiert halten, einschließlich, wenn die Sperre geplant ist, beginnen und enden. Aufbewahrung Kommentare werden in unterstützten Outlook-Clients angezeigt. Sie können auch den Retention Hold Kommentar im bevorzugte Sprache des Benutzers lokalisieren.

#### **NOTE**

Das Anhalten der Aufbewahrungszeit für ein Postfach hat keine Auswirkung auf die Verarbeitung von Speichercontingenten für das Postfach. Abhängig von der Speicherverwendung des Postfachs und den anwendbaren Postfachcontingenten sollten Sie möglicherweise das Speichercontingent des Postfachs für Benutzer erhöhen, die für längere Zeit in Urlaub sind oder nicht über Zugriff auf E-Mail verfügen. Weitere Informationen zu Speichercontingenten für Postfächer finden Sie unter [Configure Storage Quotas for a Mailbox](#).

Für Benutzer, die lange nicht am Arbeitsplatz sind, können sich sehr viele E-Mails ansammeln. Abhängig von der Anzahl der E-Mails und der Dauer der Abwesenheit können diese Benutzer einige Wochen benötigen, um ihre Nachrichten durchzusehen. Berücksichtigen Sie in diesen Fällen die zusätzliche Zeit, die die Benutzer möglicherweise benötigen, um ihre E-Mails aufzuarbeiten, bevor Sie das Anhalten der Aufbewahrungszeit beenden.

Wenn in Ihrem Unternehmen keine Messaging-Datensatzverwaltung implementiert wurde und die Benutzer mit deren Funktionen nicht vertraut sind, können Sie während der anfänglichen Aufwärm- und Schulungsphase für die Bereitstellung der Messaging-Datensatzverwaltung auch Aufbewahrungszeiten verwenden. Sie können Aufbewahrungsrichtlinien erstellen und bereitstellen sowie die Benutzer über die Richtlinien in Kenntnis setzen, ohne zu riskieren, dass Elemente verschoben oder gelöscht werden, bevor diese von Benutzern markiert werden können. Wenige Tage vor dem Ende der Aufwärm- und Schulungsphase sollten Sie die Benutzer an die Aufwärmfrist erinnern. Nachdem die Frist abgelaufen ist, können Sie die Aufbewahrungszeit für Postfächer entfernen, wodurch der Assistent für verwaltete Ordner die Möglichkeit erhält, Postfachelemente zu verarbeiten und die angegebene Aufbewahrungsaktion durchzuführen.

Weitere Informationen zum Anhalten der Aufbewahrungszeit für ein Postfach finden Sie unter [Anhalten der Aufbewahrungszeit für ein Postfach](#).

# Standardaufbewahrungsrichtlinie in Exchange Online und Exchange Server

18.12.2018 • 5 minutes to read

Exchange erstellt die Aufbewahrungsrichtlinie "MRM-Standardrichtlinie" in Exchange Online und der lokalen Exchange-Organisation. Die Richtlinie wird automatisch auf neue Benutzer in Exchange Online angewendet. In lokalen Organisationen wird die Richtlinie angewendet, wenn Sie ein Archiv für das Postfach erstellen. Sie können die auf einen Benutzer angewendete Aufbewahrungsrichtlinie jederzeit ändern.

Sie können Tags modifizieren, die in der MRM-Standardrichtlinie enthalten sind, z. B., indem Sie die Verfallszeit für die Aufbewahrung oder die Aufbewahrungsaktionen ändern, ein Tag deaktivieren oder die Richtlinie ändern, indem Sie Tags zu ihr hinzufügen oder aus ihr entfernen. Die aktualisierte Richtlinie wird ab der nächsten Verarbeitung von Postfächern durch den Assistenten für verwaltete Ordner auf die Postfächer angewendet.

## Mit der MRM-Standardrichtlinie verknüpfte Aufbewahrungstags

In der folgenden Tabelle sind die Standardaufbewahrungstags aufgeführt, die mit der MRM-Standardrichtlinie verknüpft sind.

NAME	TYP	AUFBEWARUNGSEITRAUM (TAGE)	AUFBEWARUNGSAKTION
Standard, 2 Jahre, in Archiv verschieben	Standardrichtlinientag	730	In Archiv verschieben
Wiederherstellbare Elemente, 14 Tage, in Archiv verschieben	Ordner "Wiederherstellbare Elemente"	14	In Archiv verschieben
Persönlich, 1 Jahre, in Archiv verschieben	Persönliches Tag	365	In Archiv verschieben
Persönlich, 5 Jahre, in Archiv verschieben	Persönliches Tag	1,825	In Archiv verschieben
Persönlich, nie in Archiv verschieben	Persönliches Tag	Nicht zutreffend	In Archiv verschieben
1 Woche, löschen	Persönliches Tag	7	Löschen und Wiederherstellung zulassen
1 Monat, löschen	Persönliches Tag	30	Löschen und Wiederherstellung zulassen
6 Monate, löschen	Persönliches Tag	180	Löschen und Wiederherstellung zulassen
1 Jahr, löschen	Persönliches Tag	365	Löschen und Wiederherstellung zulassen

NAME	TYP	AUFBEWARUNGZEITRAUM (TAGE)	AUFBEWARUNGSAKTION
5 Jahre, löschen	Persönliches Tag	1,825	Löschen und Wiederherstellung zulassen
Nie löschen	Persönliches Tag	Nicht zutreffend	Löschen und Wiederherstellung zulassen

## Möglichkeiten der MRM-Standardrichtlinie

SIE KÖNNEN...	IN DER EXCHANGE ONLINE...	IN EXCHANGE SERVER...
Automatisches Anwender der MRM-Standardrichtlinie auf neue Benutzer	Ja, standardmäßig angewendet. Es ist keine Aktion erforderlich.	Ja, standardmäßig angewendet, wenn Sie auch ein Archiv für den neuen Benutzer erstellen. Wenn Sie später ein Archiv für den Benutzer erstellen, wird die Richtlinie nur dann automatisch angewendet, wenn der Benutzer keine vorhandene Aufbewahrungsrichtlinie hat.
Ändern des Aufbewahrungsalters oder der Aufbewahrungsaktion eines Aufbewahrungstags, das mit der Richtlinie verknüpft ist	Ja	Ja
Deaktivieren eines Aufbewahrungstags, das mit der Richtlinie verknüpft ist	Ja	Ja
Hinzufügen eines Aufbewahrungstags zur Richtlinie	Ja	Ja
Entfernen eines Aufbewahrungstags aus der Richtlinie	Ja	Ja
Festlegen einer anderen Richtlinie als Standardaufbewahrungsrichtlinie, die automatisch auf neue Benutzer angewendet wird	Nein	Nein

## Weitere Informationen

- Ein Aufbewahrungstag kann mit mehr als einer Aufbewahrungsrichtlinie verknüpft werden. Weitere Informationen zum Verwalten von [Aufbewahrungstags](#) und [Aufbewahrungsrichtlinien](#) finden Sie unter [Verfahren der Messaging-Datensatzverwaltung](#).
- Die MRM-Standardrichtlinie enthält kein Standardrichtlinientag, um Elemente (sie enthält jedoch persönliche Tags mit der Aufbewahrungsaktion zum Löschen, die Benutzer auf ihre Postfachelemente anwenden können) automatisch zu löschen. Wenn Sie Elemente nach einer bestimmten Zeit automatisch löschen möchten, können Sie ein Standardrichtlinientag mit der erforderlichen Löschaktion erstellen und es der Richtlinie hinzufügen. Ausführliche Informationen finden Sie unter [Erstellen einer Aufbewahrungsrichtlinie](#) und [Hinzufügen von Aufbewahrungstags zu oder Entfernen von Aufbewahrungstags aus einer Aufbewahrungsrichtlinie](#).
- Aufbewahrungsrichtlinien werden auf die Postfachbenutzer angewendet. Für das Postfach und das Archiv

des Benutzers gilt dieselbe Richtlinie.

# Standardordner, die Aufbewahrungsrichtlinientags unterstützen

18.12.2018 • 8 minutes to read

Sie können [Aufbewahrungstags](#) und [Aufbewahrungsrichtlinien](#) verwenden, um den E-Mail-Lebenszyklus zu verwalten. Aufbewahrungsrichtlinien enthalten Aufbewahrungstags, die Einstellungen darstellen, mit denen Sie festlegen können, wann eine Nachricht automatisch in das Archiv verschoben und wann es gelöscht werden soll.

Ein Aufbewahrungsrichtlinientag (Retention Policy Tag, RPT) ist eine Art Aufbewahrungstag, das Sie auf Standardordner in einem Postfach, wie z. B. **Posteingang** und **Gelöschte Elemente**, anwenden können.

new tag applied automatically to a default folder Help

\*Name:

Apply this tag to the following default folder:

Retention tag names are displayed to users in Microsoft Outlook and Outlook Web App along with the retention period.

Retention action:  
 Delete and Allow Recovery  
 Permanently Delete

Retention period:  
 Never  
 When the item reaches the following age (in days):

Comment:

save cancel

## Unterstützte Standardordner

Sie können Aufbewahrungsrichtlinientags für die in der folgenden Tabelle aufgeführten Standardordner erstellen.

ORDNERNAME	DETAILS
Archiv	<p>Dieser Ordner ist das standardmäßige Ziel für Nachrichten, die mit der Schaltfläche zum Archivieren in Outlook archiviert werden. Das Feature für die Archivierung bietet eine schnelle Möglichkeit für Benutzer, Nachrichten aus dem Posteingang zu entfernen, ohne sie zu löschen.</p> <p>Dieser RPT ist nur in Exchange Online verfügbar.</p>
Kalender	<p>In diesem Standardordner werden Besprechungen und Termine gespeichert.</p>
Unwichtige Elemente	<p>Dieser Ordner enthält E-Mails mit niedriger Priorität. „Unwichtige Elemente“ prüft Ihre in der Vergangenheit vorgenommenen Aktionen, um zu bestimmen, welche Nachrichten Sie wahrscheinlich ignorieren. Es verschiebt diese Nachrichten dann in den Ordner <b>Unwichtige Elemente</b>.</p>
Aufgezeichnete Unterhaltungen	<p>Dieser Ordner wird von Microsoft Lync (ehemals Microsoft Office Communicator) erstellt. Obwohl dieser Ordner von Outlook nicht als Standardordner behandelt wird, wird er von Exchange als spezieller Ordner behandelt, auf den Aufbewahrungsrichtlinientags angewendet werden können.</p>
Gelöschte Elemente	<p>In diesem Ordner werden Elemente gespeichert, die aus anderen Ordnern im Postfach gelöscht wurden. Benutzer von Outlook und Outlook Web App können diesen Ordner manuell leeren. Sie können Outlook auch derart konfigurieren, dass der Ordner beim Schließen von Outlook geleert wird.</p>
Entwürfe	<p>In diesem Ordner werden Nachrichtenentwürfe gespeichert, die vom Benutzer noch nicht gesendet wurden. In Outlook Web App wird dieser Ordner auch zum Speichern von Nachrichten verwendet, die vom Benutzer gesendet, aber noch nicht an den Hub-Transport-Server übermittelt wurden.</p>
Posteingang	<p>In diesem Standardordner werden Nachrichten gespeichert, die an ein Postfach zugestellt wurden.</p>
Journal	<p>Dieser Standardordner enthält vom Benutzer ausgewählte Aktionen. Diese Aktionen werden automatisch von Outlook aufgezeichnet und in einer Zeitachsenansicht angezeigt.</p>
Junk-E-Mail	<p>In diesem Standardordner werden Nachrichten gespeichert, die vom Inhaltsfilter auf einem Exchange-Server oder vom Antispamfilter in Outlook als Junk-E-Mails gekennzeichnet wurden.</p>
Notizen	<p>In diesem Ordner werden die von Benutzern in Outlook erstellten Notizen gespeichert. Diese Notizen werden auch in Outlook Web App angezeigt.</p>
Postausgang	<p>In diesem Standardordner werden vom Benutzer gesendete Nachrichten temporär gespeichert, bis diese an einen Hub-Transport-Server übermittelt werden. Eine Kopie der gesendeten Nachrichten wird im Standardordner "Gesendete Elemente" gespeichert. Da die Nachrichten nur für kurze Zeit in diesem Ordner verbleiben, ist es nicht erforderlich, ein Aufbewahrungsrichtlinientag für diesen Ordner zu erstellen.</p>

ORDNERNAME	DETAILS
RSS-Feeds	In diesem Standardordner sind die RSS-Feeds enthalten.
Wiederherstellbare Elemente	Hierbei handelt es sich um einen versteckten Ordner in der Nicht-IPM-Unterstruktur. Er enthält die Unterordner „Löschtätigkeiten“, „Versionen“, „Endgültige Löschtätigkeiten“, „In-Situ-Speicher“ und „Überwachungen“. Durch Aufbewahrungstags für diesen Ordner werden Elemente aus dem Ordner „Wiederherstellbare Elemente“ im primären Postfach des Benutzers in den Ordner „Wiederherstellbare Elemente“ im Archivpostfach des Benutzers verschoben. Sie können den Tags für diesen Ordner nur die Aufbewahrungsaktion <b>In Archiv verschieben</b> zuweisen. Weitere Informationen finden Sie unter <a href="#">Recoverable Items Folder</a> .
Gesendete Elemente	In diesem Standardordner werden Nachrichten gespeichert, die an einen Hub-Transport-Server übermittelt wurden.
Synchronisierungsprobleme	Dieser Ordner enthält Synchronisierungsprotokolle. Weitere Informationen finden Sie unter <a href="#">Ordner für Synchronisierungsprobleme</a> .
Tasks	In diesem Standardordner Aufgaben zu speichern. Um ein Aufbewahrungsrichtlinientag für den Ordner Aufgaben zu erstellen, müssen Sie Exchange Online PowerShell verwenden. Weitere Informationen finden Sie unter <a href="#">New-RetentionPolicyTag</a> . Nachdem das Aufbewahrungsrichtlinientag für den Ordner Aufgaben erstellt wurde, können Sie es mithilfe der Exchange-Verwaltungskonsole verwalten.

## Weitere Informationen

- RPTs sind Aufbewahrungstags für Standardordner. Sie können für RPTs nur eine Löschaktion auswählen - either **Löschen und Wiederherstellung zulassen** oder **Permanent löschen**.
- Sie können kein RPT erstellen, um Nachrichten in das Archiv zu verschieben. Um alte Elemente in das Archiv zu verschieben, können Sie ein Standardrichtlinientag (Default Policy Tag, DPT) erstellen, das für das gesamte Postfach gilt, oder Persönliche Tags erstellen, die in Outlook und Outlook Web App (OWA) als Archivrichtlinien angezeigt werden. Die Benutzer können sie auf Ordner oder einzelne Nachrichten anwenden.
- Sie können Aufbewahrungsrichtlinientags nicht auf den Ordner "Kontakte" anwenden.
- Sie können nur ein RPT für einen bestimmten Standardordner zu einer Aufbewahrungsrichtlinie hinzufügen. Wenn eine Aufbewahrungsrichtlinie beispielsweise über ein Tag für den Posteingang verfügt, können Sie ihr kein weiteres Aufbewahrungsrichtlinientag vom Typ "Posteingang" hinzufügen.
- Informationen dazu, wie Sie RPTs oder andere Arten von Aufbewahrungstags erstellen und sie zu einer Aufbewahrungsrichtlinie hinzufügen, finden Sie unter [Erstellen einer Aufbewahrungsrichtlinie](#).
- In Exchange gilt Server und Exchange Online, um ein Standardrichtlinientag auch für den **Kalender** und Standardordner **Aufgaben**. Dies kann dazu führen, dass Elemente gelöscht oder in das Archiv, basierend auf der DPT Einstellungen verschoben wird. Um die Einstellungen DPT aus Löschen von Elementen in diese Ordner zu verhindern, erstellen Sie Aufbewahrungsrichtlinientags mit Retention deaktiviert. Um die Einstellungen DPT aus Verschieben von Elementen in einem Standardordner zu verhindern, können Sie

eine deaktivierte persönliches Tag erstellen, mit dem Verschieben Aktion archivieren, die Aufbewahrungsrichtlinie hinzufügen, und klicken Sie dann Benutzer auf den Standardordner angewendet haben. Weitere Informationen hierzu finden Sie unter [Archivierung von Elementen in einem Standardordner in Exchange 2010 zu verhindern](#).

# Berechnung von Aufbewahrungszeiträumen

18.12.2018 • 9 minutes to read

Der Assistent für verwaltete Ordner ist einer von zahlreichen Prozessen vom Typ Postfach-Assistent, der auf Postfachservern ausgeführt wird. Seine Aufgabe besteht darin, Postfächer mit einer Aufbewahrungsrichtlinie zu verarbeiten, in der Richtlinie enthaltene Aufbewahrungstags auf das Postfach anzuwenden und die Elemente im Postfach zu verarbeiten. Wenn die Elemente ein Aufbewahrungstag aufweisen, prüft der Assistent das Alter dieser Elemente. Wenn das Aufbewahrungslimit eines Elements überschritten wurde, wird die entsprechende Aufbewahrungsaktion gestartet. Zu den Aufbewahrungsaktionen zählt das Verschieben von Elementen in das Archiv eines Benutzers, das Löschen von Elementen und Zulassen der Wiederherstellung oder das dauerhafte Löschen von Elementen.

Weitere Informationen finden Sie unter [Aufbewahrungstags und Aufbewahrungsrichtlinien](#).

## Ermitteln des Alters von unterschiedlichen Elementtypen

Das Aufbewahrungslimit für Postfachelemente wird ab dem Datum der Zustellung oder dem Datum der Erstellung für Elemente berechnet, wie beispielsweise Entwürfe, die vom Benutzer erstellt, aber nicht zugestellt wurden. Wenn der Assistent für verwaltete Ordner Elemente in einem Postfach verarbeitet, werden alle Elemente, die Aufbewahrungstags mit der Aufbewahrungsaktion **Löschen und Wiederherstellung zulassen** oder **Endgültig löschen** aufweisen, mit einem Start- und einem Ablaufdatum gestempelt. Elemente, die ein Archivierungstag aufweisen, werden ebenfalls mit einem Verschiebungsdatum gestempelt.

Elemente im Ordner "Gelöschte Elemente" und Elemente mit einem Start- und Enddatum, wie beispielsweise Kalenderelemente (Besprechungen und Termine) und Aufgaben, werden anders behandelt (siehe Angaben in dieser Tabelle).

WENN SIE DER ELEMENTTYP IST...	UND DAS ELEMENT IST...	DER AUFBEWAHRUNGSZEITRAUM IST AUF DER GRUNDLAGE BERECHNET....
E-Mail Dokument Fax- Journalelement Besprechungsanfrage, -antwort oder -absage Verpasster Anruf	Nicht im Ordner "Gelöschte Elemente"	Zustellungsdatum oder Erstellungsdatum

WENN SIE DER ELEMENT TYP IST...	UND DAS ELEMENT IST...	DER AUFBEWAHRUNGSZEITRAUM IST AUF DER GRUNDLAGE BERECHNET....
E-Mail Dokument Fax- Journalelement Besprechungsanfrage, -antwort oder -absage Verpasster Anruf	Im Ordner "Gelöschte Elemente"	Zustellungs- oder Erstellungsdatum, es sei denn, das Element wurde aus einem Ordner gelöscht, der weder ein geerbtes noch ein implizites Aufbewahrungstag aufweist. Wenn sich ein Element in einem Ordner befindet, auf den ein geerbtes oder ein implizites Aufbewahrungstag angewendet wird, wird das Element vom Assistenten für verwaltete Ordner nicht verarbeitet und verfügt daher nicht über ein vom Assistenten gestempeltes Startdatum. Wenn der Benutzer ein solches Element löscht und der Assistent für verwaltete Ordner das Element zum ersten Mal im Ordner "Gelöschte Elemente" verarbeitet, kennzeichnet er das aktuelle Datum als Startdatum.
Kalender	Nicht im Ordner "Gelöschte Elemente"	Nicht-Kalenderserienelemente laufen entsprechend ihrem Enddatum ab. Kalenderserienelemente laufen entsprechend dem Enddatum ihres letzten Auftretens ab. Kalenderserienelemente ohne Enddatum laufen niemals ab.
Kalender	Im Ordner "Gelöschte Elemente"	
Ein Kalenderelement läuft entsprechend dem Wert des Parameters message-received date ab, sofern vorhanden. Wenn der Parameter message-received date für ein Kalenderelement nicht angegeben wurde, läuft es entsprechend dem Wert des Parameters message-creation date ab. Wenn für ein Kalenderelement weder der Parameter message-received date noch der Parameter message-creation date festgelegt wurde, läuft es nie ab.		

WENN SIE DER ELEMENT TYP IST...	UND DAS ELEMENT IST...	DER AUFBEWAHRUNGSZEITRAUM IST AUF DER GRUNDLAGE BERECHNET....
Task	Nicht im Ordner "Gelöschte Elemente"	<p>Nicht wiederkehrende Aufgaben: Eine nicht wiederkehrende Aufgabe läuft ab nach seiner <code>message-received date</code>, sofern vorhanden.</p> <p>Wenn eine nicht wiederkehrende Aufgabe besitzt eine <code>message-received date</code>, sie läuft, entsprechend seine <code>message-creation date</code>.</p> <p>Wenn eine nicht wiederkehrende Aufgabe weder wurde eine <code>message-received date</code> noch eine <code>message-creation date</code>, es läuft nicht ab.</p> <p>Eine wiederkehrende Aufgabe läuft ab nach der <code>end date</code> letzten auftreten.</p> <p>Wenn auf ein sich wiederholenden Vorgang ist ein <code>end date</code>, es läuft nicht ab.</p> <p>Eine Aufgabe, die erneut generiert wird (d. h. eine Aufgabenserie, die zu einem bestimmten Zeitpunkt nach Abschluss der vorherigen Instanz der Aufgabenserie erneut generiert wird), läuft nie ab.</p>
Task	Im Ordner "Gelöschte Elemente"	
Eine Aufgabe läuft entsprechend dem Wert des Parameters <code>message-received date</code> ab, sofern vorhanden. Wenn der Parameter <code>message-received date</code> für eine Aufgabe nicht angegeben wurde, läuft sie entsprechend dem Wert des Parameters <code>message-creation date</code> ab. Wenn für eine Aufgabe weder der Parameter <code>message-received date</code> noch der Parameter <code>message-creation date</code> festgelegt wurde, läuft sie nie ab.		
Kontakt	In allen Ordnern	Kontakte werden nicht mit einem Start- oder Ablaufdatum gestempelt. Sie werden vom Assistenten für verwaltete Ordner übersprungen und laufen nicht ab.
Beschädigt	In allen Ordnern	Beschädigte Elemente werden vom Assistenten für verwaltete Ordner übersprungen und laufen nicht ab.

## Beispiele

WENN DER BENUTZER...	DIE AUFBEWAHRUNGSTAGS FÜR ORDNER...	DER ASSISTENT FÜR VERWALTETE ORDNER...
Empfängt eine Nachricht im Posteingang am 01/26/2013. Löscht die Nachricht am 2/27/2013.	Posteingang: Löschen in 365 Tagen Gelöschte Elemente: Löschen in 30 Tagen	Verarbeitet die Nachricht im Posteingang am 1/26/2013, stempelt sie mit dem Startdatum 01/26/2013 und einem Ablaufdatum 01/26/2014. Verarbeitet die Nachricht erneut im Ordner "Gelöschte Elemente" auf 2/27/2013. Diese neu berechnet das Ablaufdatum basierend auf den gleichen Datum (26/01/2013). Da das Element älter als 30 Tage ist, wird es sofort abgelaufen.
Empfängt eine Nachricht im Posteingang am 01/26/2013. Löscht die Nachricht am 2/27/2013.	Posteingang: Keine (geerbt oder implizit) Gelöschte Elemente: Löschen in 30 Tagen	Verarbeitet die Nachricht im Ordner "Gelöschte Elemente" auf 02/27/2013 und bestimmt, dass das Element kein Startdatum ist. Es versieht das aktuelle Datum als das Startdatum und 03/27/2013 als das Ablaufdatum. Das Element ist abgelaufen auf 3/27/2013 30 Tage nach dem der Benutzer gelöscht oder in den Ordner Gelöschte Objekte verschoben.

## Weitere Informationen

- In Exchange Online verarbeitet Assistenten für verwaltete Ordner ein Postfach einmal in sieben Tagen. Dadurch kann Elemente abgelaufenen bis zu sieben Tage nach das Ablaufdatum für das Element versehen.
- Elemente, für die das Anhalten der Aufbewahrungszeit aktiviert ist, werden erst vom Assistenten für verwaltete Postfächer verarbeitet, wenn das Anhalten der Aufbewahrungszeit aufgehoben wurde.
- Wenn für ein Postfach das Compliance-Archiv oder das Beweissicherungsverfahren aktiviert ist, werden ablaufende Elemente aus dem Posteingang entfernt, aber so lange im Ordner "Wiederherstellbare Elemente" aufbewahrt, bis das Postfach aus dem [In-Situ-Speicher und Beweissicherungsverfahren](#) entfernt wurde.
- In hybridbereitstellungen müssen die gleichen aufbewahrungtags und Aufbewahrungsrichtlinien in Ihrer lokalen und Exchange Online-Organisationen, um ständig verschieben und Elemente für beide Organisationen ablaufen vorhanden. Weitere Informationen finden Sie unter [Export und Import Retention Tags](#).

# Erstellen einer Aufbewahrungsrichtlinie

18.12.2018 • 12 minutes to read

Aufbewahrungsrichtlinien können Sie in Exchange Online e-Mail-Lebenszyklus verwalten.

Aufbewahrungsrichtlinien werden einer Aufbewahrungsrichtlinie hinzugefügt, Erstellen von aufbewahrungstags und Anwenden der Richtlinie auf Postfachbenutzer angewendet.

Nachfolgend finden Sie ein [video](#), das Sie zeigt, wie Sie eine Aufbewahrungsrichtlinie zu erstellen und Zuweisen eines Postfachs in Exchange Online.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Aufbewahrungsrichtlinien finden Sie unter [Messaging Records Management Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen dieser Aufgabe: 30 Minuten.
- Für die Verfahren in diesem Thema sind bestimmte Berechtigungen erforderlich. Informationen zu den Berechtigungen finden Sie in den einzelnen Verfahren.
- Postfächer, auf die Aufbewahrungsrichtlinien angewendet werden, müssen auf Exchange Server 2010 oder höher-Servern befinden.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## Schritt 1: Erstellen eines Aufbewahrungstags

Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Messaging-Datensatzverwaltung" im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#).

### Erstellen eines Aufbewahrungstags mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie zu **Verwaltung der Richtlinientreue > aufbewahrungstags**, und klicken Sie dann auf **Hinzufügen**

2. Wählen Sie eine der folgenden Optionen aus:

- **Automatisch für das gesamte Postfach (Standard)**: Wählen Sie diese Option, um eine Richtlinie Standardtag (DPT) zu erstellen. DPTs können Sie erstellen eine Standardrichtlinie löschen und eine Standardrichtlinie für die Archivierung, die auf alle Elemente im Postfach angewendet wird.

#### NOTE

Sie können nicht der Exchange-Verwaltungskonsole verwenden, um ein Standardrichtlinientag zum Löschen von voicemailelementen erstellen. Ausführliche Informationen zum Erstellen einer DPT zum Löschen von voicemailelementen finden Sie unter Exchange Online PowerShell Beispiel unten.

- **Wird automatisch in einen bestimmten Ordner angewendet**: Wählen Sie diese Option zum Erstellen einer Aufbewahrungsrichtlinien-Tag (außer) für einen Standardordner wie **Posteingang** oder **Gelöschte Elemente**.

#### NOTE

Aufbewahrungsrichtlinientags können nur mit der Aktion **Löschen und Wiederherstellung zulassen** oder **Endgültig löschen** erstellt werden.

- **Applied von Benutzern auf Elemente und Ordner (persönlich):** Wählen Sie diese Option, um persönliche Tags erstellen. Diese Tags können Outlook und Outlook Web App Benutzer gelten archivieren oder Löschen von Einstellungen für eine Nachricht oder Ordner, die sich von den Einstellungen auf dem übergeordneten Ordner oder das gesamte Postfach angewendet werden.

3. Titel und Optionen auf der Seite **Neues Aufbewahrungstag** sind je nach gewähltem Tagtyp unterschiedlich. Füllen Sie folgende Felder aus:

- **Name:** Geben Sie einen Namen für die aufbewahrungstag. Der Name des Tags ist für die Anzeige und keinen Einfluss auf den Ordner oder das Element, das auf ein Tag angewendet wird. Beachten Sie, dass die persönliche Tags, denen, die Sie für Benutzer bereitstellen, in Outlook und Outlook Web App verfügbar sind.
- **Übernehmen dieses Tag in den folgenden Standardordner:** Diese Option ist nur verfügbar, wenn Sie **wird automatisch in einen bestimmten Ordner angewendet ausgewählt**.
- **Aufbewahrungsaktion:** Wählen Sie eine der folgenden Aktionen ausgeführt werden soll, nachdem das Element der Aufbewahrungszeitraum erreicht:
- **Löschen und Wiederherstellung zulassen:** Wählen Sie diese Aktion für Elemente löschen, aber ermöglichen wiederherstellbar mit der Option **Gelöschte Elemente wiederherstellen** in Outlook oder Outlook Web App-Elemente werden beibehalten, bis die Aufbewahrungszeit für konfiguriert die Postfachdatenbank oder den Postfachbenutzer erreicht ist.
- **Endgültig löschen:** Wählen Sie diese Option, um das Element aus der Postfachdatenbank endgültig löschen.

#### IMPORTANT

Postfächer oder Elemente, die der Compliance-Archivierung bzw. dem Beweissicherungsverfahren unterliegen, werden aufbewahrt und bei Compliance-eDiscovery-Suchvorgängen zurückgegeben. Weitere Informationen finden Sie unter [In-Situ-Speicher und Beweissicherungsverfahren](#).

- **In Archiv verschieben:** Diese Aktion ist nur verfügbar, wenn Sie ein Standardrichtlinientag oder ein persönliches Tag erstellen. Wählen Sie diese Aktion zum Verschieben von Elementen in des Benutzers Compliance-Archiv.
- **Beibehaltungszeitraum:** Wählen Sie eine der folgenden Optionen aus:
- **Never:** Wählen Sie diese Option, um anzugeben, dass Elemente nie gelöscht oder in das Archiv verschoben.
- **Wenn das Element das folgende Alter (in Tagen) erreicht:** Wählen Sie diese Option aus, und geben Sie die Anzahl der Tage, die Elemente beibehalten werden, bevor sie verschoben oder gelöscht werden. Ein Element empfangen oder erstellt wird, wird der Aufbewahrungszeitraum für alle unterstützten Elemente außer Kalender und Aufgaben nach dem Datum berechnet. Aufbewahrungszeitraum für Kalender und Aufgaben Elemente wird vom Enddatum berechnet.
- **Kommentar:** Benutzer dieses Feld optional alle administrativen Hinweise oder Kommentare eingeben. Das Feld ist nicht für Benutzer angezeigt.

## **Verwenden Sie Exchange Online PowerShell, um ein Aufbewahrungstag zu erstellen.**

Verwenden Sie das Cmdlet **New-RetentionPolicyTag**, um ein Aufbewahrungstag zu erstellen. Verschiedene im Cmdlet verfügbaren Optionen können Sie verschiedene Typen von Aufbewahrungstags zu erstellen. Den *Type*-Parameter verwenden, um ein Standardrichtlinientag zu erstellen ( `All` ), außer (Geben Sie einen Ordner Standardtyp wie `Inbox` ) oder ein persönliches Tag ( `Personal` ).

Dieser Befehl erstellt ein Standardrichtlinientag zum Löschen aller Nachrichten im Postfach nach 7 Jahren (2556 Tagen).

```
New-RetentionPolicyTag -Name "DPT-Corp-Delete" -Type All -AgeLimitForRetention 2556 -RetentionAction DeleteAndAllowRecovery
```

Dieser Befehl erstellt ein Standardrichtlinientag zum Verschieben aller Nachrichten in das Compliance-Archiv in 2 Jahren (730 Tagen).

```
New-RetentionPolicyTag -Name "DPT-Corp-Move" -Type All -AgeLimitForRetention 730 -RetentionAction MoveToArchive
```

Dieser Befehl erstellt ein Standardrichtlinientag zum Löschen von Voicemailnachrichten nach 20 Tagen.

```
New-RetentionPolicyTag -Name "DPT-Corp-Voicemail" -Type All -MessageClass Voicemail -AgeLimitForRetention 20 -RetentionAction DeleteAndAllowRecovery
```

Dieser Befehl erstellt ein Aufbewahrungsrichtlinientag zum endgültigen Löschen der Nachrichten im Junk-E-Mail-Ordner nach 30 Tagen.

```
New-RetentionPolicyTag -Name "RPT-Corp-JunkMail" -Type JunkEmail -AgeLimitForRetention 30 -RetentionAction PermanentlyDelete
```

Dieser Befehl erstellt ein persönliches Tag, bei dessen Anwendung Nachrichten nie gelöscht werden.

```
New-RetentionPolicyTag -Name "Never Delete" -Type Personal -RetentionAction DeleteAndAllowRecovery -RetentionEnabled $false
```

## **Schritt 2: Erstellen Sie eine Aufbewahrungsrichtlinie**

Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Messaging-Datensatzverwaltung" im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#).

### **Erstellen einer Aufbewahrungsrichtlinie mithilfe der Exchange-Verwaltungskonsole**

1. Navigieren Sie zu **Verwaltung der Richtlinientreue > Aufbewahrungsrichtlinien**, und klicken Sie dann auf **Hinzufügen**

2. Füllen Sie unter **Neue Aufbewahrungsrichtlinie** die folgenden Felder aus:

- **Name:** Geben Sie einen Namen für die Aufbewahrungsrichtlinie.
- **Aufbewahrungstags:** Klicken Sie auf **Add**  die Tags wählen Sie diese Aufbewahrungsrichtlinie hinzufügen möchten.

Eine Aufbewahrungsrichtlinie kann die folgenden Tags enthalten:

- Ein Standardrichtlinientag mit der Aktion **in Archiv verschieben** .
- Ein Standardrichtlinientag mit der Aktionen **Löschen und Wiederherstellung zulassen** oder **Endgültig löschen** .
- Ein Standardrichtlinientag für Voicemailnachrichten mit den Aktionen **Löschen und Wiederherstellung zulassen** oder **Endgültig löschen** .
- Ein Aufbewahrungsrichtlinientag pro Standardordner wie **Posteingang** , Elemente zu löschen.
- Eine beliebige Anzahl von persönlichen Tags.

**NOTE**

Sie können einer Aufbewahrungsrichtlinie zwar beliebig viele persönliche Tags hinzufügen; viele persönliche Tags mit unterschiedlichen Aufbewahrungseinstellungen können Benutzer aber zusätzlich verwirren. Es wird empfohlen, mit einer Aufbewahrungsrichtlinie nicht mehr als 10 persönliche Tags zu verknüpfen.

Sie können eine Aufbewahrungsrichtlinie zu erstellen, ohne alle aufbewahrungstags hinzuzufügen, aber Elemente im Postfach auf den die Richtlinie angewendet wird wird nicht verschoben oder gelöscht werden. Sie können auch hinzufügen und entfernen aufbewahrungstags aus einer Aufbewahrungsrichtlinie, nachdem er erstellt wurde.

**Verwenden Sie Exchange Online PowerShell, um eine Aufbewahrungsrichtlinie zu erstellen.**

In diesem Beispiel wird die Aufbewahrungsrichtlinie "RetentionPolicy-corp" erstellt und den Parameter *RetentionPolicyTagLinks* zum Zuordnen von fünf Tags der Richtlinie verwendet.

```
New-RetentionPolicy "RetentionPolicy-Corp" -RetentionPolicyTagLinks "DPT-Corp-Delete", "DPT-Corp-Move", "DPT-Corp-Voicemail", "RPT-Corp-JunkMail", "Never Delete"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-RetentionPolicy](#).

## Schritt 3: Anwenden einer Aufbewahrungsrichtlinie auf Postfachbenutzer

Nachdem Sie eine Aufbewahrungsrichtlinie erstellt haben, wenden Sie sie auf Postfachbenutzer an. Sie können auf mehrere Benutzer unterschiedliche Aufbewahrungsrichtlinien anwenden. Ausführliche Anweisungen finden Sie unter [Anwenden einer Aufbewahrungsrichtlinie auf Postfächer](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Nachdem Sie Aufbewahrungstags erstellt, diese einer Aufbewahrungsrichtlinie hinzugefügt und die Richtlinie auf einen Postfachbenutzer angewendet haben, werden Nachrichten bei der nächsten Verarbeitung des Postfachs basierend auf den in den Aufbewahrungstags konfigurierten Einstellungen verschoben oder gelöscht.

Gehen Sie wie folgt vor, um sich zu vergewissern, dass die Aufbewahrungsrichtlinie angewendet wurde:

1. Ersetzen Sie <Postfachidentität> mit dem Namen und e-Mail-Adresse oder den Alias des Postfachs, und führen Sie den folgenden Befehl in Exchange Online PowerShell-Befehl des MRM-Assistenten manuell für ein einzelnes Postfach ausführen:

```
Start-ManagedFolderAssistant -Identity "<Mailbox Identity>"
```

2. Melden Sie sich an das Postfach mithilfe von Outlook oder Outlook im Web (vormals Outlook Web App), und

stellen Sie sicher, dass Nachrichten in einem Archiv gemäß der Richtlinienkonfiguration verschoben oder gelöscht werden.

**TIP**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Hinzufügen von Aufbewahrungstags zu oder Entfernen von Aufbewahrungstags aus einer Aufbewahrungsrichtlinie

18.12.2018 • 4 minutes to read

Sie können Aufbewahrungstags zu einer Aufbewahrungsrichtlinie hinzufügen, wenn die Richtlinie erstellt wird, oder zu einem beliebigen späteren Zeitpunkt. Genaue Anweisungen zum Erstellen einer Aufbewahrungsrichtlinie, einschließlich des gleichzeitigen Hinzufügens von Aufbewahrungstags, finden Sie unter [Erstellen einer Aufbewahrungsrichtlinie](#).

Eine Aufbewahrungsrichtlinie kann die folgenden Aufbewahrungstags enthalten:

- Ein oder mehrere Aufbewahrungsrichtlinientags (Retention Policy Tag, RPT) für unterstützte Standardordner
- Ein Standardrichtlinientag (Default Policy Tag, DPT) mit der Aktion **In Archiv verschieben**
- Ein Standardrichtlinientag mit der Aktion **Löschen und Wiederherstellung zulassen** oder mit der Aktion **Endgültig löschen**
- Ein Standardrichtlinientag für Voicemail
- Eine beliebige Anzahl von persönlichen Tags

Weitere Informationen zu Aufbewahrungstags finden Sie unter [Aufbewahrungstags und Aufbewahrungsrichtlinien](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 10 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Messaging Records Management" im Thema [Mailbox Permissions](#).
- Aufbewahrungstags werden nicht an ein Postfach angewendet, bis sie mit einer Aufbewahrungsrichtlinie verknüpft sind und den Assistenten für verwaltete Ordner das Postfach verarbeitet. Um den Assistenten für verwaltete Ordner zu starten, damit sie ein Postfach verarbeitet, finden Sie unter [Configure und der Assistent für verwaltete Ordner in Exchange 2016 ausführen](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von EAC zum Hinzufügen oder Entfernen von Aufbewahrungstags

1. Navigieren Sie zu **Verwaltung der Richtlinientreue > Aufbewahrungsrichtlinien**.
2. Wählen Sie in der Listenansicht die Aufbewahrungsrichtlinie auf die Sie hinzufügen möchten aufbewahrungstags und klicken Sie dann auf **Bearbeiten**.
3. Verwenden Sie im Abschnitt **Aufbewahrungsrichtlinie** die folgenden Einstellungen:
  - **Fügen Sie hinzu** klicken Sie auf diese Schaltfläche, um ein aufbewahrungstag der Richtlinie hinzuzufügen.
  - **Entfernen** wählen Sie ein Tag aus der Liste aus, und klicken Sie dann auf diese Schaltfläche, um das Tag aus der Richtlinie zu entfernen.

## Verwenden von Exchange Online PowerShell hinzufügen oder Entfernen von aufbewahrungstags

In diesem Beispiel werden die Aufbewahrungstags "VPs-Default", "VPs-Inbox" und "VPs-DeletedItems" der Aufbewahrungsrichtlinie "RetPolicy-VPs" hinzugefügt, mit der noch keine Aufbewahrungstags verknüpft sind.

**Caution**

Wenn mit der Richtlinie bereits Aufbewahrungstags verknüpft sind, werden die vorhandenen Tags durch diesen Befehl ersetzt.

```
Set-RetentionPolicy -Identity "RetPolicy-VPs" -RetentionPolicyTagLinks "VPs-Default", "VPs-Inbox", "VPs-DeletedItems"
```

In diesem Beispiel wird das Aufbewahrungstag "VPs-DeletedItems" mit der Aufbewahrungsrichtlinie "RetPolicy-VPs" verknüpft, mit der bereits andere Aufbewahrungstags verknüpft sind.

```
$TagList = (Get-RetentionPolicy "RetPolicy-VPs").RetentionPolicyTagLinks
$TagList.Add((Get-RetentionPolicyTag 'VPs-DeletedItems').DistinguishedName)
Set-RetentionPolicy "RetPolicy-VPs" -RetentionPolicyTagLinks $TagList
```

In diesem Beispiel wird das Aufbewahrungstag "VPs-Inbox" aus der Aufbewahrungsrichtlinie "RetPolicy-VPs" entfernt.

```
$TagList = (Get-RetentionPolicy "RetPolicy-VPs").RetentionPolicyTagLinks
$TagList.Remove((Get-RetentionPolicyTag 'VPs-Inbox').DistinguishedName)
Set-RetentionPolicy "RetPolicy-VPs" -RetentionPolicyTagLinks $TagList
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [set-RetentionPolicy](#) und [get-RetentionPolicy](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Verwenden Sie das Cmdlet [Get-RetentionPolicy](#) um zu überprüfen, dass Sie erfolgreich hinzugefügt oder ein aufbewahrungstag aus einer Aufbewahrungsrichtlinie entfernt, so überprüfen Sie die *RetentionPolicyTagLinks* - Eigenschaft.

In diesem Beispiel wird das Cmdlet **Get-RetentionPolicy** dazu verwendet, Aufbewahrungstags abzurufen, die der Richtlinie "Default MRM" hinzugefügt wurden. Die Ausgabe wird dann mittels Pipe an das Cmdlet **Format-Table** umgeleitet, um nur die Namenseigenschaft für jedes Tag auszugeben.

```
(Get-RetentionPolicy "Default MRM Policy").RetentionPolicyTagLinks | Format-Table name
```

# Anwenden einer Aufbewahrungsrichtlinie auf Postfächer

18.12.2018 • 4 minutes to read

Aufbewahrungsrichtlinien ermöglichen Ihnen das Gruppieren eines oder mehrerer Aufbewahrungstags, um diese zur Durchsetzung von Nachrichtenaufbewahrungseinstellungen auf Postfächer anzuwenden. Ein Postfach kann nur eine Aufbewahrungsrichtlinie aufweisen.

## Caution

Nachrichten laufen auf der Grundlage von Einstellungen ab, die in den mit der Richtlinie verknüpften Aufbewahrungstags definiert sind. Zu diesen Einstellungen gehören Aktionen wie das Verschieben von Nachrichten in das Archiv oder das endgültige Löschen. Vor dem Anwenden einer Aufbewahrungsrichtlinie auf ein oder mehrere Postfächer sollten Sie die Richtlinie testen und die zugeordneten Aufbewahrungstags prüfen.

Weitere Verwaltungsaufgaben im Zusammenhang mit der Messaging-Datensatzverwaltung (MRM) finden Sie unter [Verfahren der Messaging-Datensatzverwaltung](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Anwenden von Aufbewahrungsrichtlinien" im Thema [Messaging Policy and Compliance Permissions](#) .
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Anwenden einer Aufbewahrungsrichtlinie auf ein einzelnes Postfach mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie zu **Empfänger > Postfächer**.
2. In der Listenansicht, wählen Sie das Postfach, dem Sie die Aufbewahrungsrichtlinie anwenden möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie in **Benutzerpostfach** auf **Postfachfunktionen**.
4. Wählen Sie in der Liste **Aufbewahrungsrichtlinie** die Richtlinie aus, die auf das Postfach angewendet werden soll, und klicken Sie auf **Speichern**.

## Anwenden einer Aufbewahrungsrichtlinie auf mehrere Postfächer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie zu **Empfänger > Postfächer**.

2. Verwenden Sie in der Listenansicht die UMSCHALT- oder die STRG-TASTE, um mehrere Postfächer auszuwählen.
3. Klicken Sie im Detailbereich auf **Weitere Optionen**.
4. Klicken Sie unter **Aufbewahrungsrichtlinie** auf **Aktualisieren**.
5. Wählen Sie in der Liste **Massenzuweisung von Aufbewahrungsrichtlinie** die Aufbewahrungsrichtlinie aus, die auf die Postfächer angewendet werden soll, und klicken Sie auf **Speichern**.

## Anwenden einer Aufbewahrungsrichtlinie auf ein einzelnes Postfach mithilfe von Exchange Online PowerShell

In diesem Beispiel wird die Aufbewahrungsrichtlinie "RP-Finance" auf das Postfach von Morris angewendet.

```
Set-Mailbox "Morris" -RetentionPolicy "RP-Finance"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailbox](#).

## Anwenden einer Aufbewahrungsrichtlinie auf mehrere Postfächer mithilfe von Exchange Online PowerShell

In diesem Beispiel wird die neue Aufbewahrungsrichtlinie "New-Retention-Policy" auf alle Postfächer angewendet, die über die alte Richtlinie "Old-Retention-Policy" verfügen.

```
$OldPolicy=(Get-RetentionPolicy "Old-Retention-Policy").distinguishedName  
Get-Mailbox -Filter {RetentionPolicy -eq $OldPolicy} -Resultsize Unlimited | Set-Mailbox -RetentionPolicy  
"New-Retention-Policy"
```

In diesem Beispiel wird die Aufbewahrungsrichtlinie "RetentionPolicy-Corp" auf alle Postfächer in der Exchange-Organisation angewendet.

```
Get-Mailbox -ResultSize unlimited | Set-Mailbox -RetentionPolicy "RetentionPolicy-Corp"
```

In diesem Beispiel wird die Aufbewahrungsrichtlinie "RetentionPolicy-Finance" auf alle Postfächer in der Organisationseinheit für Finanzen angewendet.

```
Get-Mailbox -OrganizationalUnit "Finance" -ResultSize Unlimited | Set-Mailbox -RetentionPolicy  
"RetentionPolicy-Finance"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-Mailbox](#) und [Set-Mailbox](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum Überprüfen, ob die Aufbewahrungsrichtlinie angewendet wurde, führen Sie das Cmdlet [Get-Mailbox](#) aus, um die Aufbewahrungsrichtlinie für das Postfach bzw. die Postfächer abzurufen.

In diesem Beispiel wird die Aufbewahrungsrichtlinie für das Postfach von Morris abgerufen.

```
Get-Mailbox Morris | Select RetentionPolicy
```

Dieser Befehl ruft alle Postfächer ab, auf die die Aufbewahrungsrichtlinie "RP-Finance" angewendet wird.

```
Get-Mailbox -ResultSize unlimited | Where-Object {$_.RetentionPolicy -eq "RP-Finance"} | Format-Table  
Name,RetentionPolicy -Auto
```

# Anhalten der Aufbewahrungszeit für ein Postfach

18.12.2018 • 4 minutes to read

Wenn Sie für ein Postfach die Aufbewahrungszeit anhalten, wird die Verarbeitung einer Aufbewahrungsrichtlinie oder einer Postfachrichtlinie für verwalteten Ordner für dieses Postfach angehalten. Das Anhalten der Aufbewahrungszeit ist für Situationen gedacht, bei denen ein Benutzer z. B. im Urlaub oder vorübergehend abwesend ist.

Während die Aufbewahrungszeit angehalten wird, können sich die Benutzer an ihrem Postfach anmelden und Elemente ändern oder löschen. Wenn Sie eine Postfachsuche ausführen, werden gelöschte Elemente, die die Beibehaltungsdauer für gelöschte Element überschritten haben, in Suchergebnissen nicht zurückgegeben. Wenn Sie sicherstellen möchten, dass von Benutzern geänderte oder gelöschte Elemente in Szenarien mit rechtlichen Aufbewahrungspflichten erhalten bleiben, müssen Sie für das Postfach die rechtliche Aufbewahrungspflicht festlegen. Weitere Informationen finden Sie unter [Erstellen oder Entfernen eines Compliance-Archivs](#).

Sie können auch Kommentare zur Aufbewahrung für Postfächer hinzufügen, für die Sie das Anhalten der Aufbewahrungszeit festgelegt haben. Die Kommentare werden in unterstützten Versionen von Microsoft Outlook angezeigt.

Weitere Verwaltungsaufgaben im Zusammenhang mit der Messaging-Datensatzverwaltung (MRM) finden Sie unter [Verfahren der Messaging-Datensatzverwaltung](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Messaging Records Management" im Thema [Messaging Policy and Compliance Permissions](#) .
- Sie können den Exchange-Verwaltungskonsole (EAC) an ein Postfach zur Aufbewahrung von halten nicht verwenden. Sie müssen Exchange Online PowerShell verwenden.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell, platzieren ein Postfachs zur Aufbewahrung von halten

In diesem Beispiel wird die Aufbewahrungszeit für das Postfach von Michael Allen angehalten.

```
Set-Mailbox "Michael Allen" -RetentionHoldEnabled $true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailbox](#).

# Verwenden von Exchange Online PowerShell Anhalten der Aufbewahrungszeit für ein Postfach entfernen

In diesem Beispiel wird das Anhalten der Aufbewahrungszeit für das Postfach von Michael Allen aufgehoben.

```
Set-Mailbox "Michael Allen" -RetentionHoldEnabled $false
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailbox](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie ein Postfach erfolgreich auf Anhalten der Aufbewahrungszeit gesetzt haben, verwenden Sie das Cmdlet [Get-Mailbox](#), die *RetentionHoldEnabled* -Eigenschaft des Postfachs abzurufen.

Dieser Befehl ruft die *RetentionHoldEnabled* -Eigenschaft für das Postfach von Michael Allen ab.

```
Get-Mailbox "Michael Allen" | Select RetentionHoldEnabled
```

Dieser Befehl ruft alle Postfächer in der Exchange-Organisation ab, filtert nach den Postfächern, deren Aufbewahrungszeit angehalten wurde, und führt sie zusammen mit der Aufbewahrungsrichtlinie auf, die auf jedes Postfach angewendet wird.

### IMPORTANT

Da *RetentionHoldEnabled* eine filterbare Eigenschaft in der Exchange-Server nicht, können nicht Sie den Parameter "Filter" mit dem Cmdlet [Get-Mailbox](#) auf Filter Postfächer verwenden, die auf der Serverseite Anhalten der Aufbewahrungszeit platziert werden. Mit diesem Befehl wird eine Liste aller Postfächer und Filter auf dem Client unter Exchange Online PowerShell-Sitzung abgerufen. In großen Umgebungen mit Tausenden von Postfächern kann dieser Befehl einen längeren Zeitraum für die Durchführung dauern.

```
Get-Mailbox -ResultSize unlimited | Where-Object {$_._RetentionHoldEnabled -eq $true} | Format-Table  
Name,RetentionPolicy,RetentionHoldEnabled -Auto
```

# Journale in Exchange Online

18.12.2018 • 17 minutes to read

Finden Sie Informationen zur Journalfunktion in Exchange Online. Erfahren Sie den Unterschied zwischen der Journalfunktion und dem Archivieren von Daten, wie Ihnen die Journalfunktion im Hinblick auf die Compliance hilft und vieles mehr.

Mithilfe der Aufzeichnung eingehender und ausgehender E-Mail-Kommunikation in Journalen kann Ihre Organisation rechtlichen, regulatorischen und organisatorischen Auflagen genügen. Bei der Planung von Nachrichtenaufbewahrung und Richtlinientreue ist es wichtig zu wissen, was Journale sind, wie sie in die Konformitätsrichtlinien Ihrer Organisation passen und wie Exchange Online Ihnen bei der Sicherung von Nachrichten hilft, die in einem Journal erfasst sind.

## Warum sind Journale wichtig?

Es ist wichtig, den Unterschied zwischen Journaling- und Datenarchivierungsstrategie zu verstehen:

- Journale bedeuten die Fähigkeit, alle Kommunikationsvorgänge in einer Organisation, einschließlich der E-Mail-Kommunikation, aufzuzeichnen, um sie im Rahmen der Aufbewahrungs- oder der Archivstrategie einer Organisation verwenden zu können. Um eine zunehmende Anzahl behördlicher Auflagen und Anforderungen zur Einhaltung von Vorschriften erfüllen zu können, müssen viele Organisationen die Kommunikationsdatensätze aufzubewahren, die beim Ausführen täglicher geschäftlicher Aufgaben durch Mitarbeiter erstellt werden.
- Datenarchivierung bezieht sich auf das Sichern der Daten. Sie werden aus ihrer nativen Umgebung entfernt und an anderer Stelle gespeichert, um die mit der Datenspeicherung einhergehende Last zu reduzieren. Sie können Exchange-Journaling als Tool für Ihre E-Mail-Aufbewahrungs- oder Archivstrategien verwenden.

Obwohl es keine spezielle Vorschriften gibt, die Journale zwingend erfordert, können bestimmte Bedingungen durch die Aufzeichnung in Journalen erfüllt werden. In einigen Finanzsektoren können Führungskräfte beispielsweise für die Forderungen ihrer Mitarbeiter an ihre Kunden haftbar gemacht werden. Ein Vorstandsmitglied kann sich daher entscheiden, ein System einzurichten, bei dem Manager einen Teil der Kommunikation von Mitarbeitern mit Kunden auf regelmäßiger Basis überprüfen. Jedes Quartal überprüfen die Manager die Einhaltung der Vorschriften und genehmigen das Verhalten ihrer Mitarbeiter. Nachdem alle Manager dem Vorstandsmitglied Bericht erstattet haben, meldet dieser der Aufsichtsbehörde die Einhaltung der Vorschriften seitens des Unternehmens. In diesem Beispiel können E-Mails eine Form der Kommunikation zwischen Mitarbeitern und Kunden sein, die Manager überprüfen müssen. Deshalb können Journale verwendet werden, um sämtliche E-Mails von Mitarbeitern mit Kundenkontakt zu erfassen. Zu den weiteren Verfahren der Kundenkommunikation können Faxe und Telefongespräche gehören, die ebenfalls den Bestimmungen unterliegen. Die Fähigkeit, alle Kategorien von Daten in einem Unternehmen in Journalen zu erfassen, ist eine wertvolle Funktion der IT-Architektur.

Die folgende Liste enthält einige der bekannteren US-amerikanischen und internationalen Bestimmungen, bei denen Journale Bestandteil der Strategien für die Einhaltung von Vorschriften sein können:

- Sarbanes-Oxley Act von 2002 (SOX)
- Security Exchange Commission Rule 17a-4 (SEC Rule 17 A-4)
- National Association of Securities Dealers 3010 & 3110 (NASD 3010 & 3110)
- Gramm-Leach-Bliley Act (Financial Modernization Act)

- Financial Institution Privacy Protection Act von 2001
- Financial Institution Privacy Protection Act von 2003
- Health Insurance Portability and Accountability Act von 1996 (HIPAA)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act von 2001 (Patriot Act)
- Datenschutzrichtlinie der EU (European Union Data Protection Directive, EUDPD)
- Personal Information Protection Act (Japan)

## Journalregeln

Folgende sind wichtige Aspekte von Journalregeln:

- **Journalregelbereich:** definiert, welche Nachrichten vom Journaling-Agent im Journal erfasst werden.
- **Journalempfänger:** Gibt die SMTP-Adresse des Empfängers zu einem Journal erfasst werden sollen.
- **Journalpostfach:** Gibt eine oder mehrere Postfächer zum Sammeln von Journalberichte verwendet.

### NOTE

In Office 365 können maximal 10 Journalregeln erstellt werden.

### Journalregelbereich

Mithilfe von Journalregeln können Sie nur interne, nur externe oder sowohl interne als auch externe Nachrichten in einem Journal erfassen. In der folgenden Liste sind diese Bereiche beschrieben:

- **Nur für interne Nachrichten:** Journalregeln mit dem Bereich festgelegt, interne Nachrichten, die zwischen der Empfänger in der Exchange-Organisation gesendet.
- **Nur externe Nachrichten:** Journalregeln mit dem Bereich externe Nachrichten an Empfänger gesendet oder Empfangen von Absendern außerhalb Ihrer Exchange-Organisation festgelegt.
- **Alle Nachrichten:** Journalregeln mit dem Bereich festgelegt, dass Journal alle Nachrichten, die durch Ihre Organisation unabhängig vom Ursprung oder Ziel übergeben. Dazu gehören Nachrichten, die bereits von Journalregeln in die interne und externe Bereiche verarbeitet wurden.

### Journalempfänger

Durch Angabe der SMTP-Adresse des Empfängers, der im Journal erfasst werden soll, können Sie zielgerichtete Journalregeln implementieren. Beim Empfänger kann es sich um ein Postfach, eine Verteilergruppe, einen E-Mail-Benutzer oder einen Kontakt in Exchange handeln. Diese Empfänger unterliegen möglicherweise besonderen rechtlichen Bestimmungen oder sind in juristische Verfahren involviert, bei denen E-Mails und andere Kommunikationsmittel als Beweismittel erfasst werden. Durch gezielte Auswahl bestimmter Empfänger oder Empfängergruppen können Sie auf einfache Weise eine Journalerfassungsumgebung konfigurieren, die den Prozessen Ihrer Organisation entspricht und rechtliche Bestimmungen und Vorschriften erfüllt. Indem Sie nur bestimmte Empfänger auswählen, deren Nachrichten in einem Journal erfasst werden müssen, können Sie auch den erforderlichen Speicherplatz sowie andere Kosten in Zusammenhang mit der Aufbewahrung großer Datenmengen reduzieren.

Alle Nachrichten, die von den in einer Journalregel angegebenen Empfängern gesendet oder empfangen werden, werden im Journal erfasst. Wenn Sie eine Verteilergruppe als Journalempfänger angeben, werden alle Nachrichten in einem Journal erfasst, die an die Mitglieder oder von den Mitgliedern der Verteilergruppe gesendet werden. Wenn Sie keinen Empfänger angeben, werden alle Nachrichten, die zwischen Empfängern und Absendern

ausgetauscht werden, die dem Journalbereich entsprechen, im Journal erfasst.

## Unified Messaging-aktivierte Journalempfänger

Viele Organisationen, die die Journalfunktion implementieren, verwenden möglicherweise auch Unified Messaging (UM), um ihre E-Mail-, Voicemail- und Faxinfrastruktur zu konsolidieren. Möglicherweise wünschen Sie jedoch nicht, dass der Journalvorgang Journalberichte für Nachrichten erzeugt, die von Unified Messaging generiert werden. In diesen Fällen können Sie entscheiden, ob Voicemailnachrichten und Benachrichtigungen über verpasste Anrufe, die von einem Exchange-Server mit dem Unified Messaging-Dienst verarbeitet werden, im Journal erfasst oder ausgelassen werden sollen. Wenn in Ihrer Organisation derartige Nachrichten nicht in einem Journal erfasst werden müssen, können Sie den Festplattenspeicherplatz, der zum Speichern von Journalberichten erforderlich ist, durch Ignorieren dieser Nachrichten verringern.

### NOTE

Nachrichten, die von einem Unified Messaging-Dienst generierte Faxnachrichten enthalten, werden immer in einem Journal erfasst, auch wenn Sie das Journaling von Unified Messaging-Voicemail und Benachrichtigungen über verpasste Anrufe deaktivieren.

Weitere Informationen zum Aktivieren bzw. Deaktivieren von Voicemailnachrichten und Benachrichtigungen über verpasste Anrufe finden Sie unter **Disable or Enable Journaling of Voice Mail and Missed Call Notifications**.

## Journalpostfach

Das Journalingpostfach dient zum Erfassen von Journalberichten. Wie das Journalingpostfach konfiguriert wird, hängt von den Richtlinien in Ihrer Organisation sowie den behördlichen und gesetzlichen Bestimmungen ab. Sie können ein Journalpostfach zum Erfassen der Nachrichten von allen in der Organisation konfigurierten Journalregeln angeben oder verschiedene Journalpostfächer für unterschiedliche Journalregeln oder Journalregelgruppen verwenden.

### IMPORTANT

In Office 365 können Sie ein Exchange Online-Postfach nicht als ein Journalpostfach festlegen. Sie können Journalberichte an ein lokales Archivierungssystem oder den Archivierungsdienst eines Drittanbieters senden. In einer Exchange-Hybridbereitstellung, in der sich Postfächer sowohl auf lokalen Servern als auch in Office 365 befinden, können Sie ein lokales Postfach als Journalpostfach für Ihre lokalen und Exchange Online-Postfächer festlegen.

Journalpostfächer enthalten sehr sensible Informationen. Journalpostfächer müssen geschützt werden, da in ihnen Nachrichten gesammelt werden, die von Empfängern und an Empfänger in Ihrer Organisation gesendet werden. Diese Nachrichten werden möglicherweise in juristischen Verfahren benötigt oder unterliegen gesetzlichen Bestimmungen. Verschiedene Gesetze schreiben vor, dass Nachrichten nicht verändert werden dürfen, bevor sie an eine Untersuchungsbehörde übergeben werden. Es wird empfohlen, dass Sie Richtlinien erstellen, die regeln, wer in der Organisation auf die Journalpostfächer zugreifen kann und dass Sie den Zugriff nur auf die Personen beschränken, die unmittelbaren Bedarf für den Zugriff haben. Beraten Sie sich mit den Rechtsberatern Ihrer Organisation, um sicherzustellen, dass Ihre Journallösung allen Gesetzen und Bestimmungen entspricht, denen die Organisation unterliegt.

## **IMPORTANT**

Wenn Sie eine Journalregel konfiguriert haben, durch die Journalberichte an ein Journalingpostfach gesendet werden, das ist nicht vorhanden ist oder ein ungültiges Ziel darstellt, bleibt der Journalbericht in der Transportwarteschlange auf Microsoft-Rechenzentrumsservern. Wenn dies der Fall ist, wenden sich Microsoft-Rechenzentrumsmitarbeiter an Ihre Organisation und bitten Sie, das Problem zu beheben, damit die Journalberichte an ein Journalingpostfach übermittelt werden können. Wenn Sie anschließend das Problem nicht innerhalb von zwei Tagen gelöst haben, wird die problematische Journalregel von Microsoft deaktiviert.

## **Alternatives Journalpostfach**

Wenn das Journalpostfach nicht verfügbar ist, möchten Sie eventuell nicht, dass unzustellbare Journalberichte in E-Mail-Warteschlangen auf Postfachservern gesammelt werden. Stattdessen können Sie ein alternatives Journalpostfach konfigurieren, in dem diese Journalberichte gespeichert werden. Das alternative Journalpostfach empfängt die Journalberichte als Anlage zu den Unzustellbarkeitsberichten, die generiert werden, wenn das Journalpostfach bzw. der Server, auf dem es sich befindet, die Zustellung des Journalberichts zurückweist oder nicht länger verfügbar ist.

Sobald das Journalingpostfach wieder verfügbar ist, können Sie die Funktion **Erneut senden** von OfficeOutlook verwenden, um die an das Journalingpostfach zu übermittelnden Journalberichte zu senden.

Wenn Sie ein alternatives Journalpostfach konfigurieren, werden alle Journalberichte, die innerhalb Ihrer gesamten Exchange-Organisation zurückgewiesen oder nicht zugestellt werden, an das alternative Journalpostfach übermittelt. Sie müssen deshalb sicherstellen, dass das alternative Journalpostfach und der Postfachserver, auf dem es sich befindet, zahlreiche Journalberichte unterstützen können.

### **Caution**

Wenn Sie ein alternatives Journalpostfach konfigurieren, müssen Sie das Postfach überwachen, um sicherzustellen, dass Postfach und Journalpostfächer nicht gleichzeitig nicht verfügbar sind. Wenn das alternative Journalpostfach nicht verfügbar ist oder gleichzeitig Journalberichte zurückweist, gehen die zurückgewiesenen Journalberichte verloren und können nicht abgerufen werden.

Da in dem alternativen Journalpostfach alle zurückgewiesenen Journalberichte der gesamten Exchange-Organisation gesammelt werden, müssen Sie sicherstellen, dass dadurch nicht gegen Gesetze oder Vorschriften verstößen wird, denen Ihre Organisation unterliegt. Falls Gesetze oder Vorschriften Ihrer Organisation untersagen, dass Journalberichte, die an verschiedene Journalpostfächer gesendet werden, im selben alternativen Journalpostfach gespeichert werden, können Sie ggf. kein alternatives Journalpostfach konfigurieren. Besprechen Sie sich mit Ihrer Rechtsabteilung, um festzustellen, ob Sie ein alternatives Journalpostfach verwenden dürfen.

Beim Konfigurieren des alternativen Journalpostfachs müssen dieselben Kriterien wie beim Konfigurieren des Journalpostfachs beachtet werden.

## **IMPORTANT**

Die alternativen Journalingpostfächer sollten als ein spezielles dediziertes Postfach behandelt werden. Alle Nachrichten, die direkt an das alternative Journalingpostfach gerichtet sind, werden nicht im Journal erfasst.

## **Journalberichte**

Ein Journalbericht ist die Mitteilung, die der Journal-Agent generiert, wenn eine Nachricht einer Journalregel entspricht und an das Journalpostfach übermittelt werden soll. Die Originalnachricht, die der Journalregel entspricht, wird unverändert als Anlage in den Journalbericht aufgenommen. Der Text eines Journalberichts enthält Informationen aus der ursprünglichen Nachricht wie die E-Mail-Adresse des Absenders, den Betreff der Nachricht, die Nachrichten-ID und die E-Mail-Adressen der Empfänger. Dies wird auch als Anlagejournaling bezeichnet und ist die einzige Journalingmethode, die von Office 365 unterstützt wird.

## **Journalberichte und IRM-geschützte Nachrichten**

Bei der Implementierung von Journaling müssen Sie Journalberichte und IRM-geschützte Nachrichten berücksichtigen. IRM-geschützte Nachrichten wirken sich auf die Such- und Discoveryfunktionen von Drittanbietersystemen für die Archivierung aus, die nicht über integrierte RMS-Unterstützung verfügen. In Office 365 können Sie die Journalberichtentschlüsselung konfigurieren, um eine unverschlüsselte Kopie einer Nachricht in einem Journalbericht zu speichern.

## **Problembehandlung**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#). Wenn Sie Probleme mit dem **JournalingReportDNRT0**-Postfach haben, finden Sie unter [Transport- und Postfachregeln in Exchange Online nicht wie erwartet funktionieren](#).

# Verwalten des Journalings

18.12.2018 • 16 minutes to read

Journaling helfen Ihrer Organisation auf rechtlichen, behördlichen und organisatorischen Compliance-Bestimmungen reagieren, indem Sie die Aufzeichnung von ein- und ausgehenden e-Mail-Kommunikation. In diesem Thema zeigt, wie Sie grundlegende Aufgaben im Zusammenhang mit Journaling in Exchange Server und Exchange Online.

Standard-Journalkonfiguration wird auf eine Postfachdatenbank konfiguriert. Sie können dem Journal-Agent in Erfassung aller Nachrichten, die an und von Postfächern auf ein bestimmtes Postfach-Datenbank. Auch können Premium Journaling ermöglicht den Journal-Agent bieten mehr Granularität Journaling mithilfe von Journalregeln ausführen. Anstelle von Journalen können Sie alle Postfächer in einer Postfachdatenbank Journalregeln entsprechend der Anforderungen Ihrer Organisation durch einzelne Empfänger Journaling oder Mitglieder von Verteilergruppen konfigurieren. Sie benötigen eine Exchange Enterprise-Clientzugriffs Lizenz (CAL) Premium Journaling verwendet.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Journale" im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#).
- Ein Journalpostfach erstellt wurde, oder ein vorhandenes Postfach ist zur Verwendung als Journalpostfach verfügbar. Sie können nicht als ein Journalpostfach ein Exchange Online-Postfachs festlegen. Sie bieten Journalberichte auf einem lokalen System oder einem Drittanbieter-Archivierungsdienst Archivierung. Wenn Sie eine hybridbereitstellung mit Ihren Postfächern zwischen lokalen Servern und Exchange Online Teilen ausführen, können Sie ein lokales Postfach als Journalpostfach für Exchange Online und lokalen Postfächer festlegen.

### IMPORTANT

Wenn Sie eine Journalregel in Exchange konfiguriert haben meldet Online, um das Journal senden an ein Journalpostfach, die nicht vorhanden oder ist ein ungültiges Ziel, bleibt die Journal-Bericht in der Warteschlange Transport Rechenzentrumsserver Microsoft. In diesem Fall versucht Microsoft Datacenter Personal, wenden Sie sich an Ihrer Organisation, und bitten Sie das Problem zu beheben, damit die Journalberichte an ein Journalpostfach erfolgreich übermittelt werden können. Wenn Sie nach zwei Tagen hergestellt wird das Problem behoben hatte keine, wird Microsoft die problematisch Journalregel deaktiviert.

- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#). Wenn Sie Probleme mit dem **JournalingReportDNRTo** -Postfach haben, finden Sie unter [Transport- und Postfachregeln in Exchange Online nicht wie erwartet funktionieren](#).

# Erstellen einer Journalregel

## Erstellen einer Journalregel mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue > Journalregeln**, und klicken Sie dann auf **Hinzufügen**
2. Geben Sie im Feld **Journalregel** einen Namen für die Journalregel ein, und füllen Sie dann folgende Felder aus:
  - **Wenn die Nachricht wird gesendet oder von empfangen:** Geben Sie den Empfänger, der die Regel gerichtet wird. Sie können wählen Sie einen bestimmten Empfänger oder die Regel auf alle Nachrichten anzuwenden.
  - **Erfassung der folgenden Meldungen:** Geben Sie den Bereich der Journalregel. Sie können Journal nur die internen Nachrichten nur externen Nachrichten oder alle Nachrichten unabhängig vom Ursprung oder Ziel.
  - **Journalberichte senden an:** Geben Sie die Adresse des journalingpostfachs, das alle Journalberichte empfängt.

### NOTE

Sie können auch den Anzeigenamen oder den Alias des e-Mail-Benutzer oder eine e-Mail-Kontakt als das Journalpostfach eingeben. In diesem Fall werden an die externe e-Mail-Adresse des e-Mail-Benutzer oder e-Mail-Kontakts Journalberichte gesendet. Wie bereits erklärt, die externe e-Mail-Adresse des e-Mail-Benutzer oder e-Mail-Kontakt kann jedoch werden die Adresse des Exchange Online-Postfach.

3. Klicken Sie auf **Speichern**, um die Journalregel zu erstellen.

## Verwenden von Exchange Online PowerShell zum Erstellen einer Journalregel

In diesem Beispiel wird die Journalregel "Discovery Journal Recipients" erstellt, mit der auf alle Nachrichten, die von dem Benutzer "user1@contoso.com" gesendet und empfangen werden, die Journalfunktion angewendet wird.

```
New-JournalRule -Name "Discovery Journal Recipients" -Recipient user1@contoso.com -JournalEmailAddress "Journal Mailbox" -Scope Global -Enabled $True
```

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie eine der folgenden Aktionen aus, um sich zu vergewissern, dass Sie die Journalregel erfolgreich erstellt haben:

- Überprüfen Sie in der Exchange-Verwaltungskonsole, ob die neue Journalregel, die Sie erstellt haben, auf der Registerkarte **Journalregeln** aufgeführt wird.
- Von Exchange Online PowerShell stellen Sie sicher, dass die neue Journalregel vorhanden ist, indem Sie den folgenden Befehl (das folgende Beispiel überprüft die in der Exchange Online PowerShell-Beispiel oben erstellte Regel) ausführen:

```
Get-JournalRule "Discovery Journal Recipients"
```

[Zurück zum Seitenanfang](#)

## Anzeigen oder Ändern einer Journalregel

## Anzeigen oder Ändern einer Journalregel mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Compliance > Journalregeln**.
2. In der Listenansicht sehen Sie die Journalregeln in Ihrer Organisation.
3. Doppelklicken Sie auf die Regel, die Sie anzeigen oder ändern möchten.
4. Ändern Sie in **Journalregel** die gewünschten Einstellungen. Weitere Informationen zu den Einstellungen in diesem Dialogfeld finden Sie an früherer Stelle in diesem Thema unter [Use the EAC to create a journal rule](#).

## Verwenden von Exchange Online PowerShell anzeigen oder Ändern einer Journalregel

In diesem Beispiel wird eine Übersichtsliste aller Journalregeln in der Exchange-Organisation angezeigt:

```
Get-JournalRule
```

In diesem Beispiel die Journalregel "Brokerage" abgerufen und die Ausgabe über Pipes an das Cmdlet **Format-List** übergeben, um alle Parameter der Regel in einem Listenformat anzuzeigen:

```
Get-JournalRule "Brokerage Journal Rule" | Format-List
```

Wenn Sie die Eigenschaften einer bestimmten Regel ändern möchten, müssen Sie das Cmdlet [Set-JournalRule](#) verwenden. Dieses Beispiel ändert den Namen der Journalregel `JR-Sales` auf `TraderVault`. Die folgenden regeleinstellungen werden auch geändert:

- Empfänger
- JournalEmailAddress
- Umfang

```
Set-JournalRule JR-Sales -Name TraderVault -Recipient traders@woodgrovebank.com -JournalEmailAddress tradervault@woodgrovebank.com -Scope Internal
```

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie eine der folgenden Aktionen aus, um sich zu vergewissern, dass Sie eine Journalregel erfolgreich geändert haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Richtlinientreue, > Journalregeln**. Doppelklicken Sie auf die Regel, die Sie geändert haben, und stellen Sie sicher, dass die Änderungen gespeichert wurden.
- Von Exchange Online PowerShell stellen Sie sicher, dass Sie die Journalregel erfolgreich geändert, indem Sie den folgenden Befehl ausführen. Mit diesem Befehl werden die Eigenschaften aufgelistet, die Sie zusammen mit dem Namen der Regel (im Beispiel unten wird überprüft, ob in Exchange Online PowerShell-Beispiel oben geänderte Regel) geändert:

```
Get-TransportRule "TraderVault" | Format-List Name,Recipient,JournalEmailAddress,Scope
```

[Zurück zum Seitenanfang](#)

## Aktivieren oder Deaktivieren einer Journalregel

## **IMPORTANT**

Wenn Sie eine Journalregel deaktivieren, wird der Journal-Agent Journaling Nachrichten, die durch diese Regel zielorientierten beendet. Während eine Journalregel deaktiviert ist, werden alle Nachrichten, die normalerweise von der Regel Journal hätten Journal nicht. Stellen Sie sicher, dass Sie nicht die rechtlichen oder Compliance Anforderungen Ihrer Organisation durch Deaktivieren einer Journalregel gefährdet sind.

## **Aktivieren oder Deaktivieren einer Journalregel mithilfe der Exchange-Verwaltungskonsole**

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Compliance > Journalregeln**.
2. Wählen Sie in der Listenansicht, in der Spalte **auf** neben dem Namen der Regel das Kontrollkästchen, um die Regel zu aktivieren oder deaktivieren, um die Regel zu deaktivieren.

## **Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren einer Journalregel**

In diesem Beispiel wird die Regel "Contoso" aktiviert.

```
Enable-JournalRule "Contoso Journal Rule"
```

In diesem Beispiel wird die Regel "Contoso" deaktiviert.

```
Disable-JournalRule "Contoso Journal Rule"
```

## **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Führen Sie eine der folgenden Aktionen aus, um sich zu vergewissern, dass Sie eine Journalregel erfolgreich aktiviert oder deaktiviert haben:

- Zeigen Sie in der Exchange-Verwaltungskonsole die Liste der Journalregeln an, und überprüfen Sie den Status des Kontrollkästchens in der Spalte **Ein**.
- Führen Sie von Exchange Online PowerShell den folgenden Befehl aus, um eine Liste aller Journalregeln in Ihrer Organisation zurückzugeben mit ihrem Status:

```
Get-JournalRule | Format-Table Name,Enabled
```

[Zurück zum Seitenanfang](#)

## **Entfernen einer Journalregel**

### **Entfernen einer Journalregel mithilfe der Exchange-Verwaltungskonsole**

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Verwaltung der Compliance > Journalregeln**.
2. In der Listenansicht, wählen Sie die Regel, die Sie entfernen möchten, und klicken Sie dann auf **Löschen**

### **Entfernen einer Journalregel mithilfe von Exchange Online PowerShell**

In diesem Beispiel wird die Regel "Brokerage Journal Rule" entfernt.

```
Remove-JournalRule "Brokerage Journal Rule"
```

## **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Führen Sie eine der folgenden Aktionen aus, um sich zu vergewissern, dass Sie die Journalregel erfolgreich

entfernt haben:

- Überprüfen Sie in der Exchange-Verwaltungskonsole, ob die Regel, die Sie entfernt haben, nicht mehr auf der Registerkarte **Journalregeln** aufgeführt wird.
- Führen Sie von Exchange Online PowerShell den folgenden Befehl aus, um sicherzustellen, dass die Regel, die Sie entfernen nicht mehr aufgeführt wird:

```
Get-JournalRule
```

[Zurück zum Seitenanfang](#)

## Aktivieren oder Deaktivieren des Journalings pro Postfachdatenbank

### Caution

Die Deaktivierung der Journalerstellung für Nachrichten einer Postfachdatenbank kann dazu führen, dass Ihre Organisation die geltenden Richtlinien zur Aufbewahrung von Nachrichten nicht mehr einhält. Wenn Sie die Journalerstellung für Nachrichten einer Postfachdatenbank deaktivieren, werden keine Journalbelege mehr für Nachrichten gesendet, die von Postfächern in der Postfachdatenbank gesendet oder empfangen werden.

### Aktivieren oder Deaktivieren des Journalings pro Postfachdatenbank mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Server > Datenbanken**.
2. Doppelklicken Sie in der Listenansicht auf die Postfachdatenbank, für die Sie das Journaling aktivieren möchten.
3. Klicken Sie auf **Wartung**, und klicken Sie dann neben dem Feld **Journalempfänger** auf **Durchsuchen**, um das Journalingpostfach auszuwählen. Durch Angabe eines Journalempfängers wird das Journaling für die Datenbank aktiviert.

Zum Deaktivieren des Journalings entfernen Sie den Journalempfänger durch Klicken auf **X entfernen**.

### Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren des journalings pro Postfachdatenbank

In diesem Beispiel wird das Journaling für die Postfachdatenbank "Sales Database" aktiviert, und das Journalpostfach "Sales Database" wird als Journalempfänger festgelegt.

```
Set-MailboxDatabase "Sales Database" -JournalRecipient "Sales Database Journal Mailbox"
```

In diesem Beispiel wird die Journalerstellung pro Postfachdatenbank für die Postfachdatenbank "Sales Database" deaktiviert.

```
Set-MailboxDatabase "Sales Database" -JournalRecipient $Null
```

In diesem Beispiel wird die journalings pro Postfachdatenbank auf aller Postfachdatenbanken in der Exchange-Organisation deaktiviert. Das Cmdlet **Get-MailboxDatabase** wird verwendet, um alle Postfachdatenbanken in der Exchange-Organisation abgerufen und Ergebnisse mit dem Cmdlet an das Cmdlet **Set-MailboxDatabase** weitergeleitet werden.

```
Get-MailboxDatabase | Set-MailboxDatabase -JournalRecipient $Null
```

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie eine der folgenden Aktionen aus, um sich zu vergewissern, dass Sie das Journaling pro

Postfachdatenbank erfolgreich aktiviert oder deaktiviert haben:

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Server > Datenbanken**.
  2. Doppelklicken Sie auf die Datenbank, die Sie überprüfen möchten, und wählen Sie dann die Registerkarte **Wartung** aus.
  3. Wenn der richtige Journalempfänger im Feld **Journalempfänger** aufgeführt ist, haben Sie das Journaling für die Postfachdatenbank erfolgreich aktiviert. Wenn kein Journalempfänger aufgeführt ist, ist das Journaling für die Datenbank deaktiviert.
- Von Exchange Online PowerShell, führen Sie den folgenden Befehl aus, um eine Liste aller Postfachdatenbanken in Ihrer Organisation, einschließlich der ihnen zugeordneten Journalempfänger zurückzugeben. Aufzeichnung ist aktiviert für Datenbanken, die ein Journalempfänger aufgeführt ist, andernfalls ist er deaktiviert.

```
Get-MailboxDatabase | Format-Table Name,JournalRecipient
```

[Zurück zum Seitenanfang](#)

## Weitere Informationen

[Deaktivieren Sie oder aktivieren Sie der Journalfunktion für Voicemails und Benachrichtigungen über verpasste Anrufe](#)

[New-JournalRule](#)

[Get-JournalRule](#)

[Set-JournalRule](#)

[Enable-JournalRule](#)

[Disable-JournalRule](#)

[Remove-JournalRule](#)

[Set-MailboxDatabase](#)

# Konfigurieren von Journaling in Exchange Online

18.12.2018 • 3 minutes to read

Journaling ermöglicht Ihnen, die Archivierungsanforderungen Ihrer Organisation zu erfüllen. Sie können Journalregeln erstellen und über den Bedingungen der Regel entsprechenden Nachrichten verfügen, die an die in der Regel angegebene Journalingadresse gesendet werden. Im Folgenden finden Sie zwei Dinge, die Sie wissen sollten, bevor Sie mit der Erstellung von Journalregeln beginnen.

## Angeben eines Journalingpostfachs

Ein Journalingpostfach ist das Postfach oder der Empfänger, das bzw. der Journalberichte für Nachrichten empfängt, die mit den Bedingungen einer Journalregel übereinstimmen. Sie können andere Journalingpostfächer für andere Journalregeln angeben. Beispielsweise können Sie eine Journalregel für Journalnachrichten erstellen, die durch Benutzer in Europa gesendet oder empfangen wurden, und eine weitere Journalregel, die durch Benutzer in Nordamerika gesendet oder empfangen wurden, wobei jede Regel so konfiguriert wird, Journalberichte an die Adresse in der jeweils eigenen Geografie zu senden. Konfigurieren Sie alternativ unterschiedliche Journalregeln für Benutzer in den Finanz- und Rechtsabteilungen, und lassen Sie die Journalberichte in ähnlicher Weise an unterschiedliche Adressen senden.

Von Exchange Online wird das Senden von Journalberichten an ein Exchange Online-Postfach nicht unterstützt. Sie müssen die E-Mail-Adresse eines lokalen Archivierungssystems oder eines Drittanbieterarchivierungsdiensts als das Journalingpostfach angeben.

### IMPORTANT

Wenn Sie eine Journalregel konfiguriert haben, durch die Journalberichte an ein Journalingpostfach gesendet werden, das ist nicht vorhanden ist oder ein ungültiges Ziel darstellt, bleibt der Journalbericht in der Transportwarteschlange auf Microsoft-Rechenzentrumsservern. Die Zustellung von Elementen in der Warteschlange wird regelmäßig wiederholt. Wenn dies der Fall ist, wenden sich Microsoft-Rechenzentrumsmitarbeiter an Ihre Organisation und bitten Sie, das Problem zu beheben, damit die Journalberichte an ein Journalingpostfach übermittelt werden können. Wenn Sie anschließend das Problem nicht innerhalb von zwei Tagen gelöst haben, wird die problematische Journalregel von Microsoft deaktiviert.

## Auswählen eines alternativen Journalingpostfachs für nicht zustellbare Journalberichte

Wie zuvor beschrieben, werden nicht zustellbare Journalberichte auf Servern in Microsoft-Rechenzentren in der Warteschlange platziert. Nicht zustellbare Journalberichte können nicht an den Absender in einem Unzustellbarkeitsbericht (auch als NDR bezeichnet) zurückgegeben werden, da der Absender der Exchange Online-Dienst ist. Um die Unzustellbarkeitsberichte für nicht zustellbare Journalberichte zu verarbeiten, müssen Sie ein alternatives Journalingpostfach angeben, das die Unzustellbarkeitsberichte für alle nicht zugestellten Journalberichte akzeptiert.

Verwenden Sie Journalregeln, um die gesamte Kommunikation zur Unterstützung der E-Mail-Aufbewahrungs- oder -Archivierungsstrategie der Organisation aufzuzeichnen.

**Weitere Informationen**

Nicht zustellbare Journalberichte senden an: [admin@alpinehouse.onmicrosoft.com](mailto:admin@alpinehouse.onmicrosoft.com)



EIN	REGEL	BENUTZER	JOURNALBERICHTE SENDEN AN
<input checked="" type="checkbox"/>	Alpine House-Journalregel		journalmailbox@contoso.com
<input checked="" type="checkbox"/>	Brokerage-Journalregel	sjd@alpinehouse.onmicrosoft.c...	journalmailbox@contoso.com

Der ursprüngliche Journalbericht ist eine Anlage im Unzustellbarkeitsbericht. Sobald das Journalpostfach für einen nicht zustellbaren Journalbericht wieder verfügbar ist, können Sie die Funktion **Diese Nachricht erneut senden** in Outlook für die NDRs im alternativen Journalpostfach verwenden, um den unveränderten Zustellungsberichte an das Journalpostfach zu senden.

# Nachrichtenflussregeln (Transportregeln) in Exchange Online

18.12.2018 • 18 minutes to read

Mithilfe von Nachrichtenflussregeln (auch bekannt als Transportregeln) können Sie Nachrichten, die über Ihre Office 365-Organisation fließen, identifizieren und Maßnahmen dafür ergreifen.

Nachrichtenflussregeln sind mit den Posteingangsregeln vergleichbar, die in Outlook und Outlook im Web zur Verfügung stehen. Der Hauptunterschied besteht darin, dass Nachrichtenflussregeln Nachrichten während der Übertragung behandeln und nicht nach der Übermittlung der Nachricht an das Postfach.

Nachrichtenflussregeln enthalten einen reichhaltigeren Satz an Bedingungen, Ausnahmen und Aktionen, sodass Sie über die Flexibilität verfügen, viele Arten von Nachrichtenrichtlinien zu implementieren.

In diesem Artikel werden die [Komponenten](#) von Nachrichtenflussregeln und deren [Funktionsweise](#) erläutert.

Schritte zum Erstellen, Kopieren und Verwalten von Nachrichtenflussregeln finden Sie unter [Manage Transport Rules](#). Bei jeder Regel haben Sie die Möglichkeit, sie zu erzwingen, sie zu testen oder sie zu testen und den Absender zu benachrichtigen. Weitere Informationen zum Testen von Optionen finden Sie unter [Test a transport rule](#) und [Policy Tips](#).

Eine Zusammenfassung und ausführliche Berichte zu Nachrichten, die Nachrichtenflussregeln entsprechen, finden Sie unter [Verwenden von Berichten zum E-Mail-Schutz in Office 365, um Daten über Schadsoftware, Spam und Regelerkennung anzuzeigen](#).

Informationen zur Implementierung bestimmter Nachrichtenrichtlinien mithilfe von Nachrichtenflussregeln finden Sie in den folgenden Themen:

- [Use mail flow rules to inspect message attachments in Office 365](#)
- [Enable message encryption and decryption in Office 365](#)
- [Common attachment blocking scenarios for mail flow rules](#)
- [Organization-wide message disclaimers, signatures, footers, or headers in Office 365](#)
- [Use mail flow rules so messages can bypass Clutter](#)
- [Use mail flow rules to route email based on a list of words, phrases, or patterns](#)
- [Use mail flow rules to set the spam confidence level \(SCL\) in messages](#)
- [Create organization-wide safe sender or blocked sender lists in Office 365](#)
- [Common message approval scenarios](#)
- [Definieren von Regeln zum Verschlüsseln oder Entschlüsseln von E-Mail-Nachrichten](#)

## Komponenten von Nachrichtenflussregeln

Eine Nachrichtenflussregel besteht aus Bedingungen, Ausnahmen, Aktionen und Eigenschaften:

- **Bedingung:** Identifizieren der Nachrichten, die die Aktionen, die angewendet werden soll. Einige Bedingungen untersuchen Nachrichtenkopfzeilenfeldern (beispielsweise an, aus, oder "Cc" Felder). Sonstiges untersuchen Nachrichteneigenschaften (beispielsweise den Betreff der Nachricht, Body,

Anlagen, Nachrichtengröße oder Nachrichtenklassifikation). Den meisten Fällen müssen Sie einen Vergleichsoperator angeben (beispielsweise gleich ist, entspricht nicht oder enthält) und den Wert übereinstimmen. Wenn keine Bedingungen oder Ausnahmen vorhanden sind, wird die Regel auf alle Nachrichten angewendet.

Weitere Informationen zu Mail flow regelbedingungen in Exchange Online, finden Sie unter [E-Mail-Fluss von regelbedingungen und Ausnahmen \(Prädikate\) in Exchange Online](#).

- **Ausnahmen:** optional die Nachrichten, die für die Aktionen gelten sollte nicht identifizieren. Die gleiche Nachricht-Bezeichner, die in Bedingungen verfügbar sind, sind auch in Ausnahmen verfügbar. Ausnahmen Bedingungen überschreiben und zu verhindern, dass die Regelaktionen auf eine Nachricht angewendet wird, auch wenn die Nachricht alle konfigurierten Aktionen entspricht.
- **Aktionen:** Aktionen für Nachrichten, die die Bedingungen in der Regel übereinstimmen, und Ausnahmen entsprechen nicht angeben. Viele Aktionen stehen zur Verfügung, wie etwa ablehnen, löschen oder Umleiten von Nachrichten, weitere Empfänger hinzufügen, Präfixe Betreff der Nachricht hinzuzufügen oder Haftungsausschlüsse im Textkörper Nachricht einfügen.

Weitere Informationen zu Regelaktionen, die in Exchange Online verfügbaren e-Mail-Fluss, finden Sie unter [E-Mail-Fluss Aktionen in Exchange Online Regel](#).

- **Eigenschaften:** Geben Sie andere Einstellungen von Regeln, die nicht von Bedingungen, Ausnahmen und Aktionen sind. Angenommen, wenn die Regel angewendet werden soll, ob erzwungen oder getestet, die Regel und den Zeitraum an, wenn die Regel aktiv ist.

Weitere Informationen finden Sie im Abschnitt [Eigenschaften von Nachrichtenflussregeln](#) in diesem Thema.

### Mehrere Bedingungen, Ausnahmen und Aktionen

Die folgende Tabelle zeigt, wie mehrere Bedingungen, Bedingungswerte, Ausnahmen und Aktionen in einer Regel verarbeitet werden.

KOMPONENTE	LOGIK	KOMMENTARE
Mehrere Bedingungen	UND	Eine Nachricht muss allen Bedingungen in der Regel entsprechen. Wenn eine von zwei Bedingungen erfüllt werden muss, verwenden Sie für die Bedingungen separate Regeln. Wenn Sie z. B. Nachrichten mit Anlagen und Nachrichten, die einen bestimmten Text enthalten, die gleiche Haftungsausschlusserklärung hinzufügen möchten, erstellen Sie für jede Bedingung eine Regel. In der Exchange-Verwaltungskonsole können Sie eine Regel ganz einfach kopieren.

KOMPONENTE	LOGIK	KOMMENTARE
Eine Bedingung mit mehreren Werten	ODER	Bei einigen Bedingungen können Sie mehr als einen Wert angeben. Die Nachricht muss einem der angegebenen Werte (nicht allen) entsprechen. Beispiel: Wenn eine E-Mail den Betreff Informationen zum Börsenkurs hat und die Bedingung <b>Betreff enthält eines der folgenden Wörter</b> für die Übereinstimmung mit den Wörtern Contoso oder Börsenkurs konfiguriert ist, gilt die Bedingung als erfüllt, da der Betreff mindestens einen der angegebenen Werte enthält.
Mehrere Ausnahmen	ODER	Wenn eine Nachricht einer der Ausnahmen entspricht, werden die Aktionen nicht angewendet. Die Nachricht muss nicht allen Ausnahmen entsprechen.
Mehrere Aktionen	UND	Für Nachrichten, die die Bedingungen einer Regel erfüllen, werden alle in der Regel angegebenen Aktionen ausgeführt. Wenn beispielsweise die Aktionen <b>Dem Betreff der Nachricht Folgendes voranstellen</b> und <b>Empfänger zum Feld "Bcc" hinzufügen</b> ausgewählt wurden, werden beide Aktionen auf die Nachricht angewendet. Denken Sie daran, dass einige Aktionen, wie <b>Nachricht ohne Benachrichtigung anderer Benutzer löschen</b> , verhindern, dass nachfolgende Regeln auf die Nachricht angewendet werden. Bei anderen Aktionen wie <b>Nachricht weiterleiten</b> sind keine zusätzlichen Aktionen zulässig. Sie können für eine Regel auch eine Aktion festlegen, sodass bei Anwendung dieser Regel nachfolgende Regeln nicht auf die Nachricht angewendet werden.

## Eigenschaften von Nachrichtenflussregeln

Die folgende Tabelle beschreibt die Regeleigenschaften, die in Nachrichtenflussregeln zur Verfügung stehen.

EIGENSCHAFTENNAME IN DER EXCHANGE-VERWALTUNGSKONSOLE	PARAMETERNAME IN POWERSHELL	BESCHREIBUNG
--	-----------------------------	--------------

EIGENSCHAFTENNAME IN DER EXCHANGE-VERWALTUNGSKONSOLE	PARAMETERNAME IN POWERSHELL	BESCHREIBUNG
<b>Priority</b>	<i>Priority</i>	<p>Gibt die Reihenfolge an, in der die Regeln auf Nachrichten angewendet werden. Die Standardpriorität basiert auf dem Erstellungsdatum der Regel (ältere Regeln haben eine höhere Priorität als neuere Regeln, und Regeln mit höherer Priorität werden vor Regeln mit niedrigerer Priorität verarbeitet).</p> <p>Sie ändern die Regelpriorität in der Exchange-Verwaltungskonsole, indem Sie die Regel in der Liste der Regeln nach oben oder unten verschieben. In der PowerShell legen Sie die Prioritätsnummer fest (0 ist die höchste Priorität).</p> <p>Wenn Sie z. B. eine Regel verwenden, um Nachrichten abzulehnen, die eine Kreditkartennummer enthalten, und eine andere Regel, die eine Genehmigung erfordert, sollte die Ablehnungsregel zuerst angewendet werden, und es sollten keine anderen Regeln mehr angewendet werden.</p> <p>Weitere Informationen finden Sie unter <a href="#">Festlegen der Priorität einer Regel der e-Mail-Fluss</a>.</p>
<b>Mode</b>	<i>Mode</i>	<p>Sie können angeben, ob die Regel sofort mit der Verarbeitung von Nachrichten beginnen soll oder ob Sie Regeln ohne Auswirkungen auf die Übermittlung der Nachricht (mit oder ohne Verhinderung von Datenverlust oder DLP-Richtlinientipps) testen möchten.</p> <p>Richtlinientipps zeigen dem Ersteller einer Nachricht in Outlook oder Outlook im Web einen Hinweis mit Informationen über mögliche Richtlinienverletzungen an. Weitere Informationen finden Sie unter <a href="#">Richtlinientipps</a>.</p> <p>Weitere Informationen zu den Modi finden Sie unter <a href="#">Test a mail flow rule</a>.</p>
<b>Diese Regel an folgendem Datum aktivieren</b> <b>Diese Regel an folgendem Datum deaktivieren</b>	<i>ActivationDate</i> <i>ExpiryDate</i> .	Gibt den Datumsbereich an, in dem die Regel aktiv ist.
Kontrollkästchen <b>Ein</b> aktiviert oder nicht aktiviert	<p>Neuer Regeln: Parameter <code>_Enabled</code> gibt das Cmdlet <b>New-TransportRule</b>.</p> <p>Vorhandene Regeln: Verwenden Sie die Cmdlets <b>Enable-TransportRule</b> oder <b>Disable-TransportRule</b>.</p> <p>Der Wert wird in der <b>State</b> - Eigenschaft der Regel angezeigt.</p>	<p>Sie können eine deaktivierte Regel erstellen und diese aktivieren, wenn Sie sie testen möchten. Alternativ können Sie eine Regel deaktivieren, ohne sie zu löschen, um die Einstellungen beizubehalten.</p>

EIGENSCHAFTENNAME IN DER EXCHANGE-VERWALTUNGSKONSOLE	PARAMETERNAME IN POWERSHELL	BESCHREIBUNG
<b>Nachricht zurückstellen, wenn die Regelverarbeitung nicht abgeschlossen wird</b>	<i>RuleErrorAction</i>	Sie können angeben, wie die Nachricht behandelt werden soll, wenn die Regelverarbeitung nicht abgeschlossen werden kann. Standardmäßig wird die Regel ignoriert, aber Sie können angeben, dass die Nachricht erneut zur Verarbeitung übermittelt werden soll.
<b>Absenderadresse in Nachricht vergleichen</b>	<i>SenderAddressLocation</i>	Wenn die Regel Bedingungen oder Ausnahmen verwendet, die die E-Mail-Adresse des Absenders überprüfen, finden Sie den Wert in der Nachrichtenkopfzeile und/oder im Nachrichtenumschlag.
<b>Verarbeiten weiterer Regeln beenden</b>	<i>SenderAddressLocation</i>	Dies ist eine Aktion für die Regel, aber sie sieht in der Exchange-Verwaltungskonsole wie eine Eigenschaft aus. Sie können auswählen, dass keine weiteren Regeln auf eine Nachricht angewendet werden, nachdem eine Nachricht durch eine Regel verarbeitet wurde.
<b>Comments</b>	<i>Comments</i>	Sie können beschreibende Kommentare zur Regel eingeben.

## Wie Nachrichtenflussregeln auf Nachrichten angewendet werden

Alle Nachrichten, die durch Ihre Organisation geleitet werden für die aktivierte Mail Flow Regeln in Ihrer Organisation ausgewertet. Regeln werden in der angegebenen Reihenfolge auf den **E-Mail-Fluss** verarbeitet > **Regeln** Seite in der Exchange-Verwaltungskonsole oder basierend auf *den entsprechenden Prioritätswert Parameter in der PowerShell*.

Jede Regel bietet außerdem die Möglichkeit, die Verarbeitung weiterer Regeln anzuhalten, wenn die Regel erfüllt wird. Diese Einstellung ist für Nachrichten wichtig, die die Bedingungen in mehreren E-Mail-Flussregeln erfüllen. (Welche Regel soll auf die die Nachricht angewendet werden? Alle? Nur eine?)

### Unterschiede in der Verarbeitung basierend auf dem Nachrichtentyp

Es gibt verschiedene Nachrichtentypen, die eine Organisation durchlaufen. Die folgende Tabelle zeigt, welche Nachrichtentypen von Nachrichtenflussregeln verarbeitet werden können.

NACHRICHTENTYP	KANN EINE REGEL ANGEWENDET WERDEN?
<b>Normale Nachrichten:</b> Nachrichten, die einen einzelnen rich-Text-Format (RTF), HTML oder nur-Text enthalten Nachricht Nachrichtentext oder eine Multipart oder Alternative Satz von Nachrichtentexte.	Ja

NACHRICHTENTYP	KANN EINE REGEL ANGEWENDET WERDEN?
<b>Office 365 Message Encryption:</b> Nachrichten, die von Office 365 Message Encryption in Office 365 verschlüsselt. Weitere Informationen finden Sie unter <a href="#">Office 365 Message Encryption</a> .	Regeln können immer auf Umschlagkopfzeilen zugreifen und Nachrichten auf Grundlage von Bedingungen verarbeiten, mit denen diese Kopfzeilen untersucht werden. Damit eine Regel den Inhalt einer verschlüsselten Nachricht überprüft oder ändert, müssen Sie überprüfen, ob die Transportentschlüsselung aktiviert ist („Obligatorisch“ oder „Optional“; der Standardwert ist „Optional“). Weitere Informationen finden Sie unter <a href="#">Aktivieren oder Deaktivieren der Transportentschlüsselung</a> . Sie können auch eine Regel erstellen, die verschlüsselte Nachrichten automatisch entschlüsselt. Weitere Informationen finden Sie unter <a href="#">Definieren von Regeln zum Ver- oder Entschlüsseln von E-Mail-Nachrichten</a> .
<b>S/MIME-Verschlüsselte Nachrichten</b>	Regeln können nur auf Umschlagkopfzeilen zugreifen und Nachrichten auf Grundlage von Bedingungen verarbeiten, mit denen diese Kopfzeilen untersucht werden. Regeln mit Bedingungen, die eine Untersuchung des Nachrichteninhalts erfordern, oder Aktionen, die den Inhalt der Nachricht ändern, können nicht verarbeitet werden.
<b>RMS-geschützten Nachrichten:</b> Nachrichten, die ein Active Directory-Rechteverwaltungsdienste (AD RMS) oder den Azure Rights Management (RMS) Richtlinie angewendet wurde.	Regeln können immer auf Umschlagkopfzeilen zugreifen und Nachrichten auf Grundlage von Bedingungen verarbeiten, mit denen diese Kopfzeilen untersucht werden. Damit eine Regel den Inhalt einer RMS-geschützten Nachricht überprüft oder ändert, müssen Sie überprüfen, ob die Transportentschlüsselung aktiviert ist („Obligatorisch“ oder „Optional“; der Standardwert ist „Optional“). Weitere Informationen finden Sie unter <a href="#">Aktivieren oder Deaktivieren der Transportentschlüsselung</a> .
<b>Unverschlüsselt signierte Nachrichten:</b> Nachrichten, die signiert, aber nicht verschlüsselt.	Ja
<b>UM Nachrichten:</b> Nachrichten, die erstellt oder vom Unified Messaging-Dienst verarbeitet werden, z. B. Voicemail, Fax, Benachrichtigungen über verpasste Anrufe und Nachrichten erstellt oder mithilfe von Microsoft Outlook Voice Access weitergeleitet werden.	Ja
<b>Anonyme Nachrichten:</b> von anonymen Absendern gesendete Nachrichten.	Ja
<b>Berichte lesen:</b> Berichte, die als Reaktion auf bestätigungsanforderungen Lesen von Absendern generiert werden. Lesen Berichte weisen eine Nachrichtenkategorie des <code>IPM.Note*.MdnRead</code> oder <code>IPM.Note*.MdnNotRead</code> .	Ja

## Was muss ich sonst noch wissen?

- Der **Version-** oder **RuleVersion**-Eigenschaftenwert für eine Regel ist in Exchange Online nicht

wichtig.

- Nach dem Erstellen oder Ändern einer E-Mail-Flussregel kann es bis zu 30 Minuten dauern, bis die neue oder aktualisierte Regel auf Nachrichten angewendet wird.

## Weitere Informationen

[Verwalten von Nachrichtenflussregeln](#)

[Überprüfen von Nachrichtenanlagen mithilfe von Nachrichtenflussregeln in Office 365](#)

[Organization-wide Disclaimers, Signatures, Footers, or Headers](#)

[Manage message approval](#)

[E-Mail-Fluss Regel Verfahren im Exchange Online](#)

[Transport- und Postfachregelgrenzen](#)

# Nachrichtenflussregel-Bedingungen und -Ausnahmen (Prädikate) in Exchange Online

18.12.2018 • 48 minutes to read

Bedingungen und Ausnahmen in Nachrichtenflussregeln (auch als Transportregeln bekannt) identifizieren die Nachrichten, auf welche die Regel angewendet oder nicht angewendet wird. Wenn durch die Regel beispielsweise ein Haftungsausschluss zur Nachricht hinzufügt wird, können Sie die Regel so konfigurieren, dass sie nur auf Nachrichten angewendet wird, die bestimmte Wörter enthalten, auf Nachrichten, die von bestimmten Benutzern gesendete werden, oder auf alle Nachrichten mit Ausnahme derjenigen, die von Mitgliedern einer bestimmten Gruppe gesendet werden. Die Bedingungen und Ausnahmen in Nachrichtenflussregeln werden gemeinsam auch als Prädikate bezeichnet, da es für jede Bedingung eine entsprechende Ausnahme mit genau denselben Einstellungen und derselben Syntax gibt. Der einzigen Unterschied ist: Bedingungen geben die einzuschließenden Nachrichten an, während Ausnahmen auszuschließende Nachrichten angeben.

Die meisten Bedingungen und Ausnahmen haben eine Eigenschaft, die einen oder mehrere Werte erfordern. Beispielsweise erfordert die Bedingung **Der Absender lautet** die Angabe des Absenders der Nachricht. Einige Bedingungen weisen zwei Eigenschaften auf. Wenn Sie beispielsweise die Bedingung **Eine Nachrichtenkopfzeile enthält mindestens eines dieser Wörter** verwenden, muss eine Eigenschaft den Nachrichtenkopf und eine zweite Eigenschaft den zu suchenden Text im Nachrichtenkopf angeben. Einige Bedingungen oder Ausnahmen haben keine Eigenschaften. Beispielsweise sucht die Bedingung **Mindestens eine Anlage hat ausführbaren Inhalt** einfach nach Anlagen in Nachrichten, die ausführbaren Inhalt haben.

Weitere Informationen zu e-Mail-Flussregeln in Exchange Online finden Sie unter [E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#).

Weitere Informationen zu Bedingungen und Ausnahmen in e-Mail-Fluss Regeln in Exchange Online Protection oder Exchange-Server finden Sie unter [Mail Flow regelbedingungen und Ausnahmen \(Prädikate\) in Exchange Online Protection](#) oder [E-Mail-Fluss von regelbedingungen und Ausnahmen \(Prädikate\) in Exchange Server](#).

## Bedingungen und Ausnahmen für Nachrichtenflussregeln in Exchange Online

Die Tabellen in den folgenden Abschnitten beschreiben die Bedingungen und Ausnahmen, die in Nachrichtenflussregeln in Exchange Online zur Verfügung stehen. Die Eigenschaftstypen werden im Abschnitt **Eigenschaftentypen** beschrieben.

[Absender](#)

[Empfänger](#)

[Nachrichtenbetreff oder -text](#)

[Anlagen](#)

[Alle Empfänger](#)

[Nachrichten mit Typen vertraulicher Informationen, To- und Cc-Werte, Größe und Zeichensätze](#)

[Absender und Empfänger](#)

[Nachrichteneigenschaften](#)

[Nachrichtenkopfzeilen](#)

### Hinweise:

- Nach dem Auswählen einer Bedingung oder eine Ausnahme in der Exchange-Verwaltungskonsole (EAC) ist der Wert, der letztendlich im Feld **Diese Regel anwenden, wenn** oder **Außer, wenn** angezeigt wird, häufig anders (kürzer) als der ausgewählte Klickpfadwert. Wenn Sie zudem neue Regeln basierend auf einer Vorlage (eine gefilterte Liste von Szenarien) erstellen, können Sie häufig einen kurzen Bedingungsnamen auswählen anstatt dem vollständigen Klickpfad zu folgen. Die kurzen Namen und vollständigen Klickpfadwerte werden in der Spalte "EAC" in den Tabellen angezeigt.
- Wenn Sie im EAC **[Auf alle Nachrichten anwenden]** auswählen, können Sie keine anderen Bedingungen angeben. Das Äquivalent in Exchange Online PowerShell besteht darin, eine Regel ohne Angabe von Bedingungsparametern zu erstellen.
- Die Einstellungen und Eigenschaften sind in Bedingungen und Ausnahmen gleich, daher werden in der Ausgabe des Cmdlet **Get-TransportRulePredicate** keine Ausnahmen separat aufgelistet. Darüber hinaus unterscheiden sich die Namen einiger der Prädikate, die von diesem Cmdlet zurückgegeben werden, von den entsprechenden Parameternamen. Ein Prädikat kann möglicherweise mehrere Parameter erfordern.

## Absender

Für Bedingungen und Ausnahmen, die die Adresse des Absenders überprüfen, können Sie festlegen, wo die Regel nach der Adresse des Absenders sucht.

Klicken Sie in der Exchange-Verwaltungskonsole in den Abschnitt **Eigenschaften dieser Regel** auf **Übereinstimmung**

**Absenderadresse in der Nachricht.** Beachten Sie, dass Sie möglicherweise auf **Weitere Optionen**, um diese Einstellung finden Sie unter klicken. In Exchange Online PowerShell ist der Parameter *SenderAddressLocation*. Die verfügbaren Werte sind:

- **Kopfzeile:** nur untersuchen Absender in den Kopfzeilen (beispielsweise die **aus**, **Absender** oder **Antwort-an**-Felder). Dies ist der Standardwert.
- **Briefumschlag:** Untersuchen nur Absender aus der Nachrichtenumschlag (der **MAIL FROM** Wert, der im SMTP-Übermittlung, verwendet wurde, das in der Regel im Feld **Zurückgeben Pfad** gespeichert ist). Beachten Sie, dass die Nachricht Umschlag Suche nur für die folgenden Bedingungen (und die entsprechenden Ausnahmen) verfügbar ist:
  - **Der Absender ist ( Aus)**
  - **Der Absender ist Mitglied von ( FromMemberOf)**
  - **Die Absenderadresse enthält ( FromAddressContainsWords)**
  - **Die Absenderadresse entspricht ( FromAddressMatchesPatterns)**
  - **Ist die Domäne des Absenders ( SenderDomains)**
- **Kopf- oder Umschlag ( HeaderOrEnvelope )** Absender in der Nachrichtenkopfzeile und der Nachrichtenumschlag untersucht.

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Der Absender ist Absender &gt; ist diese Person</b>	<i>From</i> <i>ExceptIfFrom</i>	<b>Addresses</b>	Nachrichten, die von den angegebenen Postfächern, E-Mail-Benutzern oder E-Mail-Kontakten in der Organisation gesendet werden.
<b>Der Absender befindet sich in Absender &gt; ist extern/intern</b>	<i>FromScope</i> <i>ExceptIfFromScope</i>	<b>UserScopeFrom</b>	Nachrichten, die entweder durch interne Absender oder externe Absender gesendet werden.
<b>Der Absender ist Mitglied von Absender &gt; ist Mitglied dieser Gruppe</b>	<i>FromMemberOf</i> <i>ExceptIfFromMemberOf</i>	<b>Addresses</b>	Nachrichten, die von einem Mitglied einer festgelegten Gruppe gesendet werden.
<b>Die Absenderadresse enthält Absender &gt; Adresse enthält eines dieser Wörter</b>	<i>FromAddressContainsWords</i> <i>ExceptIfFromAddressContainsWords</i>	<b>Words</b>	Nachrichten, die die angegebenen Wörter in der E-Mail-Adresse des Absenders enthalten.
<b>Die Absenderadresse entspricht Absender &gt; Adresse entspricht jedem dieser Textmuster</b>	<i>FromAddressMatchesPatterns</i> <i>ExceptIfFromAddressMatchesPatterns</i>	<b>Patterns</b>	Nachrichten, bei denen die E-Mail-Adresse des Absenders Textmuster enthält, die mit dem angegebenen regulären Ausdruck übereinstimmen.
<b>Der Absender befindet sich auf einer der Empfängerlisten Der Absender &gt; befindet sich in einer Aufsichtsliste eines Empfängers</b>	<i>SenderInRecipientList</i> <i>ExceptIfSenderInRecipientList</i>	<b>SupervisionList</b>	Nachrichten, für die sich der Absender in der Liste „Zulassen“ oder „Blockieren“ des Empfängers befindet.
<b>Die angegebenen Eigenschaften des Absenders enthalten eines dieser Wörter Absender &gt; hat bestimmte Eigenschaften einschließlich eines dieser Wörter</b>	<i>SenderADAttributeContainsWords</i> <i>ExceptIfSenderADAttributeContainsWords</i>	Erste Eigenschaft: <b>ADAttribute</b> Zweite Eigenschaft: <b>Words</b>	Nachrichten, bei denen das angegebene Active DirectoryAttribut des Absenders eines der angegebenen Wörter enthält. Beachten Sie, dass das Attribut <b>Country</b> den aus zwei Buchstaben bestehenden Ländercode (z. B. DE für Deutschland) erfordert.

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Die angegebenen Eigenschaften des Absenders entsprechen diesen Textmustern</b> <b>Absender &gt; verfügt über bestimmte Eigenschaften, die diesen Textmustern entsprechen</b>	<i>SenderADAttributeMatchesPattern s ExceptIfSenderADAttributeMatche sPatterns</i>	Erste Eigenschaft: ADAttribute Zweite Eigenschaft: Patterns	Nachrichten, bei denen das angegebene Active Directory-Attribut des Absenders Textmuster enthält, die mit dem angegebenen regulären Ausdruck übereinstimmen.
<b>Der Absender hat den Richtlinientipp außer Kraft gesetzt</b> <b>Der Absender &gt; hat den Richtlinientipp außer Kraft gesetzt</b>	<i>HasSenderOverride ExceptIfHasSenderOverride</i>	N/V	Nachrichten, bei denen der Absender ausgewählt hat, eine Data Loss Prevention (DLP)-Richtlinie außer Kraft zu setzen. Weitere Informationen zu DLP-Richtlinien finden Sie unter <a href="#">Verhinderung von Datenverlust</a> .
<b>Absender-IP-Adresse befindet sich im Bereich</b> <b>Der Absender &gt; IP-Adresse ist in keinem dieser Bereiche oder stimmt mit keinem Bereich völlig überein</b>	<i>SenderIPRanges ExceptIfSenderIPRanges</i>	IPAddressRanges	Nachrichten, in denen die IP-Adresse des Absenders der angegebenen IP-Adresse entspricht oder innerhalb des angegebenen IP-Adressbereichs liegt.
<b>Die Domäne des Absenders ist</b> <b>Die Domäne &gt; es Absenders ist</b>	<i>SenderDomains ExceptIfSenderDomains</i>	DomainName	Nachrichten, bei denen die Domäne der E-Mail-Adresse des Absenders dem angegebenen Wert entspricht. Wenn Sie benötigen, finden Absenderdomänen, enthalten die angegebene Domäne (beispielsweise alle Unterdomänen einer Domäne), verwenden Sie <b>die Absenderadresse entspricht (FromAddressMatchesPatterns)</b> Bedingung aus, und geben Sie die Domäne mithilfe der Syntax: '@domain\.com\$' .

[Return to top](#)

## Empfänger

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Der Empfänger ist</b> <b>Empfänger &gt; ist diese Person</b>	<i>SentTo ExceptIfSentTo</i>	Addresses	Nachrichten, bei denen es sich bei einem der Empfänger um das angegebene Postfach, den E-Mail-Benutzer oder den E-Mail-Kontakt in der Organisation handelt. Die Empfänger können in den Feldern <b>To</b> , <b>Cc</b> oder <b>Bcc</b> der Nachricht angegeben werden. <b>Hinweis:</b> Sie können nicht angeben, Verteilergruppen oder e-Mail-aktivierte Sicherheitsgruppen. Wenn Sie die Aktion auf Nachrichten angewendet werden, die an eine Gruppe gesendet werden müssen, verwenden Sie stattdessen die Bedingung aus, <b>um Feld enthält (AnyOfToHeader)</b> .
<b>Der Empfänger befindet sich in</b> <b>Empfänger &gt; ist extern/extern</b>	<i>SentToScope ExceptIfSentToScope</i>	UserScopeTo	Nachrichten, die an interne oder externe Empfänger gesendet werden.

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Der Empfänger ist Mitglied von Der Empfänger &gt; ist Mitglied dieser Gruppe</b>	<i>SentToMemberOf</i> <i>ExceptIfSentToMemberOf</i>	Addresses	Nachrichten, die Empfänger enthalten, die Mitglieder der angegebenen Gruppe sind. Die Gruppe kann in den Feldern <b>To</b> , <b>Cc</b> oder <b>Bcc</b> der Nachricht sein.
<b>Die Empfängeradresse enthält Empfänger &gt; Adresse enthält eines dieser Wörter</b>	<i>RecipientAddressContainsWords</i> <i>ExceptIfRecipientAddressContainsWords</i>	Words	Nachrichten, die die angegebenen Wörter in der E-Mail-Adresse des Empfängers enthalten. <b>Hinweis:</b> Diese Bedingung berücksichtigt keine Nachrichten, die an Proxyadressen des Empfängers gesendet werden. Es werden nur Nachrichten berücksichtigt, die an die primäre E-Mail-Adresse des Empfängers gesendet werden.
<b>Die Adresse des Empfängers entspricht Empfänger &gt; Adresse entspricht jedem dieser Textmuster</b>	<i>RecipientAddressMatchesPatterns</i> <i>ExceptIfRecipientAddressMatchesPatterns</i>	Patterns	Nachrichten, bei denen die E-Mail-Adresse des Empfängers Textmuster enthält, die mit dem angegebenen regulären Ausdruck übereinstimmen. <b>Hinweis:</b> Diese Bedingung berücksichtigt keine Nachrichten, die an Proxyadressen des Empfängers gesendet werden. Es werden nur Nachrichten berücksichtigt, die an die primäre E-Mail-Adresse des Empfängers gesendet werden.
<b>Der Empfänger befindet sich in der Liste des Absenders Der Empfänger &gt; befindet sich in der Aufsichtsliste des Absenders</b>	<i>RecipientInSenderList</i> <i>ExceptIfRecipientInSenderList</i>	SupervisionList	Nachrichten, für die sich der Empfänger in der Liste „Zulassen“ oder „Blockieren“ des Absenders befindet.
<b>Die vom Empfänger angegebenen Eigenschaften enthalten eines dieser Wörter Empfänger &gt; hat bestimmte Eigenschaften einschließlich eines dieser Wörter</b>	<i>RecipientADAttributeContainsWords</i> <i>ExceptIfRecipientADAttributeContainsWords</i>	Erste Eigenschaft: ADAttribute Zweite Eigenschaft: Words	Nachrichten, bei denen das angegebene Active Directory-Attribut eines Empfängers eines der angegebenen Wörter enthält. Beachten Sie, dass das Attribut <b>Country</b> den aus zwei Buchstaben bestehenden Ländercode (z. B. DE für Deutschland) erfordert.
<b>Die angegebenen Eigenschaften des Empfängers entsprechen diesen Textmustern Empfänger &gt; verfügt über bestimmte Eigenschaften, die diesen Textmustern entsprechen</b>	<i>RecipientADAttributeMatchesPatterns</i> <i>ExceptIfRecipientADAttributeMatchesPatterns</i>	Erste Eigenschaft: ADAttribute Zweite Eigenschaft: Patterns	Nachrichten, bei denen das angegebene Active Directory-Attribut des Empfängers Textmuster enthält, die mit dem angegebenen regulären Ausdruck übereinstimmen.
<b>Die Domäne des Empfängers ist Die Domäne &gt; es Empfängers ist</b>	<i>RecipientDomains</i> <i>ExceptIfRecipientDomains</i>	DomainName	Nachrichten, bei denen die Domäne der E-Mail-Adresse des Empfängers dem angegebenen Wert entspricht. Wenn Sie benötigen, finden Empfängerdomänen, enthalten die angegebene Domäne (beispielsweise alle Unterdomänen einer Domäne), verwenden Sie <b>die Adresse des Empfängers entspricht</b> ( <i>RecipientAddressMatchesPatterns</i> ) Bedingung, und geben Sie die Domäne mithilfe der Syntax '@domain\.com\$' .

[Return to top](#)

## Nachrichtenbetreff oder -text

### NOTE

Die Suche nach Wörtern oder Textmustern im Betreff oder anderen Kopffeldern in der Nachricht tritt auf, *nachdem* die Nachricht aus der MIME-Content-Übertragung Codierung zum Übertragen der binären Nachricht zwischen SMTP-Servern in ASCII-Text verwendete Methode decodiert wurden. Sie können Bedingungen oder Ausnahmen für die Suche (in der Regel Base64)-codierten Werte der Betreff oder anderen Kopffelder in Nachrichten.

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Der Betreff oder Nachrichtentext enthält Betreff oder Textkörper &gt; Betreff oder Nachrichtentext enthält mindestens eines dieser Wörter</b>	<code>SubjectOrBodyContainsWords ExceptIfSubjectOrBodyContainsWords</code>	Words	Nachrichten, deren Feld <b>Subject</b> oder Nachrichtentext die angegebenen Wörter enthält.
<b>Der Betreff oder Nachrichtentext entspricht Betreff oder Textkörper &gt; Betreff oder Nachrichtentext entspricht diesen Textmustern</b>	<code>SubjectOrBodyMatchesPatterns ExceptIfSubjectOrBodyMatchesPatterns</code>	Patterns	Nachrichten, bei denen das Feld <b>Subject</b> oder der Nachrichtentext Textmuster enthält, die mit dem angegebenen regulären Ausdruck übereinstimmen.
<b>Der Betreff enthält Betreff oder Textkörper &gt; Betreff enthält eines der folgenden Wörter</b>	<code>SubjectContainsWords ExceptIfSubjectContainsWords</code>	Words	Nachrichten, deren Feld <b>Subject</b> die angegebenen Wörter enthält.
<b>Der Betreff entspricht Betreff oder Textkörper &gt; Betreff entspricht diesen Textmustern</b>	<code>SubjectMatchesPatterns ExceptIfSubjectMatchesPatterns</code>	Patterns	Nachrichten, bei denen das Feld <b>Subject</b> Textmuster enthält, die mit dem angegebenen regulären Ausdruck übereinstimmen.

[Return to top](#)

## Anlagen

Weitere Informationen darüber, wie E-Mail-Anlagen von Nachrichtenflussregeln geprüft werden, finden Sie unter [Überprüfen von Nachrichtenanlagen mithilfe von Nachrichtenflussregeln in Office 365](#).

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Inhalt mindestens einer Anlage enthält Ein Anlageninhalt &gt; enthält eines dieser Wörter</b>	<code>AttachmentContainsWords ExceptIfAttachmentContainsWords</code>	Words	Nachrichten, bei denen eine Anlage die angegebenen Wörter enthält.
<b>Der Inhalt mindestens einer Anlage entspricht Mindestens eine Anlage &gt; Inhalt stimmt mit diesen Textmustern überein</b>	<code>AttachmentMatchesPatterns ExceptIfAttachmentMatchesPatterns</code>	Patterns	Nachrichten, bei denen eine Anlage Textmuster enthält, die mit dem angegebenen regulären Ausdruck übereinstimmen. <b>Hinweis:</b> Nur die ersten 150 Kilobyte (KB) der Anlagen werden durchsucht.
<b>Der Inhalt keiner Anlage konnte überprüft werden Mindestens eine Anlage &gt; Inhalt kann nicht überprüft werden</b>	<code>AttachmentIsUnsupported ExceptIfAttachmentIsUnsupported</code>	N/V	Nachrichten, für die eine Anlage von Exchange Online nicht systemintern erkannt wird.

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Der Dateiname mindestens einer Anlage entspricht Mindestens eine Anlage &gt; einen Dateinamen hat, der diesen Textmustern entspricht</b>	<i>AttachmentNameMatchesPatterns ExceptIfAttachmentNameMatches Patterns</i>	Patterns	Nachrichten, bei denen der Dateiname einer Anlage Textmuster enthält, die mit dem angegebenen regulären Ausdruck übereinstimmen.
<b>Die Dateierweiterung mindestens einer Anlage entspricht Mindestens eine Anlage &gt; eine Dateierweiterung hat, die diese Wörter enthält</b>	<i>AttachmentExtensionmatcheswords dieses Prädikat ExceptIfAttachmentExtensionMatchesWords</i>	Words	Nachrichten, bei denen die Dateierweiterung einer Anlage einem der angegebenen Wörter entspricht.
<b>Eine Anlage ist größer als oder gleich Mindestens eine Anlage &gt; Größe ist größer oder gleich</b>	<i>AttachmentSizeOver ExceptIfAttachmentSizeOver</i>	Size	Nachrichten, bei denen eine Anlage größer oder gleich dem angegebenen Wert ist. In der Exchange-Verwaltungskonsole können Sie nur die Größe in Kilobyte (KB) angeben.
<b>Die Nachricht wurde nicht vollständig überprüft Mindestens eine Anlage &gt; Überprüfung nicht abgeschlossen wurde</b>	<i>AttachmentProcessingLimitExceeded ExceptIfAttachmentProcessingLimitExceeded</i>	N/V	Nachrichten, bei denen das Regelmodul das Prüfen der Anlagen nicht abschließen konnte. Sie können diese Bedingung zum Erstellen von Regeln verwenden, die zusammenarbeiten, um Nachrichten zu ermitteln und zu verarbeiten, deren Inhalt nicht vollständig überprüft werden konnte.
<b>Mindestens eine Anlage hat ausführbaren Inhalt Mindestens eine Anlage &gt; hat ausführbaren Inhalt</b>	<i>AttachmentHasExecutableContent ExceptIfAttachmentHasExecutableContent</i>	N/V	Nachrichten, bei denen eine Anlage eine ausführbare Datei ist. Das System untersucht die Dateieigenschaften anstatt sich auf die Dateierweiterung zu verlassen.
<b>Jede Anlage ist kennwortgeschützt Jede Anlage &gt; ist kennwortgeschützt</b>	<i>AttachmentIsPasswordProtected ExceptIfAttachmentIsPasswordProtected</i>	N/V	Nachrichten, bei denen eine Anlage kennwortgeschützt ist (und daher nicht überprüft werden kann). Die Kennworterkennung funktioniert nur bei Office-Dokumenten und ZIP-Dateien.
<b>hat diese Eigenschaften, einschließlich beliebige dieser Wörter Jede Anlage &gt; hat diese Eigenschaften, einschließlich eines dieser Wörter</b>	<i>AttachmentPropertyContainsWords ExceptIfAttachmentPropertyContainsWords</i>	Erste Eigenschaft: DocumentProperties Zweite Eigenschaft: Words	Nachrichten, bei denen die angegebene Eigenschaft eines angehängten Office-Dokuments die angegebenen Wörter enthält. Diese Bedingung hilft Ihnen, die Nachrichtenflussregeln in SharePoint, UNRESOLVED_TOKEN_VAL(exFCI) (FCI) in UNRESOLVED_TOKEN_VAL(exWinSvr2012R2) oder höher oder ein Drittanbieter-Klassifizierungssystem zu integrieren. Sie können aus einer Liste mit integrierten Eigenschaften auswählen oder eine benutzerdefinierte Eigenschaft angeben.

[Return to top](#)

## Alle Empfänger

Die Bedingungen und Ausnahmen in diesem Abschnitt bieten eine einzigartige Funktion, die Alle Empfänger wirkt sich auf, wenn die

Nachricht mindestens eines der angegebenen Empfänger enthält. Nehmen wir beispielsweise an, mit denen Sie eine Regel, die Nachrichten ablehnt. Wenn Sie eine Bedingung Empfänger aus dem Abschnitt [Empfänger](#) verwenden, wird die Nachricht nur für die angegebenen Empfänger zurückgewiesen. Angenommen, wenn die Regel in einer Nachricht, aber die Nachricht den angegebenen Empfänger findet enthält fünf anderen Empfänger. Die Nachricht wird zurückgewiesen für diese einen Empfänger und wird an die fünf anderen Empfänger übermittelt.

Wenn Sie eine Empfängerbedingung aus diesem Abschnitt hinzufügen, wird die gleiche Nachricht für den erkannten Empfänger und die fünf anderen Empfänger abgelehnt.

Im Gegensatz dazu Empfänger Ausnahme aus diesem Abschnitt *wird verhindert, dass die Regelaktion an Alle Empfänger der Nachricht, nicht nur für die erkannten Empfänger angewendet wird.*

**Hinweis:** Diese Bedingung berücksichtigt keine Nachrichten, die an Proxyadressen des Empfängers gesendet werden. Es werden nur Nachrichten berücksichtigt, die an die primäre E-Mail-Adresse des Empfängers gesendet werden.

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Mindestens eine Empfängeradresse enthält</b> <b>Mindestens ein Empfänger &gt; Adresse enthält eines dieser Wörter</b>	<code>AnyOfRecipientAddressContainsWords</code> <code>ExceptIfAnyOfRecipientAddressContainsWords</code>	Words	Nachrichten mit den angegebenen Wörtern in den Feldern <b>To</b> , <b>Cc</b> oder <b>Bcc</b> der Nachricht.
<b>Mindestens eine Adresse des Empfängers entspricht</b> <b>Mindestens ein Empfänger &gt; Adresse entspricht jedem dieser Textmuster</b>	<code>AnyOfRecipientAddressMatchesPatterns</code> <code>ExceptIfAnyOfRecipientAddressMatchesPatterns</code>	Patterns	Nachrichten, bei denen das Feld <b>To</b> , <b>Cc</b> oder <b>Bcc</b> Textmuster enthält, die mit dem angegebenen regulären Ausdruck übereinstimmen.

[Return to top](#)

### Nachrichten mit Typen vertraulicher Informationen, To- und Cc-Werte, Größe und Zeichensätze

Die Bedingungen in diesem Abschnitt, die Aussehen für Werte in den Feldern **an** und **Cc** verhält sich wie die Bedingungen im Abschnitt [Empfänger](#) (*Alle Empfänger der Nachricht sind betroffen, von der Regel, nicht nur die erkannten Empfänger*).

**Hinweis:** Diese Bedingung berücksichtigt keine Nachrichten, die an Proxyadressen des Empfängers gesendet werden. Es werden nur Nachrichten berücksichtigt, die an die primäre E-Mail-Adresse des Empfängers gesendet werden.

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Die Nachricht enthält vertrauliche Informationen</b> <b>Die Nachricht &gt; enthält diese Arten von vertraulichen Informationen</b>	<code>MessageContainsDataClassifications</code> <code>ExceptIfMessageContainsDataClassifications</code>	SensitiveInformationTypes	Nachrichten, die vertraulichen Informationen enthalten, wie in den Data Loss Prevention (DLP)-Richtlinien definiert. Diese Bedingung ist erforderlich für Regeln, die die Aktion <b>Absender mit Richtlinientipp benachrichtigen</b> ( <i>NotifySender</i> ) verwenden.
<b>Das Feld "An" enthält</b> <b>Die Nachricht &gt; Feld "An" enthält diese Person</b>	<code>AnyOfToHeader</code> <code>ExceptIfAnyOfToHeader</code>	Addresses	Nachrichten, deren Feld <b>To</b> einen oder mehrere der angegebenen Empfänger enthält.
<b>Das Feld "An" enthält ein Mitglied von</b> <b>Die Nachricht &gt; das Feld "An" enthält ein Mitglied dieser Gruppe</b>	<code>AnyOfToHeaderMemberOf</code> <code>ExceptIfAnyOfToHeaderMemberOf</code>	Addresses	Nachrichten, deren Feld <b>To</b> einen Empfänger enthält, der Mitglied der angegebenen Gruppe ist.
<b>Das Feld "Cc" enthält</b> <b>Die Nachricht &gt; Feld "Cc" enthält diese Person</b>	<code>AnyOfCcHeader</code> <code>ExceptIfAnyOfCcHeader</code>	Addresses	Nachrichten, deren Feld <b>Cc</b> einen oder mehrere der angegebenen Empfänger enthält.

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Das Feld "Cc" enthält ein Mitglied von Die Nachricht &gt; enthält ein Mitglied dieser Gruppe</b>	<code>AnyOfCcHeaderMemberOf ExceptIfAnyOfCcHeaderMemberOf</code>	Addresses	Nachrichten, deren Feld <b>Cc</b> einen Empfänger enthält, der Mitglied der angegebenen Gruppe ist.
<b>Das Feld "An" oder "Cc" enthält Die Nachricht &gt; Feld "An" oder "Cc" enthält diese Person</b>	<code>AnyOfToCcHeader ExceptIfAnyOfToCcHeader</code>	Addresses	Nachrichten, deren Feld <b>To</b> oder <b>Cc</b> einen oder mehrere der angegebenen Empfänger enthält.
<b>Das Feld "An" oder "Cc" enthält ein Mitglied von Die Nachricht &gt; das Feld "An" oder "Cc" enthält ein Mitglied dieser Gruppe</b>	<code>AnyOfToCcHeaderMemberOf ExceptIfAnyOfToCcHeaderMemberOf</code>	Addresses	Nachrichten, deren Feld <b>To</b> oder <b>Cc</b> einen Empfänger enthält, der Mitglied der angegebenen Gruppe ist.
<b>Die Nachrichtengröße ist größer als oder gleich Die Nachricht &gt; Größe ist größer als oder gleich</b>	<code>MessageSizeOver ExceptIfMessageSizeOver</code>	Size	<p>Nachrichten, deren Gesamtgröße (Nachricht sowie Anlagen) größer oder gleich dem angegebenen Wert ist.</p> <p>In der Exchange-Verwaltungskonsole können Sie nur die Größe in Kilobyte (KB) angeben.</p> <p><b>Hinweis:</b> Grenzwerte für die Nachrichtengröße für Postfächer werden vor E-Mail-Flussregeln ausgewertet. Eine Nachricht, die für ein Postfach zu groß ist, wird zurückgewiesen, bevor eine Regel mit dieser Bedingung auf diese Nachricht angewendet wird.</p>
<b>Der Name des Zeichensatzes der Nachricht enthält beliebige dieser Wörter Die Nachricht &gt; Name des Zeichensatzes enthält beliebige dieser Wörter</b>	<code>ContentCharacterSetContainsWords ExceptIfContentCharacterSetContainsWords</code>	CharacterSets	Nachrichten, die beliebige der angegebenen Zeichensatznamen enthalten.

[Return to top](#)

## Absender und Empfänger

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Der Absender ist einer der Empfänger Der Absender und der Empfänger &gt; die Beziehung des Absenders zum ist</b>	<code>SenderManagementRelationship ExceptIfSenderManagementRelationship</code>	ManagementRelationship	Nachrichten, bei denen entweder der Absender der Vorgesetzte eines Empfängers ist oder bei denen der Absender den Empfänger als Vorgesetzten hat.
<b>Die Nachricht wird zwischen Mitgliedern dieser Gruppen übermittelt Der Absender und der Empfänger &gt; die Nachricht wird zwischen Mitgliedern dieser Gruppen übermittelt</b>	<code>BetweenMemberOf1 und BetweenMemberOf2 ExceptIfBetweenMemberOf1 und ExceptIfBetweenMemberOf2</code>	Addresses	Nachrichten, die zwischen Mitgliedern der angegebenen Gruppen übermittelt werden.
<b>Der Vorgesetzte des Absenders oder Empfängers ist Der Absender und der Empfänger &gt; der Vorgesetzte des Absenders oder Empfängers ist diese Person</b>	<code>ManagerForEvaluatedUser und ManagerAddress ExceptIfManagerForEvaluatedUser und ExceptIfManagerAddress</code>	Erste Eigenschaft: EvaluatedUser Zweite Eigenschaft: Addresses	Nachrichten, bei denen entweder ein bestimmter Benutzer der Vorgesetzte des Absenders ist oder bei denen ein bestimmten Benutzer der Vorgesetzte eines Empfängers ist.

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Die Absender- und Empfängereigenschaft wird verglichen als Der Absender und der Empfänger &gt; die Absender- und Empfängereigenschaft wird verglichen als.</b>	<i>ADAttributeComparisonAttribute</i> und <i>ADComparisonOperator</i> <i>ExceptIfADAttributeComparisonAttribute</i> und <i>ExceptIfADComparisonOperator</i>	Erste Eigenschaft: <code>ADAttribute</code> Zweite Eigenschaft: <code>Evaluation</code>	Nachrichten, bei denen das angegebene Active Directory-Attribut für den Absender und den Empfänger übereinstimmt oder nicht übereinstimmt.

[Return to top](#)

## Nachrichteneigenschaften

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Der Nachrichttyp ist Nachrichteneigenschaften &gt; Nachrichtentyp einschließen</b>	<i>MessageTypeMatches</i> <i>ExceptIfMessageTypeMatches</i>	<code>MessageType</code>	Nachrichten vom angegebenen Typ. > [!NOTE]> Wenn Outlook oder Outlook Web App konfiguriert ist, um eine Nachricht weiterzuleiten, wird die <b>ForwardingSmtpAddress</b> - Eigenschaft zur Nachricht hinzugefügt. Der Nachrichtentyp wird nicht geändert, um <code>AutoForward</code> .
<b>Die Nachricht ist klassifiziert als Nachrichteneigenschaften &gt; diese Klassifikation einschließen</b>	<i>HasClassification</i> <i>ExceptIfHasClassification</i>	<code>MessageClassification</code>	Nachrichten mit der angegebenen Klassifikation. Hierbei handelt es sich um eine benutzerdefinierte Nachrichtenklassifikation, die Sie in Ihrer Organisation mit dem Cmdlet <b>New-MessageClassification</b> erstellen können.
<b>Die Nachricht ist nicht mit einer Klassifikation markiert Nachrichteneigenschaften &gt; enthalten keine Klassifikation</b>	<i>HasNoClassification</i> <i>ExceptIfHasNoClassification</i>	N/V	Nachrichten, die nicht über eine Nachrichtenklassifikation verfügen.
<b>Die Nachricht hat eine SCL-Bewertung größer oder gleich Nachrichteneigenschaften &gt; mit einer SCL-Bewertung größer oder gleich</b>	<i>SCLOver</i> <i>ExceptIfSCLOver</i>	<code>SCLValue</code>	Nachrichten, deren SCL-Bewertung (Spam Confidence Level) mit dem angegebenen Wert übereinstimmt bzw. diesen Wert überschreitet.
<b>Für die Nachricht ist eine Wichtigkeit festgelegt von Nachrichteneigenschaften &gt; Wichtigkeitsstufe einschließen</b>	<i>WithImportance</i> <i>ExceptIfWithImportance</i>	<code>Importance</code>	Nachrichten mit der angegebenen Wichtigkeitsstufe.

[Return to top](#)

## Nachrichtenkopfzeilen

### NOTE

Die Suche nach Wörtern oder Textmustern im Betreff oder anderen Kopffelder in der Nachricht tritt auf, *nachdem* die Nachricht aus der MIME-Content-Übertragung Codierung zum Übertragen der binären Nachricht zwischen SMTP-Server in ASCII-Text verwendete Methode decodiert wurden. Sie können Bedingungen oder Ausnahmen für die Suche (in der Regel Base64)-codierten Werte der Betreff oder anderen Kopffelder in Nachrichten.

BEDINGUNG ODER AUSNAHME IN DER EXCHANGE-VERWALTUNGSKONSOLE	BEDINGUNGS- UND AUSNAHMEPARAMETER IN EXCHANGE ONLINE POWERSHELL	EIGENSCHAFTENTYP	BESCHREIBUNG
<b>Ein Nachrichtenkopf enthält Eine Nachrichtenkopfzeile &gt; enthält mindestens eines dieser Wörter</b>	<i>HeaderContainsMessageHeader</i> und <i>HeaderContainsWords</i> <i>ExceptIfHeaderContainsMessageHeader</i> und <i>ExceptIfHeaderContainsWords</i>	Erste Eigenschaft: MessageHeaderField Zweite Eigenschaft: Words	Nachrichten, die das angegebene Header-Feld enthalten, und der Wert des Header-Felds enthält die angegebenen Wörter. Der Name des Header-Felds und der Wert des Header-Felds werden immer zusammen verwendet.
<b>Ein Nachrichtenkopf entspricht A message header &gt; matches these text patterns</b>	<i>HeaderMatchesMessageHeader</i> und <i>HeaderMatchesPatterns</i> <i>ExceptIfHeaderMatchesMessageHeader</i> und <i>ExceptIfHeaderMatchesPatterns</i>	Erste Eigenschaft: MessageHeaderField Zweite Eigenschaft: Patterns	Nachrichten, die das angegebene Header-Feld enthalten, und der Wert des Header-Felds enthält die angegebenen regulären Ausdrücke. Der Name des Header-Felds und der Wert des Header-Felds werden immer zusammen verwendet.

[Return to top](#)

## Eigenschaftentypen

Die in Bedingungen und Ausnahmen verwendeten Eigenschaftentypen werden in der folgenden Tabelle beschrieben.

### NOTE

Wenn die Eigenschaft eine Zeichenfolge ist, sind nachfolgende Leerzeichen nicht zulässig.

EIGENSCHAFTENTYP	GÜLTIGE WERTE	BESCHREIBUNG
ADAttribute	Wählen Sie aus einer vordefinierten Liste von Active Directory-Attributen aus.	<p>UNRESOLVED_TOKENBLOCK_VAL (PD_Transport_Rules_ADAttributes_Snippet) In der Exchange-Verwaltungskonsole an mehreren Wörtern oder Textmuster für das gleiche Attribut, trennen Sie die Werte durch Kommas getrennt werden. Beispielsweise sieht der Wert San Francisco Palo auch für das Attribut <b>Ort</b> für "Stadt oder gleich dem San Francisco" Stadt gleich Palo auch". Verwenden Sie die Syntax in Exchange Online PowerShell</p> <div style="border: 1px solid black; padding: 5px; background-color: #f9f9f9;"> <pre>"AttributeName1:Value1,Value 2 with spaces,Value3...","AttributeName2:Word4,Value 5 with spaces,Value6..."</pre> </div> <p>, wobei <b>Value</b> ist das Wort oder Text Muster, das übereinstimmen soll. Beispielsweise "City:San Francisco,Palo Alto" oder "City:San Francisco,Palo Alto", "Department:Sales,Finance". Wenn Sie mehrere Attribute oder für das gleiche Attribut mehrere Werte angeben, wird der Operator <b>oder</b> verwendet. Verwenden Sie keine Werte mit führenden oder nachstehenden Leerzeichen. Beachten Sie, dass das <b>Land</b>-Attribut des zwei Buchstaben ISO 3166-1 Ländercodes (z. B. DE für Deutschland) erfordert. Zum Suchen nach Werten finden Sie unter <a href="https://go.microsoft.com/fwlink/p/?LinkId=331680">https://go.microsoft.com/fwlink/p/?LinkId=331680</a>.</p>

EIGENSCHAFTENTYP	GÜLTIGE WERTE	BESCHREIBUNG
Addresses	Exchange Online-Empfänger	<p>Je nach Art der Bedingung oder Ausnahme können Sie möglicherweise ein beliebiges E-Mail-aktiviertes Objekt in der Organisation (z. B. empfängerbezogene Bedingungen) angeben, oder Sie müssen sich möglicherweise auf einen bestimmten Objekttyp beschränken (z. B. Gruppen für Gruppenmitgliedschaftsbedingungen). Zudem kann es sein, dass die Bedingung oder Ausnahme einen Wert erfordert oder mehrere Werte zulässt. Trennen Sie in Exchange Online PowerShell die einzelnen Werte durch Komma.</p> <p><b>Hinweis:</b> Diese Bedingung berücksichtigt keine Nachrichten, die an Proxyadressen des Empfängers gesendet werden. Es werden nur Nachrichten berücksichtigt, die an die primäre E-Mail-Adresse des Empfängers gesendet werden.</p>
CharacterSets	Array von Zeichensatznamen	<p>Eine oder mehrere Content Zeichensätze, die in einer Nachricht vorhanden sind. Beispiel:</p> <pre>Arabic/iso-8859-6 Chinese/big5 Chinese/euc-cn Chinese/euc-tw Chinese/gb2312 Chinese/iso-2022-cn Cyrillic/iso-8859-5 Cyrillic/koi8-r Cyrillic/windows-1251 Greek/iso-8859-7 Hebrew/iso-8859-8 Japanese/euc-jp Japanese/iso-022-jp Japanese/shift-jis Korean/euc-kr Korean/johab Korean/ks_c_5601-1987 Turkish/windows-1254 Turkish/iso-8859-9` Vietnamese/tcvn</pre>
DomainName	Array von SMTP-Domänen	<p>Beispielsweise <code>contoso.com</code> oder <code>eu.contoso.com</code>. In Exchange Online PowerShell können Sie mehrere Domänen, die durch Kommas getrennt angeben.</p>
EvaluatedUser	Einzelwert von <b>Sender</b> oder <b>Recipient</b>	<p>Gibt an, ob die Regel nach dem Vorgesetzten des Absenders oder dem Vorgesetzten des Empfängers sucht.</p>
Evaluation	Einzelner Wert <b>gleich</b> oder <b>ungleich</b> ( <code>NotEqual</code> )	<p>Beim Vergleichen des Attributs Active Directory des Absenders und der Empfänger wird hiermit angegeben, ob die Werte übereinstimmen sollen oder nicht.</p>
Importance	Einzelwert von <b>Low</b> , <b>Normal</b> oder <b>High</b>	<p>Die Wichtigkeitsstufe, die der Nachricht vom Absender in Outlook oder Outlook Web App zugewiesen wurde.</p>
IPAddressRanges	Array von IP-Adressen oder Adressbereichen	<p>Geben Sie die IPv4-Adressen mithilfe der folgenden Syntax: <b>eine IP-Adresse</b>: beispielsweise <code>192.168.1.1</code>. <b>IP-Adressbereich</b>: beispielsweise <code>192.168.0.1-192.168.0.254</code>. <b>Classless InterDomain Routing (CIDR) IP-Adressbereich</b>: beispielsweise <code>192.168.0.1/25</code>. In Exchange Online PowerShell können Sie mehrere IP-Adressen oder Bereiche durch Kommas getrennt angeben.</p>
ManagementRelationship	Einzelwert von <b>Vorgesetzter</b> oder <b>DirectReport</b> ( <code>DirectReport</code> )	<p>Gibt die Beziehung zwischen Absender und einem der Empfänger an. Die Regel überprüft das Attribut <b>Manager</b> in Active Directory, um festzustellen, ob der Absender der Vorgesetzte eines Empfängers ist oder ob der Absender den Empfänger als Vorgesetzten hat.</p>

EIGENSCHAFTENTYP	GÜLTIGE WERTE	BESCHREIBUNG
<code>MessageClassification</code>	Einzelne Nachrichtenklassifikation	<p>In der Exchange-Verwaltungskonsole wählen Sie aus der Liste der Nachrichtenklassifikationen, die Sie erstellt haben. In Exchange Online PowerShell verwenden Sie das Cmdlet <b>Get-MessageClassification</b>, um die Nachrichtenklassifikation zu identifizieren.</p> <p>Verwenden Sie beispielsweise den folgenden Befehl zum Suchen nach Nachrichten mit der <code>Company Internal</code> Klassifizierung und dem Nachrichtenbetreff mit dem Wert <code>CompanyInternal</code>.</p> <pre>New-TransportRule "Rule Name" -HasClassification @(Get-MessageClassification "Company Internal").Identity -PrependSubject "CompanyInternal"</pre>
<code>MessageHeaderField</code>	Einzelne Zeichenfolge	<p>Gibt den Namen des Header-Felds an. Der Name des Header-Felds wird immer zusammen mit dem Wert im Header-Feld angegeben (Wort- oder Text-Musterübereinstimmung). Die Nachrichtenkopfzeile ist eine Sammlung erforderlicher und optionaler Kopfzeilenfelder in der Nachricht. Beispiele für Kopfzeilenfelder sind <b>To</b>, <b>From</b>, <b>Received</b> und <b>Content-Type</b>. Offizielle Kopfzeilenfelder sind in RFC 5322 definiert. Inoffizielle Kopfzeilenfelder beginnen mit <b>X-</b> und werden als X-Header bezeichnet.</p>
<code>MessageType</code>	Einzelner Nachrichtentypwert	<p>Gibt einen der folgenden Nachrichtentypen:</p> <p><b>Automatische Antwort</b> (<code>OOF</code>) <b>automatisch weiterleiten</b> (<code>AutoForward</code>) <b>verschlüsselt Kalender Berechtigung gesteuert</b> (<code>PermissionControlled</code>) <b>Voicemail Signed</b> ** (<code>ApprovalRequest</code>) <b>Lesen des Empfangs</b> (<code>ReadReceipt</code>) &gt; [!NOTE]&gt; Wenn Outlook oder Outlook Web App ist so konfiguriert, dass eine Nachricht weiterleiten, wird die <b>ForwardingSmtpAddress</b>-Eigenschaft zur Nachricht hinzugefügt. Der Nachrichtentyp wird nicht geändert, um <code>AutoForward</code>.</p>
<code>Patterns</code>	Array regulärer Ausdrücke	<p>Gibt einen oder mehrere reguläre Ausdrücke an, die zur Identifizierung von Textmustern in Werte verwendet werden. Weitere Informationen finden Sie unter <a href="#">Syntax für reguläre Ausdrücke</a>. In Exchange Online PowerShell geben Sie mehrere reguläre Ausdrücke durch Komma getrennt an und setzen vor und nach jedem regulären Ausdruck Anführungszeichen (").</p>
<code>SCLValue</code>	Einer der folgenden Werte: <b>Umgehung Spamfilterung</b> ( <code>-1</code> ) ganzen Zahlen 0 bis 9	<p>Gibt den Schwellenwert der SCL-Bewertung (Spam Confidence Level) an, der einer Nachricht zugewiesen ist. Ein höherer SCL-Wert gibt an, dass eine Nachricht mit größerer Wahrscheinlichkeit Spam ist.</p>

EIGENSCHAFTENTYP	GÜLTIGE WERTE	BESCHREIBUNG
SensitiveInformationTypes	Array vertraulicher Informationstypen	<p>Gibt einen oder mehrere Typen vertraulicher Informationen, die in Ihrer Organisation definiert sind. Eine Liste mit integrierten vertraulichen Informationstypen finden Sie unter <a href="#">welche den Typen in Exchange suchen Sie nach vertraulichen Informationen</a>. Verwenden Sie die Syntax in Exchange Online PowerShell</p> <pre>@{&lt;SensitiveInformationType1&gt;},@{&lt;SensitiveInformationType2&gt;}</pre> <p>. Um nach Inhalten zu suchen, die mindestens zwei Kreditkarte Zahlen und mindestens eine ABA routing Zahl enthält, verwenden Sie beispielsweise den Wert</p> <pre>@{Name="Credit Card Number"; minCount="2"},@{Name="ABA Routing Number"; minCount="1"}</pre> <p>.</p>
Size	Wert der einzelnen Größe	<p>Gibt die Größe der Anlage oder die gesamte Nachricht an. In der Exchange-Verwaltungskonsole können Sie nur die Größe in Kilobyte (KB) angeben. In Exchange Online PowerShell Wenn Sie einen Wert eingeben, qualifizieren Sie ihn mit einem der folgenden Einheiten:</p> <ul style="list-style-type: none"> <li>• B (Bytes)</li> <li>• KB (KB)</li> <li>• MB (MB)</li> <li>• GB (GB)</li> </ul> <p>Beispielsweise 20MB . Nicht qualifizierte Werte werden in der Regel als Bytes behandelt, aber möglicherweise kleine Werte bis zu der nächste KB gerundet.</p>
SupervisionList	Einzelwert von <b>Zulassen</b> oder <b>Blockieren</b>	Aufsichtsrichtlinien waren ein Feature in Live@edu, mit dem Sie steuern konnten, wer E-Mails an Benutzer in Ihrer Organisation senden und von diesen empfangen konnte (z. B. die Richtlinie für geschlossenen Campus und die Antimobbing-Richtlinie). In Office 365 können Sie keine Aufsichtslisteneinträge für Postfächer konfigurieren.
UserScopeFrom	Einzelner Wert, der <b>innerhalb der Organisation</b> ( <code>InOrganization</code> ) oder <b>außerhalb der Organisation</b> ( <code>NotInOrganization</code> )	<p>Ein Absender wird als innerhalb der Organisation befindlich angesehen, wenn eine der folgenden Bedingungen erfüllt ist: Bei dem Absender handelt es sich um ein Postfach, einen E-Mail-Benutzer, eine Gruppe oder einen E-Mail-aktivierten öffentlichen Ordner, der innerhalb von Active Directory der Organisation vorhanden ist. Die E-Mail-Adresse des Absenders befindet sich in einer akzeptierten Domäne, die als autorisierende Domäne oder interne Relaydomäne konfiguriert ist, <b>und</b> die Nachricht wurde über eine authentifizierte Verbindung gesendet oder empfangen. Weitere Informationen zu akzeptierten Domänen finden Sie unter <a href="#">Accepted Domains</a>. Ein Absender wird als außerhalb der Organisation befindlich angesehen, wenn eine der folgenden Bedingungen erfüllt ist: Die E-Mail-Adresse des Absenders befindet sich nicht in einer akzeptierten Domäne. Die E-Mail-Adresse des Absenders befindet sich in einer akzeptierten Domäne, die als externe Relaydomäne konfiguriert ist. &gt; [!NOTE]&gt; Um zu ermitteln, ob E-Mail-Kontakte als innerhalb oder außerhalb der Organisation befindlich angesehen werden, wird die Absenderadresse mit den akzeptierten Domänen der Organisation verglichen.</p>

EIGENSCHAFTENTYP	GÜLTIGE WERTE	BESCHREIBUNG
UserScopeTo	Einer der folgenden Werte: <b>innerhalb der Organisation</b> ( <code>InOrganization</code> ) <b>außerhalb der Organisation</b> ( <code>NotInOrganization</code> )	Ein Empfänger wird als innerhalb der Organisation befindlich angesehen, wenn eine der folgenden Bedingungen erfüllt ist: Bei dem Empfänger handelt es sich um ein Postfach, einen E-Mail-Benutzer, eine Gruppe oder einen E-Mail-aktivierten öffentlichen Ordner, der innerhalb von Active Directory der Organisation vorhanden ist. Die E-Mail-Adresse des Empfängers befindet sich in einer akzeptierten Domäne, die als autorisierende Domäne oder interne Relaydomäne konfiguriert ist, <b>und</b> die Nachricht wurde über eine authentifizierte Verbindung gesendet oder empfangen. Ein Empfänger wird als außerhalb der Organisation befindlich angesehen, wenn eine der folgenden Bedingungen erfüllt ist: Die E-Mail-Adresse des Empfängers befindet sich nicht in einer akzeptierten Domäne. Die E-Mail-Adresse des Empfängers befindet sich in einer akzeptierten Domäne, die als externe Relaydomäne konfiguriert ist.
Words	Array aus Zeichenfolgen	Gibt ein oder mehrere zu suchende Wörter an. Die Groß-/Kleinschreibung wird nicht berücksichtigt, und der Text kann von Leerzeichen und Satzzeichen umgeben sein. Platzhalter und teilweise Übereinstimmungen werden nicht unterstützt. Beispiel: "contoso" stimmt mit " Contoso." überein. Wenn der Text jedoch von anderen Zeichen umgeben ist, wird dies nicht als Übereinstimmung betrachtet. "Contoso" entspricht beispielsweise nicht den folgenden Werten: Acontoso Contosoa Acontosob Das Sternchen (*) wird als literales Zeichen betrachtet und nicht als Platzhalter verwendet.

[Zurück zum Seitenanfang](#)

## Weitere Informationen

[Nachrichtenflussregeln \(Transportregeln\) in Exchange Online](#)

[Aktionen für Nachrichtenflussregeln in Exchange Online](#)

[E-Mail-Fluss Regel Verfahren im Exchange Online](#)

[Transportregelbedingungen \(Prädikate\) für Exchange Server](#)

[Transport Rule Conditions \(Predicates\) für Exchange Online Protection](#)

[New-TransportRule](#)

# Aktionen für Nachrichtenflussregeln in Exchange Online

18.12.2018 • 32 minutes to read

Aktionen in Nachrichtenflussregeln (auch als Transportregeln bekannt) geben an, was mit Nachrichten geschehen soll, die den Bedingungen der Regel entsprechen. Sie können beispielsweise eine Regel erstellen, die eine Nachricht eines bestimmten Absenders an einen Moderator weiterleitet oder allen ausgehenden Nachrichten einen Haftungsausschluss oder eine personalisierte Signatur hinzufügt.

Aktionen erfordern normalerweise zusätzliche Eigenschaften. Wenn durch die Regel beispielsweise eine Nachricht umgeleitet werden soll, müssen Sie angeben, wohin die Nachricht geleitet werden soll. Einige Aktionen weisen mehrere Eigenschaften auf, die verfügbar oder erforderlich sind. Wenn durch die Regel beispielsweise dem Nachrichtenkopf ein Kopfzeilenfeld hinzugefügt werden soll, müssen Sie den Namen und den Wert der Kopfzeile angeben. Wenn durch die Regel Nachrichten ein Haftungsausschluss hinzufügt werden soll, müssen Sie den Text für den Haftungsausschluss angeben. Darüber hinaus können Sie festlegen, wo der Text eingefügt werden soll und was passieren soll, wenn der Haftungsausschluss der Nachricht nicht hinzugefügt werden kann. Normalerweise können Sie in einer Regel mehrere Aktionen konfigurieren, einige Aktionen sind jedoch ausgeschlossen. Eine Regel kann z. B. nicht gleiche Nachricht gleichzeitig ablehnen und umleiten.

Weitere Informationen zu e-Mail-Flussregeln in Exchange Online finden Sie unter [E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#).

Weitere Informationen zu Bedingungen und Ausnahmen in Nachrichtenflussregeln finden Sie unter [Mail flow rule conditions and exceptions \(predicates\) in Exchange Online](#).

Weitere Informationen zu Aktionen in e-Mail-Flussregeln in der Exchange Online Protection oder Exchange-Server finden Sie unter [Mail Flow Regelaktionen in Exchange Online Protection](#) oder [e-Mail-Flussregeln \(Transportregeln\)](#).

## Aktionen für Nachrichtenflussregeln in Exchange Online

Die Aktionen, die in Nachrichtenflussregeln in Exchange Online verfügbar sind, werden in der folgenden Tabelle beschrieben. Gültige Werte für die einzelnen Eigenschaften werden im Abschnitt [Eigenschaftswerte](#) erläutert.

### Hinweise:

- Nach dem Auswählen einer Aktion in der Exchange-Verwaltungskonsole (EAC) unterscheidet sich der Wert, der letztendlich im Feld **Gehen Sie wie folgt vor** angezeigt wird, häufig vom ausgewählten Klickpfad. Wenn Sie zudem neue Regeln erstellen, können Sie manchmal (je nach vorgenommener Auswahl) einen kurzen Aktionsnamen aus einer Vorlage (eine gefilterte Liste von Aktionen) wählen anstatt dem vollständigen Klickpfad zu folgen. Die kurzen Namen und vollständigen Klickpfadwerte werden in der Spalte „EAC“ in der Tabelle angezeigt.
- Darüber hinaus unterscheiden sich die Namen einiger der Aktionen, die vom Cmdlet **Get-TransportRuleAction** zurückgegeben werden, von den entsprechenden Parameternamen. Für eine Aktion sind möglicherweise mehrere Parameter erforderlich.

ACTION IN DER EXCHANGE-VERWALTUNGSKONSOLE	AKTIONSPARAMETER IN POWERSHELL	EIGENSCHAFT	BESCHREIBUNG
<p><b>Nachricht zur Genehmigung weiterleiten an... diese Personen</b></p> <p><b>Weiterleiten der Nachricht zur Genehmigung &gt; an diese Personen</b></p>	<code>ModerateMessageByUser</code>	<code>Addresses</code>	<p>Leitet die Nachricht als Anlage, die in eine Genehmigungsanforderung eingeschlossen ist, an die angegebenen Moderatoren weiter. Weitere Informationen finden Sie unter <a href="#">Gängige Szenarien der Nachrichtengenehmigung</a>. Eine Verteilergruppe kann nicht als Moderator verwendet werden.</p>
<p><b>Nachricht zur Genehmigung weiterleiten an ... den Vorgesetzten des Absenders</b></p> <p><b>Nachricht zur Genehmigung weiterleiten an &gt; den Vorgesetzten des Absenders</b></p>	<code>ModerateMessageByManager</code>	N/V	<p>Nachricht zur Genehmigung weiterleiten an den Vorgesetzten des Absenders. Diese Aktion funktioniert nur, wenn das <b>Manager</b> - Attribut des Absenders definiert ist. Andernfalls wird die Nachricht ohne Moderation an die Empfänger übermittelt.</p>
<p><b>Die Nachricht umleiten an...diese Empfänger</b></p> <p><b>Die Nachricht umleiten an &gt; diese Empfänger</b></p>	<code>RedirectMessageTo</code>	<code>Addresses</code>	<p>Leitet die Nachricht an die angegebene Empfänger um. Die Nachricht wird nicht an die Originalempfänger übermittelt, und der Absender und die Originalempfänger werden nicht benachrichtigt.</p>
<p><b>Nachricht in gehostete Quarantäne stellen</b></p> <p><b>Die Nachricht umleiten an &gt; Gehostete Quarantäne</b></p>	<code>Quarantine</code>	N/V	<p>Übermittelt die Nachricht an das gehostete Quarantänepostfach. Weitere Informationen zum gehosteten Quarantänepostfach in Office 365 finden Sie unter <a href="#">Quarantine</a>.</p>
<p><b>Folgenden Connector verwenden</b></p> <p><b>Die Nachricht umleiten an &gt; Der folgende Connector</b></p>	<code>RouteMessageOutboundConnector</code>	<code>OutboundConnector</code>	<p>Verwendet den angegebenen ausgehenden Connector zum Übermitteln der Nachricht. Weitere Informationen zu Connectors finden Sie unter <a href="#">Configure mail flow using connectors in Office 365</a>.</p>

ACTION IN DER EXCHANGE-VERWALTUNGSKONSOLE	AKTIONSPARAMETER IN POWERSHELL	EIGENSCHAFT	BESCHREIBUNG
<b>Nachricht mit Erklärung ablehnen</b>  <b>Nachricht blockieren &gt; Nachricht ablehnen und Erläuterung einfügen</b>	<i>RejectMessageReasonText</i>	String	<p>Gibt die Nachricht in einem Unzustellbarkeitsbericht (auch als NDR bekannt) mit dem angegebenen Text als Ablehnungsgrund an den Absender zurück. Der Empfänger empfängt weder die Originalnachricht noch eine Benachrichtigung. Der Standardwert ist erweitertem Statuscode, der verwendet wird <b>5.7.1</b>. Wenn Sie erstellen oder ändern die Regel in PowerShell, können Sie den DSN-Code mit dem Parameter <i>RejectMessageEnhancedStatusCode</i> angeben.</p>
<b>Nachricht ablehnen mit erweitertem Statuscode</b>  <b>Nachricht blockieren &gt; Nachricht ablehnen mit erweitertem Statuscode</b>	<i>RejectMessageEnhancedStatusCode</i>	DSNEnhancedStatusCode	<p>Gibt die Nachricht in einem Unzustellbarkeitsbericht mit dem angegebenen erweiterten Delivery Status Notification (DSN)-Code an den Absender zurück. Der Empfänger empfängt weder die Originalnachricht noch eine Benachrichtigung. Gültige DSN-Codes sind <b>5.7.1</b> oder <b>5.7.900</b> über <b>5.7.999</b>. Der Grund Standardtext, der verwendet wird, ist <b>Delivery not authorized, message refused</b>.</p> <p>Wenn Sie erstellen oder ändern die Regel in PowerShell, können Sie die Ablehnung Grundtext mit dem Parameter <i>RejectMessageReasonText</i> angeben.</p>
<b>Löschen der Nachricht ohne Benachrichtigung</b>  <b>Nachricht blockieren &gt; Nachricht ohne Benachrichtigung löschen</b>	<i>DeleteMessage</i>	N/V	Ignoriert die E-Mail-Nachricht, ohne eine Benachrichtigung an Empfänger oder Absender zu senden.

ACTION IN DER EXCHANGE-VERWALTUNGSKONSOLE	AKTIONSPARAMETER IN POWERSHELL	EIGENSCHAFT	BESCHREIBUNG
<b>BCC-Empfänger hinzufügen</b>  <b>Empfänger hinzufügen &gt; zu Bcc-Feld</b>	<i>BlindCopyTo</i>	<code>Addressses</code>	Fügt einen oder mehrere Empfänger zum Feld <b>Bcc</b> der Nachricht hinzu. Die Originalempfänger werden nicht benachrichtigt und können die zusätzlichen Adressen nicht sehen.
<b>AN-Empfänger hinzufügen</b>  <b>Empfänger hinzufügen &gt; zu An-Feld</b>	<i>AddToRecipients</i>	<code>Addressses</code>	Fügt einen oder mehrere Empfänger zum Feld <b>To</b> der Nachricht hinzu. Die Originalempfänger können die zusätzlichen Adressen sehen.
<b>CC-Empfänger hinzufügen</b>  <b>Empfänger hinzufügen &gt; zu Cc-Feld</b>	<i>CopyTo</i>	<code>Addressses</code>	Fügt einen oder mehrere Empfänger zum Feld <b>Cc</b> der Nachricht hinzu. Die Originalempfänger können die zusätzliche Adresse sehen.
<b>Vorgesetzten des Absenders als Empfänger hinzufügen</b>  <b>Empfänger hinzufügen &gt; Vorgesetzten des Absenders als Empfänger hinzufügen</b>	<i>AddManagerAsRecipientType</i>	<code>AddedManagerAction</code>	Fügt den Vorgesetzten des Absenders als angegebenen Empfängertyp der Nachricht hinzu ( <b>To</b> , <b>Cc</b> , <b>Bcc</b> ) oder leitet die Nachricht an den Vorgesetzten des Absenders ohne Benachrichtigung des Absenders oder des Empfängers um. Diese Aktion funktioniert nur, wenn das <b>Manager</b> - Attribut des Absenders in Active Directory definiert ist.
<b>Haftungsausschluss anfügen</b>  <b>Haftungsausschluss auf die Nachricht anwenden &gt; Haftungsausschluss anfügen</b>	<i>ApplyHtmlDisclaimerText</i> <i>ApplyHtmlDisclaimerFallbackAction</i> <i>ApplyHtmlDisclaimerLocation</i>	Erste Eigenschaft: <code>DisclaimerText</code> Zweite Eigenschaft: <code>DisclaimerFallbackAction</code> Dritte-Eigenschaft (nur PowerShell): <code>DisclaimerTextLocation</code>	Fügt den angegebenen HTML-Haftungsausschluss am Ende der Nachricht ein. Wenn Sie erstellen oder ändern die Regel in PowerShell, verwenden Sie den Parameter <i>ApplyHtmlDisclaimerLocation</i> mit dem Wert <code>Append</code> .
<b>Dem Haftungsausschluss voranstellen</b>  <b>Haftungsausschluss auf die Nachricht anwenden &gt; Haftungsausschluss voranstellen</b>	<i>ApplyHtmlDisclaimerText</i> <i>ApplyHtmlDisclaimerFallbackAction</i> <i>ApplyHtmlDisclaimerLocation</i>	Erste Eigenschaft: <code>DisclaimerText</code> Zweite Eigenschaft: <code>DisclaimerFallbackAction</code> Dritte-Eigenschaft (nur PowerShell): <code>DisclaimerTextLocation</code>	Fügt den angegebenen HTML-Haftungsausschluss am Anfang der Nachricht ein. Wenn Sie erstellen oder ändern die Regel in PowerShell, verwenden Sie den Parameter <i>ApplyHtmlDisclaimerLocation</i> mit dem Wert <code>Prepend</code> .

ACTION IN DER EXCHANGE-VERWALTUNGSKONSOLE	AKTIONSPARAMETER IN POWERSHELL	EIGENSCHAFT	BESCHREIBUNG
<b>Diese Kopfzeile entfernen</b>  <b>Nachrichteneigenschaften ändern &gt; Nachrichtenkopfzeile entfernen</b>	<code>RemoveHeader</code>	<code>MessageHeaderField</code>	Entfernt das angegebene Feld für die Nachrichtenkopfzeilen.
<b>Nachrichtenkopf auf diesen Wert festlegen</b>  <b>Nachrichteneigenschaften ändern &gt; Nachrichtenkopfzeile festlegen</b>	<code>SetHeaderName</code> <code>SetHeaderValue</code>	Erste Eigenschaft: <code>MessageHeaderField</code> Zweite Eigenschaft: <code>String</code>	Ändert oder fügt das angegebene Kopfzeilenfeld im Nachrichtenkopf hinzu und legt das für das Kopfzeilenfeld den angegebenen Wert fest.
<b>Nachrichtenklassifikation anwenden</b>  <b>Nachrichteneigenschaften ändern &gt; Nachrichtenklassifikation anwenden</b>	<code>ApplyClassification</code>	<code>MessageClassification</code>	Wendet die angegebene Nachrichtenklassifikation auf die Nachricht an.
<b>SCL-Bewertung (Spam Confidence Level) festlegen</b>  <b>Nachrichteneigenschaften ändern &gt; SCL-Bewertung (Spam Confidence Level) festlegen</b>	<code>SetSCL</code>	<code>SCLValue</code>	Legt die SCL-Bewertung (Spam Confidence Level) einer Nachricht auf den angegebenen Wert fest.
<b>Office 365 Message Encryption und Rechte Dokumentschutz angewendet</b>  <b>Die Nachricht mit Office 365 Message Encryption und Rechte Schutz zuweisen</b>  <b>Ändern der nachrichtensicherheit &gt; Office 365-Nachrichtenverschlüsselung anwenden und Rechteschutz</b>	<code>ApplyRightsProtectionTemplate</code>	<code>RMSTemplate</code>	Wendet die angegebene Vorlage Azure-Rechteverwaltung (RMS Azure) auf die Nachricht an. Azure RMS ist Teil der Azure Information Protection. Weitere Informationen finden Sie unter <a href="#">Einrichten von neuen Funktionen von Office 365 Message Encryption</a> .
<b>TLS-Verschlüsselung erforderlich</b>  <b>Nachrichtensicherheit ändern &gt; TLS-Verschlüsselung erforderlich</b>	<code>RouteMessageOutboundRequireTls</code>	n/v	Erzwingt eine Weiterleitung der ausgehenden Nachrichten über eine TLS-verschlüsselte Verbindung.

ACTION IN DER EXCHANGE-VERWALTUNGSKONSOLE	AKTIONSPARAMETER IN POWERSHELL	EIGENSCHAFT	BESCHREIBUNG
<p><b>Verschlüsseln Sie mit der vorherigen Version von OME-Nachrichten</b></p> <p><b>Ändern der nachrichtensicherheit &gt; Office gelten die vorherige Version des OME</b></p>	<i>ApplyOME</i>	n/v	<p>Wenn Sie Office 365-Organisation zu Office 365 Message Encryption (OME) verschoben noch nicht, die auf Azure Information Protection erstellt wird, werden diese Aktion die Nachricht und die Anlagen mit der vorherigen Version von OME verschlüsselt.</p> <p><b>Hinweise:</b></p> <ul style="list-style-type: none"> <li>• Es empfiehlt sich, dass Sie einen Plan für die OME auf Azure Information Protection ans, wie es für Ihre Organisation angemessen ist herstellen. Anweisungen finden Sie unter <a href="#">Einrichten von neuen Funktionen von Office 365 Message Encryption</a>.</li> <li>• Wenn Sie erhalten eine Fehlermeldung, die diesem IRM-Lizenziierung nicht aktiviert, die frühere Version von OME kann nicht eingerichtet werden. Wenn Sie nun OME einrichten, benötigen Sie die OME-Funktionen einrichten, die auf Azure Information Protection integriert sind.</li> </ul>
<p><b>Entfernen Sie die vorherige Version des OME aus der Nachricht</b></p> <p><b>Ändern der nachrichtensicherheit &gt; Entfernen Sie die vorherige Version des OME</b></p>	<i>RemoveOME</i>	n/v	<p>Die Nachricht und Anlagen aus der vorherigen Version von OME entschlüsselt werden, damit Benutzer nicht zur Anmeldung bei des Verschlüsselung-Portals, um diese anzeigen müssen. Diese Aktion ist nur verfügbar für Nachrichten, die in Ihrer Organisation gesendet werden.</p>
<p><b>Entfernen Sie den Schutz für Office 365 Message Encryption und Rechte</b></p> <p><b>Ändern der nachrichtensicherheit &gt; Office 365-Nachrichtenverschlüsselung entfernen und Rechteschutz</b></p>	<i>RemoveOMEv2</i>	n/v	<p>Entfernen Sie die Azure RMS-Vorlage aus der Nachricht.</p>

AKTION IN DER EXCHANGE-VERWALTUNGSKONSOLE	AKTIONSPARAMETER IN POWERSHELL	EIGENSCHAFT	BESCHREIBUNG
<b>Dem Betreff der Nachricht Folgendes voranstellen</b>	<i>PrependSubject</i>	String	<p>Fügt den angegebenen Text am Anfang des Felds <b>Subject</b> der Nachricht ein.</p> <p>Verwenden Sie ein Leerzeichen oder einen Doppelpunkt (:) als letztes Zeichen des angegebenen Texts, um ihn vom ursprünglichen Betrefftext zu unterscheiden.</p> <p>Um zu verhindern, dass Sie dieselbe Zeichenfolge hinzugefügte Nachrichten, die den Text im Betreff (beispielsweise Antworten) bereits enthalten, fügen Sie die <b>der Betreff enthält</b> (<i>ExceptIfSubjectContainsWords</i>) Ausnahme zur Regel hinzu.</p>

ACTION IN DER EXCHANGE-VERWALTUNGSKONSOLE	AKTIONSPARAMETER IN POWERSHELL	EIGENSCHAFT	BESCHREIBUNG
<b>Absender mit Richtlinientipp benachrichtigen</b>	<i>NotifySender</i> <i>RejectMessageReasonText</i> <i>RejectMessageEnhancedStatusCode</i> (nur PowerShell)	Erste Eigenschaft: <code>NotifySenderType</code> Zweite Eigenschaft: <code>String</code> Dritte-Eigenschaft (nur PowerShell): <code>DSNEnhancedStatusCode</code>	Benachrichtigt den Absender oder blockiert die Nachricht, wenn die Nachricht einer DLP-Richtlinie entspricht. Wenn Sie diese Aktion verwenden, müssen Sie mithilfe der <b>Nachricht enthält vertrauliche Informationen</b> ( <i>MessageContainsDataClassification</i> -Bedingung). Wenn Sie erstellen oder ändern die Regel in PowerShell, ist der Parameter <i>RejectMessageReasonText</i> optional. Wenn Sie diesen Parameter, den Standardtext nicht verwenden <code>Delivery not authorized, message refused</code>
<b>Schadensbericht generieren und senden an</b>	<i>GenerateIncidentReport</i> <i>IncidentReportContent</i>	Erste Eigenschaft: <code>Addresses</code> Zweite Eigenschaft: <code>IncidentReportContent</code>	Sendet einen Schadensbericht, der den angegebenen Inhalt an die angegebenen Empfänger enthält. Ein Schadensbericht wird für Nachrichten generiert, die den Data Loss Prevention (DLP)-Richtlinien in Ihrer Organisation entsprechen.

ACTION IN DER EXCHANGE-VERWALTUNGSKONSOLE	AKTIONSPARAMETER IN POWERSHELL	EIGENSCHAFT	BESCHREIBUNG
<b>Empfänger durch Nachricht benachrichtigen</b>	<code>GenerateNotification</code>	<code>NotificationMessageText</code>	Gibt den Text, HTML-Tags und Nachrichtenschlüsselwörter an, die in der Benachrichtigungs-E-Mail einbezogen werden sollen, die an die Empfänger der Nachricht gesendet wird. Sie können beispielsweise Empfänger benachrichtigen, dass die Nachricht von der Regel abgelehnt oder als Spam markiert und Ihrem Junk-E-Mail-Ordner zugestellt wurde.
Abschnitt <b>Eigenschaften dieser Regel</b> > Überwachen Sie diese Regel mit Schweregrad	<code>SetAuditSeverity</code>	<code>AuditSeverityLevel</code>	Gibt an, ob: die Generierung eines Schadensberichts und des entsprechenden Eintrags im Nachrichtenverfolgungsprotokoll verhindert werden soll. ein Schadensbericht und der entsprechende Eintrag im Nachrichtenverfolgungsprotokoll mit dem angegebenen Schweregrad (niedrig, mittel oder hoch) generiert werden soll.
Abschnitt <b>Eigenschaften dieser Regel</b> > Verarbeiten weiterer Regeln beenden  Weitere Optionen > Abschnitt <b>Eigenschaften dieser Regel</b> > Verarbeiten weiterer Regeln beenden	<code>StopRuleProcessing</code>	N/V	Gibt an, dass die Nachricht nach dem Anwenden der Regel nicht mehr von anderen Regeln verarbeitet werden kann.

## Eigenschaftswerte

Die Eigenschaftswerte, die für die Aktionen in den Nachrichtenflussregeln verwendet werden, sind in der folgenden Tabelle beschrieben.

EIGENSCHAFT	GÜLTIGE WERTE	BESCHREIBUNG
-------------	---------------	--------------

EIGENSCHAFT	GÜLTIGE WERTE	BESCHREIBUNG
AddedManagerAction	<p>Einer der folgenden Werte:</p> <p><b>n</b></p> <p><b>Cc</b></p> <p><b>Bcc</b></p> <p><b>Redirect</b></p>	<p>Gibt an, wie der Vorgesetzte des Absenders in Nachrichten einbezogen werden soll.</p> <p>Bei Auswahl von <b>n</b>, <b>Cc</b> oder <b>Bcc</b> wird der Vorgesetzte des Absenders als Empfänger in das angegebene Feld eingefügt.</p> <p>Bei Auswahl von <b>Umleiten</b> wird die Nachricht nur an den Vorgesetzten des Absenders ohne Benachrichtigung des Absenders oder des Empfängers übermittelt.</p> <p>Diese Aktion funktioniert nur, wenn der <b>Manager</b> des Absenders definiert ist.</p>
Addresses	Exchange Empfänger	Abhängig von der Aktion können Sie möglicherweise ein beliebiges E-Mail-aktiviertes Objekt in der Organisation angeben, oder Sie sind auf einen bestimmten Objekttyp beschränkt. In der Regel können Sie mehrere Empfänger auswählen, Sie können einen Schadensbericht jedoch nur an einen Empfänger senden.
AuditSeverityLevel	<p>Einer der folgenden Werte:</p> <p>Deaktivieren Sie <b>diese Regel mit Schweregrad</b>, oder wählen Sie <b>diese Regel mit Schweregrad</b> mit dem Wert <b>nicht angegeben</b> ( <code>DoNotAudit</code> )</p> <p><b>Niedrig</b></p> <p><b>Mittel</b></p> <p><b>Hoch</b></p>	<p>Die Werte <b>Niedrig</b>, <b>Mittel</b> oder <b>Hoch</b> legen den Schweregrad fest, der dem Schadensbericht und dem entsprechenden Eintrag im Nachrichtenverfolgungsprotokoll zugeordnet wird.</p> <p>Der andere Wert verhindert, dass ein Schadensbericht erstellt und der entsprechende Eintrag in das Nachrichtenverfolgungsprotokoll geschrieben wird.</p>

EIGENSCHAFT	GÜLTIGE WERTE	BESCHREIBUNG
<code>DisclaimerFallbackAction</code>	<p>Einer der folgenden Werte:</p> <p><b>Umbruch</b></p> <p><b>Ignorieren</b></p> <p><b>Ablehnen</b></p>	<p>Gibt an, wie vorzugehen ist, wenn ein Haftungsausschluss nicht auf eine Nachricht angewendet werden kann. Es kann Situationen geben, in denen die Inhalte einer Nachricht nicht verändert werden können, z. B. wenn eine Nachricht verschlüsselt ist. Die verfügbaren Ausweichaktionen sind:</p> <ul style="list-style-type: none"> <li>• <b>Umbrochen</b>: die ursprüngliche Nachricht wird in einem neuen Nachrichtenumschlag eingebunden und der Text des Haftungsausschlusses in die neue Nachricht eingefügt wird. Dies ist der Standardwert.</li> <li>• <b>Ignore</b>: die Regel wird ignoriert, und die Nachricht wird ohne Haftungsausschluss zugestellt.</li> <li>• <b>Ablehnen</b>: die Nachricht wird an den Absender eines Unzustellbarkeitsberichts zurückgegeben.</li> </ul> <p><b>Hinweise:</b> Alle nachfolgenden Nachrichtenflussregeln werden auf den neuen Nachrichtenumschlag angewendet, nicht auf die ursprüngliche Nachricht. Konfigurieren Sie diese Regeln daher mit einer niedrigeren Priorität als die anderen Regeln. Wenn die ursprüngliche Nachricht nicht in einen neuen Nachrichtenumschlag umgebrochen werden kann, wird die ursprüngliche Nachricht nicht übermittelt. Die Nachricht wird mit einem Unzustellbarkeitsbericht an den Absender zurückgesendet.</p>
<code>DisclaimerText</code>	HTML-Zeichenfolge	Gibt den Haftungsausschluss-Text, der HTML-Tags, Inline Cascading Style Stylesheet (CSS)-Tags und Bilder enthalten kann, mithilfe des IMG-Tags an. Die Höchstlänge beträgt 5000 Zeichen einschließlich Tags.
<code>DisclaimerTextLocation</code>	<p>Einzelner Wert: <code>Append</code> oder <code>Prepend</code></p>	<p>In PowerShell verwenden Sie die <code>ApplyHtmlDisclaimerLocation</code>, um den Speicherort der den Text des Haftungsausschlusses in der Nachricht anzugeben:</p> <ul style="list-style-type: none"> <li>• <code>Append</code> : Am Ende des Nachrichtentexts Haftungsausschluss hinzufügen. Dies ist der Standardwert.</li> <li>• <code>Prepend</code> : Haftungsausschluss am Anfang des Nachrichtentexts hinzugefügt.</li> </ul>

EIGENSCHAFT	GÜLTIGE WERTE	BESCHREIBUNG
DSNEnhancedStatusCode	<p>DSN-Code-Einzelwert:</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;">5.7.1</div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">5.7.900 über 5.7.999</div>	<p>Gibt den verwendeten DSN-Code an. Sie können mithilfe des Cmdlet <b>New-SystemMessage</b> benutzerdefinierte DSNs erstellen.</p> <p>Wenn Sie die Ablehnung Grundtext zusammen mit den DSN-Code nicht angeben, ist der Grund Standardtext, der verwendet wird</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;"><i>Delivery not authorized, message refused</i></div> <p>.</p> <p>Wenn Sie erstellen oder ändern die Regel in PowerShell, können Sie die Ablehnung Grundtext mit dem Parameter <i>RejectMessageReasonText</i> angeben.</p>
IncidentReportContent	<p>Einer oder mehrere der folgenden Werte:</p> <p><b>Sender</b></p> <p><b>Recipients</b></p> <p><b>Subject</b></p> <p><b>Cc'd Empfänger (Cc)</b></p> <p><b>Bcc'd Empfänger (Bcc)</b></p> <p><b>Severity</b></p> <p><b>Absender Informationen überschrieben. (Override)</b></p> <p><b>Vergleich von Regeln (RuleDetections)</b></p> <p><b>Falsch positive Berichte (FalsePositive)</b></p> <p><b>Datenklassifikationen erkannt (DataClassifications)</b></p> <p><b>Inhalt (IdMatch)</b></p> <p><b>Ursprüngliche e-Mail (AttachOriginalMail)</b></p>	<p>Legt fest, dass die Liste der Eigenschaften der ursprünglichen Nachricht in den Schadensbericht aufgenommen werden soll. Sie können eine beliebige Kombination dieser Eigenschaften wählen. Zusätzlich zu den von Ihnen angegebenen Eigenschaften ist die Nachrichten-ID immer im Schadensbericht enthalten. Die verfügbaren Eigenschaften sind:</p> <p><b>Absender:</b> der Absender der ursprünglichen Nachricht.</p> <p><b>Empfänger, Cc'd Empfänger und Bcc</b></p> <p><b>' Empfänger d:</b> alle Empfänger der Nachricht oder nur die Empfänger in den Feldern <b>Cc</b> und <b>Bcc</b>. Für jede Eigenschaft sind nur die ersten 10 Empfänger im schadensbericht enthalten.</p> <p><b>Betreff:</b> das Feld <b>Betreff</b> der ursprünglichen Nachricht.</p> <p><b>Schweregrad:</b> der überwachungsschweregrad der Regel, die ausgelöst wurde. Nachricht Nachverfolgungsprotokolle umfassen alle Audit Schweregrade und können vom überwachungsschweregrad gefiltert werden. In der Exchange-Verwaltungskonsole, wenn Sie das Kontrollkästchen <b>diese Regel mit Schwergrad</b> deaktivieren (in PowerShell, der Wert des Parameters <i>SetAuditSeverity DoNotAudit</i>), regelübereinstimmungen in den regelberichten nicht angezeigt. Wenn eine Nachricht von mehr als eine Regel verarbeitet wird, ist der höchste Schweregrad in Vorfall Berichte enthalten.</p> <p><b>Absender außer Kraft setzen</b></p> <p><b>Informationen:</b> die Überschreibung, wenn der Absender hat den Richtlinientipp außer Kraft setzen. Wenn der Absender eine Begründung bereitgestellt werden, sind die ersten</p>

EIGENSCHAFT	GÜLTIGE WERTE	100 Zeichen des Begründung ebenfalls <b>BESCHREIBUNG</b> enthalten.
		<p><b>Übereinstimmungsregeln:</b> die Liste der Regeln, die die Nachricht ausgelöst.</p> <p><b>Falsch positive Berichte:</b> das falsch positive Ergebnis, wenn der Absender die Nachricht als falsch positives Ergebnis für einen Richtlinientipp gekennzeichnet hat.</p> <p><b>Klassifikationen in der Daten erkannt:</b> die Liste der Typen vertraulicher Informationen in der Nachricht erkannt.</p> <p><b>Inhalt:</b> des erkannten Typs vertraulicher Informationen, den exakten übereinstimmenden Inhalt aus der Nachricht sowie die 150 Zeichen vor und nach den übereinstimmenden vertraulichen Informationen.</p> <p><b>Ursprüngliche e-Mail:</b> die gesamte Nachricht, die die Regel ausgelöst wird, die schadensbericht zugeordnet ist. In PowerShell können Sie mehrere Werte durch Kommata getrennt angeben.</p>
<code>MessageClassification</code>	Einzelnes Nachrichtenklassifikationsobjekt	<p>Wählen Sie in der Exchange-Verwaltungskonsole aus der Liste der Nachrichtenklassifikationen aus, die Sie erstellt haben.</p> <p>Verwenden Sie in PowerShell das Cmdlet <b>Get-MessageClassification</b>, um die verfügbaren Objekte für die Nachrichtenklassifikation anzuzeigen.</p>
<code>MessageHeaderField</code>	Einzelne Zeichenfolge	<p>Gibt das SMTP-Kopfzeilenfeld der Nachricht zum Hinzufügen, Entfernen oder Ändern an.</p> <p>Die Nachrichtenkopfzeile ist eine Sammlung erforderlicher und optionaler Kopffelder in der Nachricht. Beispiele für Kopfzeilenfelder sind <b>To</b>, <b>From</b>, <b>Received</b> und <b>Content-Type</b>. Offizielle Kopfzeilenfelder sind in RFC 5322 definiert. Inoffizielle Kopfzeilenfelder beginnen mit <b>X-</b> und werden als X-Header bezeichnet.</p>
<code>NotificationMessageText</code>	Eine beliebige Kombination aus Nur-Text, HTML-Tags und Schlüsselwörtern	<p>Gibt den Text an, der in einer Empfänger-Benachrichtigung verwendet werden soll.</p> <p>Zusätzlich zu Nur-Text und HTML-Tags können Sie die folgenden Schlüsselwörter angeben, die Werte aus der ursprünglichen Nachricht verwenden:</p> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> %%From%% </div> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> %%To%% </div> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> %%Cc%% </div> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> %%Subject%% </div> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> %%Headers%% </div> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> %%MessageDate%% </div>

EIGENSCHAFT	GÜLTIGE WERTE	BESCHREIBUNG
NotifySenderType	<p>Einer der folgenden Werte:</p> <p><b>So senden Sie können jedoch den Absender benachrichtigen (</b>  <b>NotifyOnly )</b></p> <p><b>Die Nachricht blockieren (</b>  <b>RejectMessage )</b></p> <p><b>Die Nachricht blockieren, es sei denn, es falsch positives Ergebnis ist (</b>  <b>RejectUnlessFalsePositiveOverride )</b></p> <p><b>Die Nachricht blockieren, aber Außerkraftsetzen und senden den Absender zulassen (</b>  <b>RejectUnlessSilentOverride )</b></p> <p><b>Die Nachricht blockieren, aber die Absender mit als Rechtfertigung Außerkraftsetzen und senden zuzulassen (</b>  <b>RejectUnlessExplicitOverride )</b></p>	<p>Gibt den Typ des Richtlinientipps an, den der Absender erhält, wenn die Nachricht eine DLP-Richtlinie verletzt. Die Einstellungen werden in der folgenden Liste beschrieben:</p> <p><b>So senden Sie können jedoch den Absender benachrichtigen:</b> der Absender wird benachrichtigt, die Nachricht wird jedoch normal zugestellt.</p> <p><b>Die Nachricht blockieren:</b> die Nachricht wird zurückgewiesen, und der Absender wird benachrichtigt.</p> <p><b>Die Nachricht blockieren, es sei denn, es falsch positives Ergebnis ist:</b> die Nachricht wird zurückgewiesen, wenn es vom Absender als falsch positiv gekennzeichnet ist.</p> <p><b>Die Nachricht blockieren, aber die Absender Außerkraftsetzen und senden zuzulassen:</b> die Nachricht wird zurückgewiesen, sofern der Absender ausgewählt hat, die richtlinieneinschränkung außer Kraft gesetzt.</p> <p><b>Die Nachricht blockieren, aber die Absender mit als Rechtfertigung Außerkraftsetzen und senden zuzulassen:</b> Dies ist ähnlich wie <b>die Nachricht blockieren, aber die Absender Außerkraftsetzen und senden zuzulassen</b>, aber der Absender auch eine Begründung für das Außerkraftsetzen der Richtlinie Einschränkung.</p> <p>Wenn Sie diese Aktion verwenden, müssen Sie die Bedingung (<i>MessageContainsDataClassification</i>) <b>die Nachricht enthält vertrauliche Informationen</b> verwenden.</p>
outboundConnector	Einzelner ausgehender Connector	<p>Gibt die Identität des ausgehenden Connectors an, der zum Übermitteln von Nachrichten verwendet wird. Weitere Informationen zu Connectors finden Sie unter <a href="#">Configure mail flow using connectors in Office 365</a>.</p> <p>Im EAC wählen Sie den Connector in einer Liste aus.</p> <p>In PowerShell verwenden Sie das Cmdlet <b>Get-OutboundConnector</b>, um die verfügbaren Connectors anzuzeigen.</p>

EIGENSCHAFT	GÜLTIGE WERTE	BESCHREIBUNG
<code>RMSTemplate</code>	Einzelne Azure RMS Template-Objekt	<p>Gibt die Azure Rights Management (Azure RMS)-Vorlage, die auf die Nachricht angewendet wird.</p> <p>In der Exchange-Verwaltungskonsole wählen Sie die RMS-Vorlage aus einer Liste aus.</p> <p>In PowerShell verwenden Sie das Cmdlet <b>Get-RMSTemplate</b>, um die verfügbaren RMS-Vorlagen anzuzeigen.</p> <p>Weitere Informationen zu RMS in Office 365 finden Sie unter <a href="#">Was ist Azure Information Protection?</a>.</p>
<code>SCLValue</code>	Einer der folgenden Werte: <b>Umgehung Spamfilterung</b> ( -1 ) Ganze Zahlen 0 bis 9	<p>Gibt den Schwellenwert der SCL-Bewertung (Spam Confidence Level) an, der der Nachricht zugewiesen ist. Ein höherer SCL-Wert gibt an, dass eine Nachricht mit größerer Wahrscheinlichkeit Spam ist.</p>
<code>String</code>	Einzelne Zeichenfolge	<p>Gibt den Text an, der auf das angegebene Nachrichtenkopffeld, den Unzustellbarkeitsbericht oder den Ereignisprotokolleintrag angewendet wird.</p> <p>In PowerShell schließen Sie Werte, die Leerzeichen enthalten, in Anführungszeichen ("") ein.</p>

## Weitere Informationen

[Nachrichtenflussregeln \(Transportregeln\) in Exchange Online](#)

[Nachrichtenflussregel-Bedingungen und -Ausnahmen \(Prädikate\) in Exchange Online](#)

[Verwalten von Nachrichtenflussregeln](#)

[Transport Rule Actions für Exchange Server](#)

[Transport Rule Actions für Exchange Online Protection](#)

[Organization-wide message disclaimers, signatures, footers, or headers in Office 365](#)

[Office 365-Nachrichtenverschlüsselung](#)

# Bewährte Methoden für die Konfiguration von Nachrichtenflussregeln

18.12.2018 • 7 minutes to read

Befolgen Sie diese empfohlenen bewährten Methoden für Exchange-Transportregeln, um allgemeine Konfigurationsfehler zu vermeiden. Jede Empfehlung enthält einen Link zum Thema mit einem Beispiel und schrittweisen Anleitungen.

## Testen der Regeln

Um sicherzustellen, dass keine unerwarteten Schritte können durchgeführt werden auf e-Mails von Personen und um sicherzustellen, können Sie Sie eigentlich unbedingt meeting die Business, rechtlichen oder Compliance Absichten der der Regel gründlich zu testen. Es gibt viele Optionen, und Regeln können miteinander interagieren, daher ist es wichtig, Testnachrichten, die Sie erwarten, wird die Regel übereinstimmen, sowohl die Regel wird nicht übereinstimmen, falls Sie versehentlich eine Regel zu allgemein vorgenommen. Alle Optionen für das Testen von Regeln finden Sie unter [Test Mail Flow Regel](#).

## Regelbereich

Stellen Sie sicher, dass die Regel nur auf vorgesehene Nachrichten angewendet wird. Beispiel:

- **Schränken Sie eine Regel auf Nachrichten ein, die entweder an die Organisation oder aus der Organisation gesendet werden.**

Standardmäßig gilt eine neue Regel auf Nachrichten, die gesendet oder Empfangen von Personen in Ihrer Organisation. Wenn Sie die Regel nur eine Möglichkeit anwenden möchten, werden Sie, die in die Bedingungen für die Regel angeben. Ein Beispiel finden Sie unter [Allgemeine Anlage blockierenden Szenarien für die e-Mail-Flussregeln](#).

- **Einschränken einer Regel auf Grundlage der Absender- oder Empfängerdomäne**

Standardmäßig wird eine neue Regel auf Nachrichten angewendet, die von einer beliebigen Domäne gesendet oder empfangen wird. In einigen Fällen möchten Sie ggf. eine Regel auf alle Domänen bis auf eine oder nur auf eine Domäne anwenden. Beispiele finden Sie unter [Create a Domain or User-Based Safe Sender or Blocked Sender List Using Transport Rules](#).

Eine vollständige Liste aller Bedingungen und Ausnahmen, die für Transportregeln verfügbar sind, finden Sie unter:

- [Nachrichtenflussregel-Bedingungen und -Ausnahmen \(Prädikate\) in Exchange Online](#)
- [Transport Rule Conditions \(Exchange Server\)](#)
- [Transport Rule Conditions \(Exchange Online Protection\)](#)

## Fälle, in denen zwei Regeln notwendig sind

Manchmal benötigen Sie zwei Regeln, um eine gewünschte Aktion zu erzielen. Transportregeln werden der Reihe nach verarbeitet, sodass mehrere Regeln auf dieselbe Nachricht angewendet werden können. Wenn z. B. eine Aktion zum Blockieren der Nachricht dient, und eine weitere Aktion wie Kopieren der Nachricht an den Vorgesetzten des Absenders oder Ändern des Betreffs für die Benachrichtigungs-E-Mail angewendet werden soll, benötigen Sie zwei Regeln. Die erste Regel könnte dann das Kopieren der Nachricht an den Vorgesetzten des

Absenders und das Ändern des Betreffs umfassen, und die zweite Regel das Blockieren der Nachricht.

Wenn Sie zwei Regeln wie folgt verwenden, achten Sie darauf, dass die Bedingungen identisch sind. Betrachten Sie Beispiele für Beispiel 3 in [Nachricht Genehmigung Standardszenarien](#), Beispiel 3 in [Anlage blockierenden Standardszenarien für e-Mail-Flussregeln](#) und [organisationsweite Haftungsausschlüsse, Signaturen, Fußzeilen, oder Kopfzeilen](#) aus.

## Führen Sie keine Wiederholung einer Aktion für alle E-Mails in einer Unterhaltung durch.

Eine Unterhaltung kann viele einzelne Nachrichten enthalten, und die Wiederholung der Aktion für jede Nachricht im Thread kann als lästig empfunden werden. Eine Aktion wie beispielsweise das Hinzufügen eines Haftungsausschlusses soll möglicherweise nur auf die erste Nachricht im Thread angewendet werden. Wenn dies der Fall ist, müssen Sie eine Ausnahme für Nachrichten hinzufügen, die den Text des Haftungsausschlusses bereits enthalten. Ein Beispiel finden Sie unter [Organisationsweite Haftungsausschlüsse, Signaturen, Fußzeilen oder Kopfzeilen](#).

## Beenden der Regelverarbeitung

Manchmal ist es sinnvoll, die Verarbeitung einer Regel zu beenden, nachdem eine Regel erfüllt wurde. Wenn Sie z. B. eine Regel zum Blockieren von Nachrichten mit Anlage und eine zum Einfügen eines Haftungsausschlusses in Nachrichten haben, die einem Muster entsprechen, sollten Sie die Verarbeitung der Regel ggf. beenden, nachdem die Nachricht blockiert wurde. Es ist keine weitere Aktion erforderlich.

Aktivieren Sie zum Beenden der Regelverarbeitung innerhalb der Regel das Kontrollkästchen **Verarbeitung weiterer Regeln beenden**.

## Wenn bei einer Regel eine Übereinstimmung mit zahlreichen Schlüsselwörtern oder Mustern notwendig ist, laden Sie diese aus einer Datei.

Möglicherweise möchten Sie z. B. verhindern, dass E-Mails gesendet werden, die bestimmte unzulässige Wörter enthalten. Sie können eine Textdatei mit diesen Wörtern und Ausdrücken erstellen und dann mit Windows PowerShell eine Transportregel erstellen, die Nachrichten mit diesen blockiert.

Die Textdatei kann reguläre Ausdrücke für Muster enthalten. Für diese Ausdrücke wird nicht zwischen Groß- und Kleinschreibung unterschieden. Allgemeine reguläre Ausdrücke umfassen Folgendes:

AUSDRUCK	ÜBEREINSTIMMUNGEN
.	Einen einzelnen Buchstaben
*	Alle zusätzlichen Zeichen
\d	Eine Dezimalzahl
[character_group]	Ein einzelnes Zeichen in character_group.

Ein Beispiel, das zeigt, eine Textdatei mit regulären Ausdrücken und der Exchange-Modul Windows PowerShell-Befehle verwenden, finden Sie unter [Verwenden von e-Mail-Flussregeln zum Weiterleiten von e-Mail-basierte auf eine Liste der Wörter, Ausdrücke oder Muster](#).

Informationen zum Angeben von Mustern mithilfe von regulären Ausdrücken finden Sie unter [Referenz zu regulären Ausdrücken](#).

# Überprüfen von Nachrichtenanlagen mithilfe von Nachrichtenflussregeln in Office 365

18.12.2018 • 17 minutes to read

Sie können e-Mail-Anlagen in Office 365-Organisation überprüfen, durch das Einrichten von e-Mail-Flussregeln (auch als Transportregeln bezeichnet). Exchange Online bietet Mail Flow Regeln, mit denen die Möglichkeit, e-Mail-Anlagen als Teil Ihrer messaging-Sicherheit und Einhaltung behördlicher Vorschriften zu überprüfen. Wenn Sie Anlagen überprüfen, können Sie Aktion klicken Sie dann auf die Nachrichten, die nicht überprüft wurden basierend auf dem Inhalt oder die Merkmale der diese Anlagen nutzen. Es folgen einige Aufgaben im Zusammenhang mit Anlage, die Sie mithilfe von e-Mail-Flussregeln ausführen können:

- Suchen Sie nach Dateien mit Text, der einem von Ihnen festgelegten Muster entspricht, und fügen Sie am Ende der Nachricht eine Verzichtserklärung hinzu.
- Inhalt in Anlagen überprüfen und, wenn er von Ihnen angegebene Stichwörter enthält, die Nachricht vor der Zustellung zur Genehmigung an einen Moderator weiterleiten.
- Nachrichten auf Anlagen überprüfen, die nicht überprüft werden können, und dann das Senden der gesamten Nachricht verhindern.
- Auf Anlagen prüfen, die eine bestimmte Größe überschreiten, und dann den Absender darüber informieren, wenn Sie die Zustellung der Nachricht verhindern möchten.
- Überprüfen Sie, ob die Eigenschaften eines angefügten Office-Dokuments mit den Werten entsprechen, die Sie angeben. Mit dieser Bedingung können Sie die Anforderungen Ihrer e-Mail-Flussregeln und DLP-Richtlinien mit einem Drittanbieter-Klassifizierungssystem, wie SharePoint Server 2013 oder Windows Server 2012 R2 Datei Klassifizierung-Infrastruktur (FCI) integrieren.
- Benachrichtigungen für Benutzer erstellen, falls sie eine Nachricht senden, die mit einer Nachrichtenflussregel übereinstimmt.
- Blockieren Sie alle Nachrichten mit Anlagen. Beispiele finden Sie unter [Common Anlage blockierenden Szenarien für die e-Mail-Flussregeln](#).

## NOTE

Alle diese Bedingungen überprüfen die komprimierten Archivanhänge.

Exchange Online-Administratoren können Mail Flow Regeln erstellen in der Exchange-Verwaltungskonsole (EAC) an **E-Mail-Fluss > Regeln**. Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren ausführen können. Nach dem start eine neue Regel erstellen, können Sie die vollständige Liste der Anlage-bezogene Bedingungen durch Klicken auf **Weitere Optionen** anzeigen > **mindestens eine Anlage** unter **diese Regel anwenden, wenn**. Die Anlage-bezogene Optionen sind in der folgenden Abbildung dargestellt.

new rule

Name:

\*Apply this rule if...

Select one

Select one

The sender...

The recipient...

The subject or body...

**Any attachment...**

Any recipient...

The message...

The sender and the recipient...

The message properties...

A message header...

[Apply to all messages]

Properties or message

Audit this rule with severity level:

Not specified

Weitere Informationen zum e-Mail-Flussregeln, einschließlich den gesamten Bereich der Bedingungen und Aktionen, die Sie auswählen können, finden Sie unter [E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#). Exchange Online Protection (EOP) und Hybrid-Kunden können die e-Mail-Flussregeln empfohlenen Vorgehensweisen in [Best Practices for Configuring EOP](#) nutzen. Wenn Sie zum erstmaligen Erstellen von Regeln bereit sind, finden Sie unter [Manage Mail Flow Rules](#).

## Überprüfen des Anlageninhalts

Sie können die Nachrichtenflussregelbedingungen in der folgenden Tabelle verwenden, um den Inhalt von Nachrichtenanlagen zu überprüfen. Bei diesen Bedingungen werden nur das erste Megabyte (MB) des aus einer Anlage extrahierten Texts überprüft. Beachten Sie, dass sich der Grenzwert von 1 MB auf den extrahierten Text und nicht auf die Dateigröße der Anlage bezieht. Eine 2 MB große Datei kann weniger als 1 MB Text enthalten. Auf diese Weise wird der gesamte Text geprüft.

Um diese Bedingungen beim Überprüfen von Nachrichten nutzen zu können, müssen Sie sie zu einer Nachrichtenflussregel hinzufügen. Wie Sie Regeln ändern oder erstellen können, erfahren Sie unter [Manage mail flow rules](#).

NAME DER BEDINGUNG IM EAC	NAME DER BEDINGUNG IN EXCHANGE ONLINE POWERSHELL	BESCHREIBUNG
<b>Inhalt mindestens einer Anlage enthält Ein Anlageninhalt &gt; enthält eines dieser Wörter</b>	<code>AttachmentContainsWords</code>	Diese Bedingung ermittelt Nachrichten mit unterstützten Dateitypenanlagen, die eine angegebene Zeichenfolge oder Zeichengruppe enthalten.
<b>Inhalt einer Anlage entspricht Mindestens eine Anlage &gt; Inhalt stimmt mit diesen Textmustern überein</b>	<code>AttachmentMatchesPatterns</code>	Diese Bedingung ermittelt Nachrichten mit unterstützten Dateitypenanlagen, die ein Textmuster enthalten, das mit einem angegebenen regulären Ausdruck übereinstimmt.

NAME DER BEDINGUNG IM EAC	NAME DER BEDINGUNG IN EXCHANGE ONLINE POWERSHELL	BESCHREIBUNG
<b>Der Inhalt keiner Anlage konnte überprüft werden</b> <b>Mindestens eine Anlage &gt; Inhalt kann nicht überprüft werden</b>	<i>AttachmentIsUnsupported</i>	Nachrichtenflussregeln können nur den Inhalt der unterstützten Dateitypen prüfen. Wenn die Nachrichtenflussregel auf eine nicht unterstützte Anlage trifft, wird die Bedingung <i>AttachmentIsUnsupported</i> ausgelöst. Die unterstützten Dateitypen werden im nächsten Abschnitt beschrieben.

**Hinweise:**

Die Bedingungen in Exchange Online PowerShell sind Parameternamen in den Cmdlets **New-TransportRule** und **Set-TransportRule**. Weitere Informationen finden Sie unter [New-TransportRule](#).

Weitere Informationen zu Eigenschaftstypen für diese Bedingungen finden Sie unter [Mail flow rule conditions and exceptions \(predicates\) in Exchange Online](#) und [Mail flow rule conditions and exceptions \(predicates\) in Exchange Online Protection](#).

Wie Sie mit Windows PowerShell eine Verbindung mit Exchange Online herstellen, können Sie unter [Herstellen einer Verbindung mit Exchange Online PowerShell](#) nachlesen.

### Unterstützte Dateitypen für die Inhaltsüberprüfung mit Nachrichtenflussregeln

In der folgenden Tabelle werden die Dateitypen aufgelistet, die von Nachrichtenflussregeln unterstützt werden. Das System erkennt Dateitypen durch Überprüfung der Dateieigenschaften anstatt der eigentlichen Dateierweiterung automatisch. Auf diese Weise wird verhindert, dass bösartige Hacker die Nachrichtenflussregelfilterung durch das Umbenennen von Dateien umgehen können. Eine Liste der Dateitypen mit ausführbarem Code, die im Kontext von Nachrichtenflussregeln überprüft werden können, finden Sie weiter unten in diesem Thema.

EINE LISTE DER DATEITYPEN MIT AUSFÜHRBAREM CODE, DIE IM KONTEXT VON TRANSPORTREGELN ÜBERPRÜFT WERDEN KÖNNEN, FINDEN SIE WEITER UNTEN IN DIESEM THEMA.	KATEGORIE	DATEIERWEITERUNG
Office 2007 und höher	docm, DOCX, pptm, PPTX, pub, One, XLSB, xlsm, XLSX	Microsoft OneNote- und Microsoft Publisher-Dateien werden nicht standardmäßig unterstützt. Der Inhalt in diesen Dateitypen eingebetteter Teile wird ebenfalls überprüft. Objekte, die jedoch nicht eingebettet sind (z. B. verknüpfte Dokumente) werden nicht überprüft.
Office 2003	doc-, PPT-, xls	Keine
Office 2003	RTF, VDW, VSD, VSS, VST	Keine
.rtf, .vdw, .vsd, .vss, .vst	PDF	Keine
HTML	HTML	Keine

EINE LISTE DER DATEITYPEN MIT AUSFÜHRBAREM CODE, DIE IM KONTEXT VON TRANSPORTREGELN ÜBERPRÜFT WERDEN KÖNNEN, FINDEN SIE WEITER UNten IN DIESEM THEMA.	KATEGORIE	DATEIERWEITERUNG
.xml, .odp, .ods, .odt	.XML, ODP, ODS, ODT	Keine
Text	.odp, .ods, .odt	Keine
OpenDocument	ODP, ODS, ODT	Von ODF-Dateien werden keine Teile verarbeitet. Wenn die ODF-Datei beispielsweise ein eingebettetes Dokument enthält, wird der Inhalt dieses eingebetteten Dokuments nicht überprüft.
AutoCAD-Zeichnung	DXF	Nur diesen Bilddateien zugeordneter Metadatentext wird überprüft. Es gibt keine optische Zeichenerkennung.
Nur diesen Bilddateien zugeordneter Metadatentext wird überprüft.	JPG, TIFF	Nur diesen Bilddateien zugeordneter Metadatentext wird überprüft. Es gibt keine optische Zeichenerkennung.
Komprimierte Archivdateien	.bz2, cab, .gz, .rar, .tar, .zip, .7z	Der Inhalt dieser Dateien, die ursprünglich ein unterstütztes Dateiformat hatten, wird auf ähnliche Weise geprüft und verarbeitet wie Nachrichten mit mehreren Anhängen. Die Eigenschaften der komprimierten Archivdatei selbst werden nicht geprüft. Wenn beispielsweise der Dateityp "Container" Kommentare unterstützt, wird dieses Feld nicht überprüft.

## Überprüfen der Dateieigenschaften von Anlagen

Folgendes können in e-Mail-Flussregeln verwendet werden, um verschiedene Eigenschaften der Dateien zu überprüfen, die Nachrichten zugeordnet sind. Um diese Bedingungen verwenden, wenn Nachrichten prüfen von starten, müssen Sie diese an eine e-Mail-Flussregel hinzufügen. Weitere Informationen zum Erstellen oder Ändern von Regeln finden Sie unter [Manage Mail Flow Rules](#).

NAME DER BEDINGUNG IM EAC	NAME DER BEDINGUNG IN EXCHANGE ONLINE POWERSHELL	BESCHREIBUNG
<b>Der Dateiname mindestens einer Anlage entspricht Mindestens eine Anlage &gt; einen Dateinamen hat, der diesen Textmustern entspricht</b>	<i>AttachmentNameMatchesPatterns</i>	Diese Bedingung ermittelt Nachrichten mit Anlagen, deren Dateiname die von Ihnen festgelegten Zeichen enthält.
<b>Die Dateierweiterung mindestens einer Anlage entspricht Mindestens eine Anlage &gt; eine Dateierweiterung hat, die diese Wörter enthält</b>	<i>Attachmentextensionmatcheswords dieses Prädikat</i>	Diese Bedingung ermittelt Nachrichten mit Anlagen, deren Dateinamenerweiterung mit den von Ihnen festgelegten Zeichen übereinstimmt.

NAME DER BEDINGUNG IM EAC	NAME DER BEDINGUNG IN EXCHANGE ONLINE POWERSHELL	BESCHREIBUNG
<b>Eine Anlage ist größer als oder gleich</b> <b>Mindestens eine Anlage &gt; Größe ist größer oder gleich</b>	<i>AttachmentSizeOver</i>	Diese Bedingung ermittelt Nachrichten mit Anlagen, deren Anlagen größer als oder gleich der angegebenen Größe sind.
<b>Die Nachricht wurde nicht vollständig überprüft</b> <b>Mindestens eine Anlage &gt; Überprüfung nicht abgeschlossen wurde</b>	<i>AttachmentProcessingLimitExceeded</i>	Diese Bedingung ermittelt Nachrichten, deren Anlage nicht vom Nachrichtenflussregel-Agent überprüft wird.
<b>Mindestens eine Anlage hat ausführbaren Inhalt</b> <b>Mindestens eine Anlage &gt; hat ausführbaren Inhalt</b>	<i>AttachmentHasExecutableContent</i>	Diese Bedingung ermittelt Nachrichten, die ausführbare Dateien als Anlagen enthalten. Die unterstützten Dateitypen finden Sie hier.
<b>Jede Anlage ist kennwortgeschützt</b> <b>Jede Anlage &gt; ist kennwortgeschützt</b>	<i>AttachmentIsPasswordProtected</i>	Diese Bedingung ermittelt Nachrichten mit Anlagen, die durch ein Kennwort geschützt sind. Kennwort Erkennung funktioniert nur für Office-Dokumente und ZIP-Dateien.
<b>Jede Anlage hat diese Eigenschaften, einschließlich eines dieser Wörter</b> <b>Jede Anlage &gt; hat diese Eigenschaften, einschließlich eines dieser Wörter</b>	<i>AttachmentPropertyContainsWords</i>	Diese Bedingung ermittelt Nachrichten, bei denen die angegebene Eigenschaft des angehängten Office-Dokuments bestimmte Wörter enthält. Eine Eigenschaft und deren mögliche Werte werden durch einen Doppelpunkt getrennt. Mehrere Werte werden durch ein Komma getrennt. Mehrere Eigenschafts-/Wertpaare werden ebenfalls durch ein Komma getrennt.

#### Hinweise:

Die Bedingungen in Exchange Online PowerShell sind Parameternamen in den Cmdlets **New-TransportRule** und **Set-TransportRule**. Weitere Informationen finden Sie unter [New-TransportRule](#).

Weitere Informationen zu Eigenschaftstypen für diese Bedingungen finden Sie unter [Mail flow rule conditions and exceptions \(predicates\) in Exchange Online](#) und [Mail flow rule conditions and exceptions \(predicates\) in Exchange Online Protection](#).

Wie Sie mit Windows PowerShell eine Verbindung mit Exchange Online herstellen, können Sie unter [Herstellen einer Verbindung mit Exchange Online PowerShell](#) nachlesen.

#### Unterstützte ausführbare Dateitypen für die Überprüfung mit Nachrichtenflussregeln

Die e-Mail-Flussregeln mithilfe TrueType-Erkennung Dateieigenschaften, sondern lediglich die Dateierweiterungen überprüfen. Dadurch wird verhindert, dass Hacker die Regel durch das Umbenennen einer Datei Erweiterungen umgehen. Die folgende Tabelle enthält die ausführbare Dateitypen, die durch diese Bedingungen unterstützt. Wenn eine Datei gefunden wird, ist hier nicht aufgeführt, die **AttachmentIsUnsupported** Bedingung ausgelöst wird.

.RAR	AUSFÜHRBARE 32-BIT-WINDOWS-DATEI MIT EINER DLL-ERWEITERUNG (DYNAMIC LINK LIBRARY)
.exe	DLL
.jar	EXE
Ausführbare Datei für die Deinstallation.	EXE
.obj	EXE
Ausführbare 32-Bit-Windows-Datei	EXE
.os2	VXD
.w16	.OS2
.dos	.w16
.com	.DOS
.pif	COM
.exe	PIF
Die in diesem Artikel aufgeführten Dateitypen können jederzeit mithilfe der IFilter-Integration überprüft werden. Weitere Informationen finden Sie unter Registrieren von Filterpaket-IFiltern für Exchange 2013.	EXE

#### IMPORTANT

Dateien mit den Erweiterungen **.rar** (selbstextrahierende Archivdateien, die mit dem WinRAR-Archivierungsprogramm erstellt wurden), **.jar** (Java-Archivdateien) und **.obj** (kompilierter Quellcode, 3D-Objekt- oder Sequenzdateien) gelten **nicht** als ausführbare Dateitypen. Um diese Dateien zu blockieren, können Sie Nachrichtenflussregeln verwenden, die nach Dateien mit diesen Erweiterungen suchen, wie weiter oben in diesem Thema beschrieben. Oder Sie können eine Antischadsoftware-Richtlinie konfigurieren, die diese Dateitypen blockiert (der gängige Anlagetypenfilter). Weitere Informationen finden Sie unter [Configure Anti-Malware Policies](#).

## Richtlinien zur Verhinderung von Datenverlust und Nachrichtenflussregeln für Anlagen

Um Ihnen die Verwaltung wichtiger Geschäftsinformationen in E-Mails zu erleichtern, können Sie zusätzlich zu den Regeln einer DLP-Richtlinie (Data Loss Prevention, Verhinderung von Datenverlust) eine beliebige anlagenbezogene Bedingung einschließen.

DLP-Richtlinien und Bedingungen Anlage-bezogene helfen Ihnen die Anforderungen Ihres Geschäfts gerecht zu erzwingen, indem Sie diese Anforderungen als e-Mail-Fluss regelbedingungen, Ausnahmen und Aktionen definieren. Wenn Sie die Überprüfung vertrauliche Informationen in einer DLP-Richtlinie einschließen, werden alle Anlagen von Nachrichten für diese Informationen nur überprüft. Anlage-bezogene Bedingungen wie Größe oder Dateityp werden jedoch nicht einbezogen, bis Sie die in diesem Thema aufgeführten Bedingungen hinzufügen. DLP ist nicht in allen Versionen von Exchange verfügbar. Weitere Informationen finden Sie unter [Verhinderung von Datenverlust](#).

## Weitere Informationen

Informationen zum umfassenden Blockieren von E-Mails mit Anlagen unabhängig vom Schadsoftware-Status finden Sie unter [Reducing Malware Threats Through File Attachment Blocking in Exchange Online Protection](#).

# Enable message encryption and decryption in Office 365

18.12.2018 • 2 minutes to read

Office 365 Message Encryption können e-Mail-Benutzer Senden verschlüsselter Nachrichten an Personen innerhalb und außerhalb ihrer Organisation. Informationen zu Office 365 Message Encryption finden Sie unter [Einrichten der neuen Funktionen von Office 365 Message Encryption](#). Weitere Informationen zum Erstellen von Mail Flow Regeln für die Verschlüsselung finden Sie unter [Definieren von Regeln zum Ver- oder Entschlüsseln von e-Mail-Nachrichten](#).

## See also

[Verschlüsselung in Office 365](#)

# Standardszenarien für Anlagensperre für Nachrichtenflussregeln

18.12.2018 • 7 minutes to read

Ihre Organisation erfordern möglicherweise, dass bestimmte Arten von Nachrichten abgelehnt, um die rechtlichen oder Compliance-Anforderungen erfüllen oder entsprechend den geschäftlichen implementieren oder blockiert werden. In diesem Artikel werden Beispiele für häufige Szenarien für das Blockieren aller Anlagen, die Sie mithilfe von Transportregeln in Exchange einrichten.

Weitere Beispiele für das Blockieren bestimmter Anlagen finden Sie unter:

- [Verwenden von Transportregeln von Nachrichtenanlagen](#) (Exchange Server)
- [Verwenden von e-Mail-Flussregeln von Nachrichtenanlagen in Office 365](#) (Exchange Online, Exchange Online Protection)

Der Schadsoftwarefilter enthält einen Filter für gängige Anlagentypen. Klicken Sie in der Exchange-Verwaltungskonsole (EAC) auf **Schutz**, und klicken Sie dann auf **Neu** (), um Filter hinzuzufügen. Navigieren Sie im Exchange Online-Portal zu **Schutz**, und wählen Sie dann **Schadsoftwarefilter** aus.

Führen Sie die folgenden Aktionen durch, um mit dem Implementieren eines dieser Szenarien zum Blockieren bestimmter Nachrichtentypen zu beginnen:

1. Melden Sie sich bei der Exchange-Verwaltungskonsole an.
2. Wechseln Sie zu **Nachrichtenfluss > Regeln**.
3. Klicken Sie auf **Neu** () , und wählen Sie dann **Neue Regel erstellen** aus.
4. Geben Sie im Feld **Name** einen Namen für die Regel an, und klicken Sie dann auf **Weitere Optionen**.
5. Wählen Sie die gewünschten Bedingungen und Aktionen aus.

**Hinweis:** In der Exchange-Verwaltungskonsole die kleinste Anlagengröße, die Sie eingeben ist 1 Kilobyte, die meisten Anlagen erkannt werden sollte. Wenn Sie alle möglichen Anlage beliebiger Größe erkennen möchten, müssen Sie jedoch mithilfe von PowerShell passen die Anlagengröße 1 Byte, nachdem Sie die Regel in der Exchange-Verwaltungskonsole erstellen. Herstellen einer Verbindung mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#). Herstellen einer Verbindung mit Exchange Online Protection PowerShell finden Sie unter [Connect to Exchange Online Protection PowerShell](#).

Ersetzen Sie \_ <Regelname> \_ mit dem Namen des vorhandenen Regel, und führen Sie den folgenden Befehl aus, um die Größe der Anlage auf 1 Byte festzulegen:

```
Set-TransportRule -Identity "<Rule Name>" -AttachmentSizeOver 1B
```

Nachdem Sie die Größe von Anlagen auf 1 Byte angepasst haben, wird als Wert für die Regel in der Exchange-Verwaltungskonsole **0,00 KB** angezeigt.

## Beispiel 1: Blockieren von Nachrichten mit Anlagen und Benachrichtigen des Absenders

Wenn Sie nicht möchten, dass Personen in Ihrer Organisation Anlagen senden oder empfangen, können Sie eine Transportregel einrichten, mit der alle Nachrichten mit Anlagen blockiert werden.

In diesem Beispiel werden alle Nachrichten mit Anlagen blockiert, die an die oder aus der Organisation gesendet wurden.

new rule

Name:

\*Apply this rule if...  
Any attachment is greater than or equal to...

\*Do the following...  
Reject the message with the explanation...

Wenn Sie die Nachricht lediglich blockieren möchten, müssen Sie möglicherweise die Verarbeitung der Regel beenden, sobald diese Regel erfüllt ist. Scrollen Sie im Dialogfeld „Regel“ nach unten, und aktivieren Sie das Kontrollkästchen **Verarbeitung weiterer Regeln beenden**.

## Beispiel 2: Benachrichtigen der vorgesehenen Empfänger, wenn eine eingehende Nachricht blockiert wird

Wenn Sie eine Nachricht ablehnen möchten, den vorgesehenen Empfänger jedoch darüber in Kenntnis setzen möchten, können Sie hierzu die Aktion **Den Empfänger benachrichtigen** verwenden.

Sie können Platzhalter in der Benachrichtigung verwenden, sodass diese Informationen über die ursprüngliche Nachricht enthält. Die Platzhalter müssen in zwei Prozentzeichen (%) eingeschlossen sein. Wenn die Benachrichtigungs-E-Mail gesendet wird, werden die Platzhalter mit Informationen aus der ursprünglichen Nachricht ersetzt. Sie können auch einfachen HTML-Code in der Nachricht verwenden, z. B. <br>, <b>, <i> und <img>.

ART DER INFORMATION	PLATZHALTER
Der Absender der Nachricht.	%%From%%
Die im Feld „An“ aufgeführten Empfänger.	%%To%%
Die im Feld „Cc“ aufgeführten Empfänger.	%%Cc%%
Betreff der ursprünglichen Nachricht.	%%Subject%%
Kopfzeilen aus der ursprünglichen Nachricht. Dies ist mit der Liste von Kopfzeilen in einer Benachrichtigung über den Zustellungsstatus (Delivery Status Notification, DSN) vergleichbar, die für die ursprüngliche Nachricht generiert wurde.	%%Headers%%
Datum, an dem die ursprüngliche Nachricht gesendet wurde.	% MessageDate %

In diesem Beispiel werden alle Nachrichten mit Anlagen blockiert, die an Personen innerhalb Ihrer Organisation

gesendet wurden, und eine Benachrichtigung an die Empfänger gesendet.

new rule

Name:

\*Apply this rule if...

The recipient is located...

and

Any attachment is greater than or equal to...

\*Do the following...

Reject the message with the explanation...

Notify the recipient with a message...

## Beispiel 3: Ändern der Betreffzeile für Benachrichtigungen

Wenn eine Benachrichtigung an den Empfänger gesendet wird, entspricht die Betreffzeile dem Betreff der ursprünglichen Nachricht. Wenn Sie den Betreff ändern möchten, damit dieser für den Empfänger klarer ist, müssen Sie zwei Transportregeln verwenden:

- Die erste Regel fügt das Wort „Unzustellbar“ an den Anfang des Betreffs von Nachrichten mit Anlagen.
- Die zweite Regel blockiert die Nachricht und sendet eine Benachrichtigung an den Absender mit dem neuen Betreff der ursprünglichen Nachricht.

### IMPORTANT

Beide Regeln müssen über die gleichen Bedingungen verfügen. Regeln werden der Reihe nach verarbeitet, sodass die erste Regel das Wort „Unzustellbar“ hinzufügt, und die zweite Regel die Nachricht blockiert und eine Benachrichtigung an den Empfänger sendet.

Die erste Regel könnte folgendermaßen aussehen, wenn Sie das Wort „Unzustellbar“ zum Betreff hinzufügen möchten:

new rule

Name:

\*Apply this rule if...

The sender is located...

and

Any attachment is greater than or equal to...

\*Do the following...

Prepend the subject of the message with...

Und die zweite Regel führt das Blockieren und die Benachrichtigung aus (die gleiche Regel aus Beispiel 2):

new rule

Name:

\*Apply this rule if...

The recipient is located...

and

Any attachment is greater than or equal to...

\*Do the following...

Reject the message with the explanation...

and

Notify the recipient with a message...

## Beispiel 4: Anwenden einer Regel mit einer Zeitbegrenzung

Bei einem Schadsoftwareausbruch müssen Sie ggf. eine Regel mit einer Zeitbegrenzung anwenden, damit Anlagen vorübergehend blockiert werden. Die folgende Regel verfügt beispielsweise über einen Start- und Endzeitpunkt:

Block attachments

\*Do the following...

Except if...

Properties of this rule:

Priority:

Audit this rule with severity level:

Choose a mode for this rule:

Enforce  
 Test with Policy Tips  
 Test without Policy Tips

Activate this rule on the following date:

Deactivate this rule on the following date:

## See also

[Nachrichtenflussregeln \(Transportregeln\) in Exchange Online](#)

[Transportregeln \(Exchange Server 2016\)](#)

[Transport rules \(Exchange Online Protection\)](#)

# Organisationsweite Haftungsausschlüsse, Signaturen, Fußzeilen oder Kopfzeilen für E-Mail-Nachrichten in Office 365

18.12.2018 • 9 minutes to read

**Zusammenfassung:** Administratoren können erfahren Sie, wie Text auf der oberen oder unteren Rand in Office 365 ausgehende Nachrichten anwenden.

Sie können einen Haftungsausschluss, eine Offenlegungserklärung, eine Signatur oder andere Informationen im HTML- oder Nur-Text-Format am Anfang oder Ende von E-Mail-Nachrichten hinzufügen, die aus Ihrer Organisation verschickt oder von ihr empfangen werden. Zu diesem Zweck können Sie eine Nachrichtenflussregel (auch als Transportregel bezeichnet) erstellen, mit der die erforderlichen Informationen zu E-Mail-Nachrichten hinzugefügt werden.

## Hinweise:

- Benutzer können ihre eigenen ausgehenden Nachrichten in Outlook oder Outlook im Web (vormals Outlook Web App) Signaturen anwenden. Weitere Informationen finden Sie unter [erstellen, und fügen Sie eine e-Mail-Signatur in Outlook Web App](#).
- Wenn Sie möchten, dass die Informationen nur an ausgehende Nachrichten angehängt werden, müssen Sie eine entsprechende Bedingungen hinzufügen (z. B. Empfänger außerhalb Ihrer Organisation). Standardmäßig werden Nachrichtenflussregeln auf eingehende und ausgehende Nachrichten angewendet.
- Wenn Sie vermeiden möchten, dass einer E-Mail-Unterhaltung mehrere Haftungsausschlüsse hinzugefügt werden, fügen Sie eine Ausnahme hinzu, die nach eindeutigen Text im Haftungsausschluss sucht. So wird sichergestellt, dass der Haftungsausschluss nur zur Originalnachricht hinzugefügt wird.
- Testen Sie den Haftungsausschluss. Wenn Sie die Nachrichtenflussregel erstellen, haben Sie die Möglichkeit, sofort mit ihrer Verwendung zu beginnen (**Erzwingen**) oder sie zuerst zu testen und die Ergebnisse im Nachrichtenprotokoll anzuzeigen. Es wird empfohlen, alle Nachrichtenflussregeln zu testen, bevor Sie sie auf **Erzwingen** setzen.

Beispiele und Informationen zur Verwendung von Bereich und Format Haftungsausschlüsse, Signaturen und andere Ergänzungen e-Mail-Nachrichten finden Sie unter [organisationsweiten Haftungsausschlüsse, Signaturen, Fußzeilen, oder Kopfzeilen in Exchange 2016](#).

## Was sollten Sie wissen, bevor Sie beginnen?

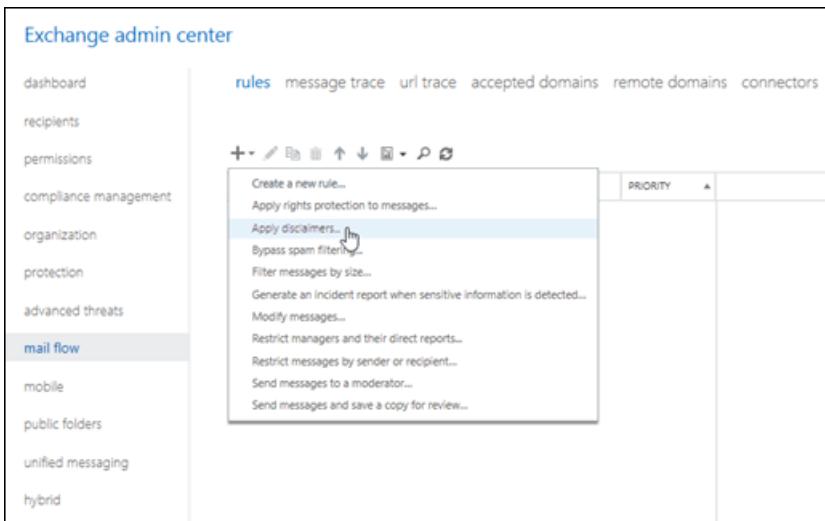
- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 15 Minuten.
- Informationen dazu, wie Sie die Exchange-Verwaltungskonsole (EAC) zugreifen finden Sie unter [Exchange Admin center in Exchange Online](#). So verwenden Sie Windows PowerShell für die Verbindung zu Exchange Online finden Sie unter [Connect to Exchange Online PowerShell](#).
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Nachrichtenübermittlung" im Thema [Featureberechtigungen in Exchange Online](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der EAC zum Einfügen eines Haftungsausschlusses oder einer anderen Kopf- und Fußzeile in eine E-Mail

1. Öffnen Sie das EAC, und wechseln Sie zu **Nachrichtenfluss > Regeln**.
2. Klicken Sie auf **Hinzufügen** , und klicken Sie dann auf **Übernehmen Haftungsausschlüsse**.



3. Geben Sie im daraufhin angezeigten Fenster **Neue Regel** einen eindeutigen Namen für die Regel ein.
4. Wählen Sie im Feld **Diese Regel anwenden, wenn** die Bedingungen zur Anzeige des Haftungsausschlusses aus. Wählen Sie z. B. die Bedingung **Der Empfänger befindet sich** und anschließend **Außerhalb der Organisation** aus. Wenn Sie diese Regel auf jede Nachricht anwenden möchten, die die Organisation verlässt oder von dieser empfangen wird, wählen Sie **[Auf alle Nachrichten anwenden]** aus.
5. Klicken Sie neben dem Feld **Gehen Sie wie folgt vor** auf **Text eingeben**, um den Text Ihres Haftungsausschlusses einzugeben. Informationen darüber, was hinzugefügt werden kann, finden Sie unter [Formatting your disclaimer](#).
6. Klicken Sie auf **Auswählen**, und wählen Sie eine der [alternativen Optionen, wenn der Haftungsausschluss nicht hinzugefügt werden kann](#).
7. Geben Sie den Überwachungsschweregrad an, um den Schweregrad zuzuordnen, der im Nachrichtenprotokoll erscheint.
8. Wählen Sie den Modus für die Regel aus. Wählen Sie **Erzwingen** aus, um den Haftungsausschluss sofort zu aktivieren, oder wählen Sie **Test ohne Richtlinientipps** aus, um eine Nachricht in das Nachrichtenverfolgungsprotokoll zu verschieben, anstatt den Haftungsausschluss hinzuzufügen.
9. Wenn Sie weitere Bedingungen oder Ausnahmen hinzufügen möchten, wählen Sie **Weitere Optionen** am unteren Rand der Seite aus; daraufhin werden weitere Einstellungen angezeigt. Um z. B. die Ausnahme hinzuzufügen, die verhindert, dass mehrere Haftungsausschlüsse in einer E-Mail-Unterhaltung hinzugefügt werden, wählen Sie **Ausnahme hinzufügen** und dann **Betreff oder Nachrichtentext > Betreff oder Nachrichtentext entspricht diesen Textmustern** aus, und geben Sie die Wörter oder Ausdrücke in Ihrem Haftungsausschluss ein. Um Ihren Haftungsausschluss am oberen statt am unteren Rand der E-

Mail-Nachricht zu platzieren, wählen Sie unter **Gehen Sie wie folgt vor** die Option **Haftungsausschluss auf die Nachricht anwenden > Haftungsausschluss voranstellen** aus.

10. Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

Weitere Beispiele für die Gestaltung Ihres Haftungsausschlusses finden Sie unter [Festlegen des Gültigkeitsbereichs des Haftungsausschlusses](#).

## Verwenden von Exchange Online PowerShell zum Hinzufügen eines Haftungsausschlusses oder einer anderen Kopf- und Fußzeile zu einer E-Mail

Verwenden Sie das Cmdlet [New-TransportRule](#) zum Erstellen der Haftungsausschlussregel. Ausführliche Informationen zu Parametern finden Sie unter [Mail flow rule conditions and exceptions \(predicates\) in Exchange Online](#) oder [Mail flow rule conditions and exceptions \(predicates\) in Exchange Online Protection](#).

In diesem Beispiel wird eine neue Nachrichtenflussregel erstellt, mit der ein Haftungsausschluss mit einem Bild am Ende aller E-Mail-Nachrichten eingefügt wird, die an Empfänger außerhalb der Organisation gesendet werden.

```
New-TransportRule -Name "External Disclaimer" -SentToScope NotInOrganization -ApplyHtmlDisclaimerText "<h3>Disclaimer Title</h3><p>This is the disclaimer text.</p><img alt='Contoso logo' src='http://www.contoso.com/images/logo.gif'>"
```

In diesem Beispiel wird eine neue Nachrichtenflussregel erstellt, mit der einen Monat lang eine Werbebotschaft am Anfang aller ausgehenden Nachrichten eingefügt wird.

```
New-TransportRule -Name "March Special" -Enabled $true -SentToScope NotInOrganization -ApplyHtmlDisclaimerLocation Prepend -ActivationDate '03/1/2017' -ExpiryDate '03/31/2017' -ApplyHtmlDisclaimerText "<table align=center width=200 border=1 bordercolor=blue bgcolor=green cellpadding=10 cellspacing=0><tr><td nowrap><a href=http://www.contoso.com/marchspecials.htm>Click to see March specials</a></td></tr></table>"
```

Weitere Beispiele für die Gestaltung Ihres Haftungsausschlusses finden Sie unter [Scoping your disclaimer](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um zu überprüfen, ob Sie erfolgreich einen Haftungsausschluss erstellt haben und ob der Haftungsausschluss wie erwartet funktioniert, führen Sie die folgenden Schritte aus:

- Senden Sie eine reine Text-E-Mail und eine HTML-E-Mail an sich selbst, die alle Bedingungen und Ausnahmen erfüllt, die Sie definiert haben, und prüfen Sie, ob der Text wie beabsichtigt erscheint.
- Wenn Sie eine Ausnahme hinzugefügt haben, um zu vermeiden, dass der Haftungsausschluss in alle Nachrichten innerhalb einer Unterhaltung eingefügt wird, leiten Sie Ihre Textnachrichten an sich selbst weiter, um sicherzustellen, dass Sie den Haftungsausschluss nur einmal erhalten.
- Senden Sie einige Nachrichten an sich selbst, die den Haftungsausschluss nicht enthalten sollen, und prüfen Sie, ob der Haftungsausschluss tatsächlich nicht enthalten ist.

## Weitere Informationen

Nach der Konfiguration einer Haftungsausschluss oder eine e-Mail-Kopfzeile oder eine Fußzeile finden Sie unter [Manage Mail Flow Rules](#) Informationen zum Anzeigen, bearbeiten, aktivieren, deaktivieren oder Entfernen einer Regel.

# E-Mail-Fluss Regel Verfahren im Exchange Online

18.12.2018 • 2 minutes to read

Sie können die mithilfe von Transportregeln mithilfe der folgenden Verfahren beginnen. Weitere Informationen zu Konzepten und Zielen für Transportregeln finden Sie unter [E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#).

[Organisationsweite Nachricht Haftungsausschlüsse, Signaturen, Fußzeilen, oder Kopfzeilen in Office 365](#) Informationen, mit denen Sie einen Haftungsausschluss einrichten e-Mail-Haftungsausschluss, konsistenten Signatur, e-Mail-Kopfzeile, oder e-Mail-Fußzeile mithilfe von Transportregeln.

[Create a Domain or User-Based Safe Sender or Blocked Sender List Using Transport Rules](#) Informationen, die Ihnen helfen, mithilfe von Transportregeln Domänen oder benutzerbasierte Listen von Absendern oder blockierten Absendern zu erstellen.

[Manage message approval](#) Informationen, die Ihnen dabei helfen, moderierte Verteilergruppen zu erstellen und Nachrichten an bestimmte Genehmiger weiterzuleiten, die einer großen Vielzahl an Kriterien entsprechen.

[Verwenden von e-Mail-Flussregeln basierend auf eine Liste der Wörter, Ausdrücke oder Muster e-Mail weitergeleitet](#) Informationen zu Ihrer Organisation e-Mail-Richtlinien entsprechen.

[Mail Flow-Regeln verwenden damit Nachrichten Unübersichtlichkeit umgangen werden kann](#) Informationen, mit denen Sie sicherstellen, dass Nachrichten an eine Posteingang und nicht in den Ordner **Unübersichtlichkeit** gesendet werden.

Themen in Bezug auf das Verhindern von Spam:

- [Create a transport rule that sets the Spam Confidence Level \(SCL\) of a message](#)
- [Überprüfen von Nachrichtenanlagen mithilfe von Nachrichtenflussregeln in Office 365](#)
- [Common attachment blocking scenarios for mail flow rules](#)
- [Verwenden von Exchange-Transportregeln zum aggressiven Filtern von Massennachrichten](#)
- [Weitere Überlegungen zum Konfigurieren von Listen zugelassener IP-Adressen](#)

[Manage e-Mail-Flussregeln](#) Informationen zum Erstellen, anzeigen, bearbeiten, aktivieren, deaktivieren oder Entfernen von Transportregeln und Informationen zum Importieren und Exportieren von Transport regelauflistungen.

[Test Mail Flow Regel](#) Informationen über verschiedene Methoden, mit einer Transportregel zu testen.

[Bewährte Methoden für das Konfigurieren von e-Mail-Flussregeln](#) Informationen zur gemeinsamen Konfigurationsfehler zu vermeiden.

[Verwenden von Berichten zum E-Mail-Schutz in Office 365, um Daten über Schadsoftware, Spam und Regelerkennung anzuzeigen](#) Informationen zum Anzeigen von Zusammenfassungs- und Detailberichten zu Übereinstimmungen mit Transportregeln.

# Verwalten von Nachrichtenflussregeln

18.12.2018 • 28 minutes to read

Mithilfe von E-Mail-Flussregeln, die auch als Transportregeln bezeichnet werden, können Sie Nachrichten, die Ihre Organisation durchlaufen, auf bestimmte Bedingungen prüfen und entsprechende Aktionen ausführen. In diesem Thema wird gezeigt, wie Sie Regeln erstellen, kopieren, aktivieren bzw. deaktivieren, löschen oder importieren bzw. exportieren, deren Reihenfolge ändern, und wie Sie die Regelnutzung überwachen.

## TIP

Damit Ihre Regeln Ihren Erwartungen entsprechend funktionieren, sollten Sie alle Regeln sowie alle Interaktionen zwischen Regeln sorgfältig testen.

Sie interessieren sich für Szenarien, in denen dieses Verfahren verwendet wird? Siehe die folgenden Themen:

- **Organisationsweite Haftungsausschlüsse, Signaturen, Fußzeilen oder Kopfzeilen in Exchange Server**
- **Verwenden von Transportregeln von Nachrichtenanlagen in Exchange Server**
- [Common attachment blocking scenarios for mail flow rules](#)
- [Use mail flow rules to route email based on a list of words, phrases, or patterns](#)
- [Common message approval scenarios](#)
- [Use mail flow rules so messages can bypass Clutter](#)
- [Bewährte Methoden für die Konfiguration von Nachrichtenflussregeln](#)
- [Überprüfen von Nachrichtenanlagen mithilfe von Nachrichtenflussregeln in Office 365](#)
- **Konfigurieren von Transportregeln zum Konfigurieren der Massen-E-Mail-Filterung**
- [Definieren von Regeln zum Ver- oder Entschlüsseln von Nachrichten](#)
- **Erstellen von organisationsweiten Listen sicherer Absender oder blockierter Absender in Office 365**

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den "Transportregeln"-Eintrag im Feld [Berechtigungen für Textnachrichten und Richtlinientreue](#) (Exchange Server) oder in [Featureberechtigungen in Exchange Online](#).
- Wenn eine Regel als **Version 14** aufgeführt ist, bedeutet dies, dass die Regel auf einem Exchange Server 2010 e-Mail-Fluss Regel Format basiert. Alle Optionen sind für diese Regeln zur Verfügung.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen einer Nachrichtenflussregel

Sie können eine e-Mail-Flussregel durch eine Richtlinie (Data Loss Prevention, DLP) erstellen. Eine neue Regel erstellen, einrichten oder kopieren Sie eine Regel erstellen. Sie können die Exchange-Verwaltungskonsole (EAC) oder Exchange Online PowerShell verwenden.

#### NOTE

Nach dem Erstellen oder Ändern einer E-Mail-Flussregel kann es bis zu 30 Minuten dauern, bis die neue oder aktualisierte Regel auf E-Mails angewendet wird.

### Verwenden einer DLP-Richtlinie zum Erstellen von E-Mail-Flussregeln

Jede DLP-Richtlinie ist eine Sammlung von E-Mail-Flussregeln. Nachdem Sie die DLP-Richtlinie erstellt haben, können Sie die Regeln anhand der unten genannten Verfahren verfeinern.

1. Erstellen Sie eine DLP-Richtlinie. Weitere Anweisungen finden Sie in:

- [DLP-Prozeduren für Exchange Server](#)
- [DLP-Verfahren für Exchange Online](#)

2. Ändern der e-Mail-Flussregeln durch die DLP-Richtlinie erstellt. Finden Sie unter [anzeigen oder ändern eine e-Mail-Flussregel](#).

### Verwenden des EAC zum Erstellen einer E-Mail-Flussregel

Im EAC können Sie E-Mail-Flussregeln erstellen, indem Sie eine Vorlage verwenden, eine vorhandene Regel kopieren oder eine Regel von Grund auf neu erstellen.

1. Wechseln Sie zu **Nachrichtenfluss > Regeln**.

2. Erstellen Sie die Regel mithilfe einer der folgenden Optionen:

- Klicken Sie auf **Hinzufügen**, um eine Regel aus einer Vorlage zu erstellen,  und eine Vorlage auswählen.
- Um eine Regel zu kopieren, wählen Sie die Regel aus, und wählen Sie dann **Kopieren**
- Erstellen eine neue Regel von Grund auf neu, **Hinzufügen**  und wählen Sie dann auf **neue Regel erstellen**.

3. Geben Sie im Dialogfeld **Neue Regel** einen Namen für die Regel ein, und wählen Sie dann die Bedingungen und Aktionen für diese Regel aus:

4. Wählen Sie in der **Regel if... anwendet** aus der Liste verfügbarer Bedingungen die gewünschte Bedingung.

- Einige Bedingungen müssen Sie Werte angeben. Wenn Sie **die Absender-Clientbetriebssystems** Bedingung auswählen, müssen Sie eine Adresse des Absenders angeben. Wenn Sie ein Wort oder Ausdruck hinzufügen, beachten Sie, dass Leerzeichen nicht zulässig sind.
- Wählen Sie Wenn die gewünschte Bedingung nicht aufgeführt ist, oder Ausnahmen hinzugefügt werden

müssen, **Weitere Optionen**. Zusätzliche Bedingungen und Ausnahmen werden aufgelistet.

- Wenn Sie keine Bedingung angeben möchten und diese Regel auf alle Nachrichten in Ihrer Organisation angewendet werden soll, wählen Sie die Bedingung **[Auf alle Nachrichten anwenden]** aus.
2. Wählen Sie in **die folgenden Schritte aus...** die Aktion, die die Regel, die auf Nachrichten anhand der Kriterien aus der Liste der verfügbaren Aktionen angewendet werden soll.
- Einige der Aktionen benötigen Sie Werte angeben. Wenn Sie die Bedingung **Weiterleiten der Nachricht zur Genehmigung an...** auswählen, müssen Sie einen Empfänger in der Organisation auszuwählen.
  - Wenn die gewünschte Bedingung nicht aufgeführt ist, wählen Sie **Weitere Optionen**. Zusätzliche Bedingungen werden aufgelistet.
3. Geben Sie an, wie regelübereinstimmungsdaten für diese Regel in der [Data Loss Prevention \(DLP\)-Berichte](#) und die [transportregelberichteangezeigt](#) werden.
- Wählen Sie unter **diese Regel mit Schweregrade** eine Ebene den Schweregrad für diese Regel angeben. Die Office 365-Aktivität-Berichte für e-Mail-Flussregeln, die nach dem Schweregrad Gruppe regelübereinstimmungen. Schweregrad nur ein Filter ist, verwenden Sie die Berichte vereinfachen. Der Schweregrad hat keine Auswirkung auf die Priorität, in der die Regel verarbeitet wird.

```
> [ !NOTE ]
> <span data-ttu-id="1fd02-171">Wenn Sie das Kontrollkästchen **Diese Regel mit Schweregrad überwachen** deaktivieren, werden Regelübereinstimmungen in den Regelberichten nicht angezeigt.</span><span class="sxs-lookup"><span data-stu-id="1fd02-171">If you clear the **Audit this rule with severity level** checkbox, rule matches will not show up in the rule reports.</span></span>
```

4. Legen Sie den Modus für die Regel fest. Sie können einen von zwei Testmodi verwenden, um die Regel zu testen, ohne den E-Mail-Fluss zu beeinträchtigen. In beiden Testmodi wird der Nachrichtenablaufverfolgung ein Eintrag hinzugefügt, wenn die Bedingungen erfüllt werden.
- **Enforce:** Dadurch wird die Regel aktiviert und Verarbeitung von Nachrichten sofort beginnt. Alle Aktionen für die Regel werden ausgeführt.
  - **Test mit Richtlinientipps:** dies die Regel wird aktiviert und alle Aktionen für Richtlinientipps (**Absender mit Richtlinientipp benachrichtigen**) gesendet, aber keine Aktionen im Zusammenhang mit der Nachrichtenübermittlung werden ausgeführt. Data Loss Prevention (DLP) ist erforderlich, um diesen Modus verwenden. Weitere Informationen finden Sie unter [Tipps zu Richtlinien](#).
  - **Test ohne Richtlinientipps:** nur die generieren schadensbericht Aktion werden erzwungen. Es werden keine Aktionen im Zusammenhang mit der Nachrichtenübermittlung ausgeführt.
4. Wenn Sie mit der Regel zufrieden sind, wechseln Sie zu Schritt 5. Klicken Sie auf **Weitere Optionen**, um weitere Bedingungen oder Aktionen hinzuzufügen, Ausnahmen anzugeben oder zusätzliche Eigenschaften festzulegen. Nachdem Sie auf **Weitere Optionen** geklickt haben, füllen Sie die folgenden Felder aus, um Ihre Regel zu erstellen:
5. Klicken Sie auf **Bedingung hinzufügen**, um weitere Bedingungen hinzuzufügen. Wenn Sie über mehrere Bedingungen verfügen, können Sie eine beliebige Bedingung entfernen, indem Sie daneben auf **X entfernen** klicken. Beachten Sie, dass eine größere Auswahl an Bedingungen zur Verfügung steht, nachdem Sie auf **Weitere Optionen** geklickt haben.
6. Klicken Sie auf **Aktion hinzufügen**, um weitere Aktionen hinzuzufügen. Wenn Sie über mehrere Aktionen verfügen, können Sie eine beliebige Aktion entfernen, indem Sie daneben auf **X entfernen**

klicken. Beachten Sie, dass eine größere Auswahl an Aktionen zur Verfügung steht, nachdem Sie auf **Weitere Optionen** geklickt haben.

7. Klicken Sie zum Angeben von Ausnahmen auf **Ausnahme hinzufügen**, und wählen Sie anschließend die Ausnahmen in der Dropdownliste **Außer wenn...** aus. Sie können beliebige Ausnahmen aus der Regel entfernen, indem Sie neben der jeweiligen Ausnahme auf **X entfernen** klicken.
8. Wenn diese Regel nach einem bestimmten Datum wirksam werden soll, klicken Sie auf **Diese Regel an folgendem Datum aktivieren:** Geben Sie anschließend ein Datum an. Beachten Sie, dass die Regel vor diesem Datum weiterhin aktiviert ist, aber nicht verarbeitet wird.

```
<span data-ttu-id="1fd02-p125">Ebenso können Sie festlegen, dass die Regel an einem bestimmten Datum nicht verarbeitet wird. Klicken Sie hierzu auf **Diese Regel an folgendem Datum deaktivieren:** Geben Sie anschließend ein Datum an. Beachten Sie, dass die Regel aktiviert bleibt, aber nicht verarbeitet wird.</span><span class="sxs-lookup"><span data-stu-id="1fd02-p125">Similarly, you can have the rule stop processing at a certain date. To do so, click **Deactivate this rule on the following date:** and specify a date. Note that the rule will remain enabled, but it won't be processed.</span></span>
```

5. Sie können auswählen, dass keine weiteren Regeln angewendet werden, nachdem diese Regel auf eine Nachricht angewendet wurde. Klicken Sie hierzu auf **Keine weiteren Regeln anwenden**. Wenn Sie diese Option aktivieren und eine Nachricht von dieser Regel verarbeitet wird, werden auf diese Nachricht keine nachfolgenden Regeln angewendet.
6. Sie können angeben, wie die Nachricht behandelt werden soll, wenn die Regelverarbeitung nicht abgeschlossen werden kann. Standardmäßig wird die Regel ignoriert, und die Nachricht wird normal verarbeitet. Sie können jedoch die Nachricht zur Verarbeitung erneut senden. Aktivieren Sie hierfür das Kontrollkästchen **Nachricht zurückstellen, wenn die Regelverarbeitung nicht abgeschlossen wird**.
7. Wenn Ihre Regel die Absenderadresse analysiert, wird standardmäßig nur der Nachrichtenkopf untersucht. Sie können die Regel jedoch so konfigurieren, dass auch der SMTP-Nachrichtenumschlag untersucht wird. Um anzugeben, was untersucht wird, klicken Sie für **Absenderadresse in Nachricht untersuchen** auf einen der folgenden Werte:
  - **Kopfzeile:** nur die Nachrichtenkopfzeilen untersucht werden.
  - **Briefumschlag:** nur der SMTP-Nachrichtenumschlag werden untersucht.
  - **Kopf- oder Umschlag:** sowohl der Nachrichtenkopf Kopf- und SMTP-Nachrichtenumschlag werden untersucht.
8. Im Feld **Kommentare** können Sie Kommentare zu dieser Regel hinzufügen.
9. Klicken Sie auf **Speichern**, um die Erstellung der Regel abzuschließen.

#### Verwenden Sie Exchange Online PowerShell, um eine e-Mail-Flussregel erstellen

In diesem Beispiel wird das Cmdlet [New-TransportRule](#) eine neue e-Mail-Flussregel erstellen, die voranzustellen " `External message to Sales DG:` " auf Nachrichten, die von außerhalb der Organisation an die Verteilergruppe "Sales Department" gesendet.

```
New-TransportRule -Name "Mark messages from the Internet to Sales DG" -FromScope NotInOrganization -SentTo "Sales Department" -PrependSubject "External message to Sales DG:"
```

Die Regelparameter und -aktionen, die in den oben stehenden Schritten verwendet werden, dienen nur zu Demonstrationszwecken. Prüfen Sie alle verfügbaren E-Mail-Flussregelbedingungen und -aktionen, um die für Ihre Anforderungen geeigneten Prädikate und Aktionen zu ermitteln.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie wie folgt vor, um sich zu vergewissern, dass Sie erfolgreich eine neue E-Mail-Flussregel erstellt haben:

- Überprüfen Sie im EAC, ob die von Ihnen neu erstellte E-Mail-Flussregel in der Liste **Regeln** aufgeführt ist.
- Von Exchange Online PowerShell stellen Sie sicher, dass Sie die neue e-Mail-Flussregel erfolgreich erstellt mithilfe des folgenden Befehls (das folgende Beispiel überprüft die in der Exchange Online PowerShell-Beispiel oben erstellte Regel):

```
Get-TransportRule "Mark messages from the Internet to Sales DG"
```

## Anzeigen oder Ändern einer E-Mail-Flussregel

### NOTE

Nach dem Erstellen oder Ändern einer E-Mail-Flussregel kann es bis zu 30 Minuten dauern, bis die neue oder aktualisierte Regel auf E-Mails angewendet wird.

### Anzeigen oder Ändern einer E-Mail-Flussregel mithilfe des EAC

1. Navigieren Sie im EAC zu **Nachrichtenfluss > Regeln**.
2. Wenn Sie eine Regel in der Liste, die Bedingungen, Aktionen auswählen, werden Ausnahmen und wählen Sie Eigenschaften dieser Regel im Detailbereich angezeigt. Um alle Eigenschaften einer bestimmten Regel anzuzeigen, double klicken Sie darauf. Daraufhin wird das Regel-Editor-Fenster, in dem Sie die Regel ändern können. Weitere Informationen zu Eigenschaften der Regel finden Sie unter [Verwenden der Exchange-Verwaltungskonsole zum Erstellen einer Regel der e-Mail-Fluss](#) Abschnitt weiter oben in diesem Thema.

### Verwenden von Exchange Online PowerShell anzeigen oder Ändern einer e-Mail-Fluss-Regel

Das folgende Beispiel bietet Ihnen eine Liste aller in Ihrer Organisation konfigurierten Regeln:

```
Get-TransportRule
```

Um die Eigenschaften einer bestimmten e-Mail-Fluss Regel anzuzeigen, müssen Sie den Namen der Regel oder seine GUID. Es empfiehlt sich in der Regel die Ausgabe an das Cmdlet **Format-List** formatieren Sie die Eigenschaften zu senden. Das folgende Beispiel gibt alle Eigenschaften der e-Mail-Flussregel mit dem Namen Absender ist Mitglied von Marketing:

```
Get-TransportRule "Sender is a member of marketing" | Format-List
```

Um die Eigenschaften einer bestehenden Regel zu ändern, verwenden Sie das Cmdlet [Set-TransportRule](#). Mit diesem Cmdlet können Sie beliebige Eigenschaften, Bedingungen, Aktionen oder Ausnahmen ändern, die einer Regel zugeordnet sind. Im folgenden Beispiel wird der Regel "Sender is a member of marketing" eine Ausnahme hinzugefügt, damit sie nicht auf Nachrichten angewendet wird, die vom Benutzer "Kelly Rollin" gesendet werden:

```
Set-TransportRule "Sender is a member of marketing" -ExceptIfFrom "Kelly Rollin"
```

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um die erfolgreiche Änderung einer E-Mail-Flussregel zu überprüfen, gehen Sie wie folgt vor:

- Klicken Sie im EAC in der Liste **Regeln** auf die von Ihnen geänderte Regel, und zeigen Sie den Detailbereich an.
- Von Exchange Online PowerShell stellen Sie sicher, dass Sie die e-Mail-Flussregel erfolgreich geändert mithilfe des folgenden Befehls die Eigenschaften aufgelistet, die Sie zusammen mit dem Namen der Regel (im Beispiel unten wird überprüft, ob die Regel, die in Exchange Online PowerShell geändert geändert Beispiel oben):

```
Get-TransportRule "Sender is a member of marketing" | Format-List Name,ExceptIfFrom
```

## Eigenschaften von Nachrichtenflussregeln

Sie können auch mit dem Set-TransportRule-Cmdlet verwenden, um vorhandene Transportregeln in Ihrer Organisation zu ändern. Im folgenden ist eine Liste Eigenschaften nicht verfügbar ist, in der Exchange-Verwaltungskonsole, die Sie ändern können. Weitere Informationen zur Verwendung von das Cmdlet **Set-TransportRule**, um diese **Set-TransportRule** finden Sie unter Änderungen vornehmen

NAME DER BEDINGUNG IN DER EXCHANGE-VERWALTUNGSKONSOLE	NAME DER BEDINGUNG IN EXCHANGE ONLINE POWERSHELL	BESCHREIBUNG
<b>Verarbeiten von Regeln beenden</b>	<i>StopRuleProcessing</i>	Ermöglicht es Ihnen, die Verarbeitung zusätzlicher Regeln zu beenden
<b>Kopf/Umschlag stimmen überein</b>	<i>SenderAddressLocation</i>	Ermöglicht es Ihnen, den SMTP-Nachrichtenumschlag zu untersuchen, um sicherzustellen, dass der Kopf und der Umschlag übereinstimmen
<b>Überwachungsschweregrad</b>	<i>SetAuditSeverity</i>	Ermöglicht es Ihnen, einen Schweregrad für die Überwachung auszuwählen
<b>Regelmodi</b>	<i>Mode</i>	Ermöglicht es Ihnen, den Modus für die Regel festzulegen

## Festlegen der Priorität einer E-Mail-Flussregel

Die Regel oben in der Liste wird zuerst verarbeitet. Diese Regel weist die **Priorität** 0 auf.

### Festlegen der Priorität einer Regel im EAC

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Regeln**. Dadurch werden die Regeln in der Reihenfolge, in der sie verarbeitet werden, angezeigt.
2. Wählen Sie eine Regel aus, und verschieben Sie die Regeln mithilfe der Pfeile in der Liste nach oben oder unten.

### Verwenden von Exchange Online PowerShell festlegen die Priorität einer Regel

Im folgenden Beispiel wird die Priorität von "Sender is a member of marketing" auf 2 festgelegt:

```
Set-TransportRule "Sender is a member of marketing" priority "2"
```

## **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Um die erfolgreiche Änderung einer E-Mail-Flussregel zu überprüfen, gehen Sie wie folgt vor:

- Prüfen Sie im EAC in der Regelliste die Reihenfolge der Regeln.
- Überprüfen Sie von Exchange Online PowerShell die Priorität der Regeln (im Beispiel unten wird überprüft, ob in Exchange Online PowerShell-Beispiel oben geänderte Regel):

```
Get-TransportRule * | Format-List Name,Priority
```

## Aktivieren oder Deaktivieren einer E-Mail-Flussregel

Regeln werden bei ihrer Erstellung aktiviert. Sie können eine E-Mail-Flussregel deaktivieren.

### **Aktivieren oder Deaktivieren einer E-Mail-Flussregel mithilfe des EAC**

1. Navigieren Sie im EAC zu **Nachrichtenfluss > Regeln**.
2. Deaktivieren Sie das Kontrollkästchen neben dem Namen einer Regel, um diese Regel zu deaktivieren.
3. Aktivieren Sie das Kontrollkästchen neben dem Namen einer Regel, um die deaktivierte Regel zu aktivieren.

### **Verwenden von Exchange Online PowerShell aktivieren oder deaktivieren eine e-Mail-Fluss-Regel**

Im folgenden Beispiel wird die E-Mail-Flussregel "Sender is a member of marketing" deaktiviert:

```
Disable-TransportRule "Sender is a member of marketing"
```

Im folgenden Beispiel wird die E-Mail-Flussregel "Sender is a member of marketing" aktiviert:

```
Enable-TransportRule "Sender is a member of marketing"
```

## **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Gehen Sie wie folgt vor, um sich zu vergewissern, dass Sie erfolgreich eine E-Mail-Flussregel aktiviert oder deaktiviert haben:

- Zeigen Sie im EAC die Liste **Regeln** an, und überprüfen Sie den Status des Kontrollkästchens in der Spalte **EIN**.
- Von Exchange Online PowerShell, führen Sie den folgenden Befehl, der eine Liste aller Regeln in Ihrer Organisation einschließlich Status zurückgegeben wird:

```
Get-TransportRule | Format-Table Name,State
```

## Entfernen einer E-Mail-Flussregel

### **Verwenden des EAC zum Entfernen einer E-Mail-Flussregel**

1. Navigieren Sie im EAC zu **Nachrichtenfluss > Regeln**.

2. Wählen Sie die Regel, die Sie entfernen möchten und klicken Sie dann auf **Löschen** [ ].

### **Verwenden Sie Exchange Online PowerShell, um eine e-Mail-Flussregel zu entfernen**

Im folgenden Beispiel wird die E-Mail-Flussregel "Sender is a member of marketing" entfernt:

```
Remove-TransportRule "Sender is a member of marketing"
```

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie wie folgt vor, um sich zu vergewissern, dass Sie die E-Mail-Flussregel erfolgreich entfernt haben:

- Zeigen Sie im EAC die Liste **Regeln** an und überprüfen Sie, dass die von Ihnen entfernte Regel nicht länger angezeigt wird.
- Exchange Online PowerShell führen Sie den folgenden Befehl aus, und stellen Sie sicher, dass die Regel, die Sie entfernen nicht mehr aufgeführt wird:

```
Get-TransportRule
```

## Überwachung der Regelnutzung

Wenn Sie Exchange Online oder Exchange Online Protection verwenden, können Sie die Anzahl der Male überprüfen, die mithilfe eines regelberichts jede Regel erfüllt werden. Um in den Bericht einbezogen werden, muss eine Regel das Kontrollkästchen **diese Regel mit Schweregrad** ausgewählt haben. Sie können einen Bericht online betrachten, oder laden eine Excel-Version von allen e-Mail-schutzberichte.

#### NOTE

Die meisten Daten werden innerhalb von 24 Stunden im Bericht erfasst. Bei einigen Daten kann es bis zu 5 Tage dauern, bis sie angezeigt werden.

### Generieren eines Regelberichts mithilfe des Office 365 Admin Center

1. Wählen Sie im Office 365 Admin Center **Berichte** aus.
2. Wählen Sie im Abschnitt **Regeln\*\*\*\*Häufigste Regelübereinstimmungen bei E-Mails** oder **Regelübereinstimmungen bei E-Mails** aus.

Weitere Informationen finden Sie unter [Anzeigen von Berichten zum E-Mail-Schutz](#).

### Herunterladen einer Excel-Version der Berichte

1. Wählen Sie im Office 365 Admin Center auf der Berichtsseite **Berichte zum E-Mail-Schutz (Excel)** aus.
2. Wenn Sie die Excel-Berichte zum E-Mail-Schutz zum ersten Mal verwenden, wird eine Registerkarte mit der Downloadseite geöffnet.
3. Wählen Sie **Download** aus, um das Microsoft Office-365-Excel-Plug-In für Exchange Online-Berichte herunterzuladen.
4. Öffnen Sie den Download.
5. Wählen Sie im Dialogfeld **Mail Protection reports for Office 365 Setup** (Einrichtung für Berichte zum E-Mail-Schutz für Office 365) **Weiter** aus, stimmen Sie den Bedingungen des Lizenzvertrags zu, und wählen Sie dann **Weiter** aus.
6. Wählen Sie den Dienst aus, den Sie verwenden, und wählen Sie dann **Weiter** aus.
7. Überprüfen Sie die Voraussetzungen, und klicken Sie auf **Weiter**.
8. Wählen Sie **Installieren** aus. Auf Ihrem Desktop wird eine Verknüpfung zu den Berichten erstellt.

9. Wählen Sie auf dem Desktop **Berichte zum E-Mail-Schutz für Office 365** aus.

10. Wählen Sie im Bericht die Registerkarte **Regeln** aus.

## Importieren oder Exportieren von E-Mail-Flussregelsammlungen

Sie müssen Exchange Online PowerShell importieren oder Exportieren eine e-Mail-Fluss Regelsammlung verwenden. Informationen dazu, wie Sie eine e-Mail-Fluss Regelsammlung aus einer XML-Datei importieren finden Sie unter [Import-TransportRuleCollection](#). Informationen dazu, wie Sie eine e-Mail-Fluss Regelsammlung in eine XML-Datei zu exportieren finden Sie unter [Export-TransportRuleCollection](#).

## Benötigen Sie weitere Hilfe?

Ressourcen für Exchange Online:

[Nachrichtenflussregeln \(Transportregeln\) in Exchange Online](#)

[Nachrichtenflussregel-Bedingungen und -Ausnahmen \(Prädikate\) in Exchange Online](#)

[Aktionen für Nachrichtenflussregeln in Exchange Online](#)

[Transport- und Postfachregelgrenzen](#)

Ressourcen für Exchange Online Protection:

[Transport rules](#)

[Transport Rule Conditions](#)

[Transport Rule Actions](#)

[Transport- und Postfachregelgrenzen](#)

Ressourcen für Exchange Server 2016:

[Transport Rules](#)

[Transport Rule Conditions](#)

[Transport Rule Actions](#)

# Testen einer Nachrichtenflussregel

18.12.2018 • 11 minutes to read

Immer wenn Sie eine Exchange-E-Mail-Flussregel erstellen, die auch als Transportregel bezeichnet wird, sollten Sie sie zunächst testen, bevor Sie sie aktivieren. Wenn Sie versehentlich eine Bedingung erstellen, die nicht exakt das Gewünschte macht oder mit anderen Regeln auf unerwartete Weise interagiert, vermeiden Sie dadurch unvorhersehbare Folgen.

## IMPORTANT

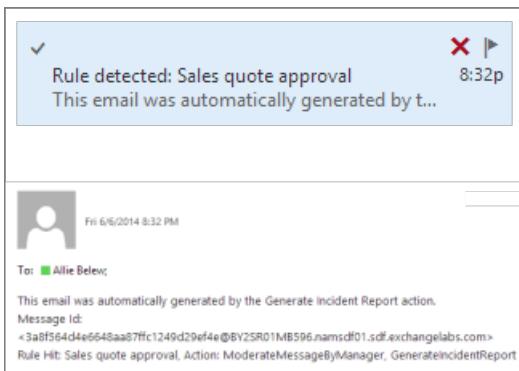
Warten Sie nach dem Erstellen einer Regel 30 Minuten, ehe Sie sie testen. Wenn Sie die Regel sofort nach dem Erstellen testen, ist das Verhalten möglicherweise inkonsistent. Bei Verwendung von Exchange Server und mehreren Exchange-Server kann es sogar länger dauern, bis alle Server die Regel empfangen haben.

## Schritt 1: Erstellen einer Regel im Testmodus

Sie können die Bedingungen für eine Regel auswerten, ohne Aktionen auszuführen, die die Nachrichtenübermittlung beeinträchtigen, indem Sie einen Testmodus auswählen. Sie können eine Regel so einrichten, dass Sie jedes Mal eine E-Mail-Benachrichtigung erhalten, wenn es eine Regelübereinstimmung gibt. Oder Sie können die [Untersuchen der Nachrichtenablaufverfolgung](#) auf Nachrichten untersuchen, die ggf. mit der Regel übereinstimmen. Es gibt zwei Testmodi:

- **Test ohne Richtlinientipps:** Verwenden Sie diesen Modus zusammen mit einer Aktion schadensbericht, und Sie erhalten eine e-Mail-Nachricht jedes Mal eine e-Mail mit der Regel übereinstimmt.
- **Test mit Richtlinientipps:** in diesem Modus ist nur verfügbar, wenn Sie [Verhinderung von Datenverlust](#) (DLP), verwenden das mit einigen Abonnementpläne Exchange Online und Exchange Online Protection (EOP) verfügbar ist. In diesem Modus wird eine Nachricht an den Absender festgelegt, wenn eine Richtlinie mit einer Nachricht, die sie senden möchten übereinstimmt, aber keine e-Mail-Fluss Aktionen werden ausgeführt.

Nachstehend sehen Sie die Meldung bei einer Regelübereinstimmung, wenn Sie die Schadensberichtsaktion hinzufügen:



## Verwenden eines Testmodus mit einer Schadensberichtsaktion

1. Navigieren Sie im Exchange-Verwaltungskonsole (EAC) zu **Nachrichtenfluss > Regeln**.
2. Erstellen Sie eine neue Regel, oder wählen Sie eine vorhandene Regel und dann **Bearbeiten** aus.
3. Führen Sie einen Bildlauf nach unten zum Abschnitt **Modus für diese Regel auswählen** durch, und wählen Sie dann **Test ohne Richtlinientipps** oder **Test mit Richtlinientipps** aus.

4. Fügen Sie eine Schadensberichtsaktion hinzu:
5. Wählen Sie **Aktion hinzufügen**, oder, falls nicht angezeigt, **Weitere Optionen**, und dann **Aktion hinzufügen** aus.
6. Wählen Sie **Schadensbericht erstellen und senden an** aus.
7. Klicken Sie auf **Wählen Sie eine...**, und wählen Sie selbst oder eine andere Person.
8. Wählen Sie **Nachrichteneigenschaften einbeziehen** und dann alle Eigenschaften aus, die die E-Mail enthalten soll, die Sie empfangen. Wenn Sie keine auswählen, erhalten Sie dennoch eine E-Mail, falls die Regel erfüllt ist.
9. Klicken Sie auf **Speichern**.

## Schritt 2: Prüfen, ob die Regel wie gewünscht funktioniert

Zum Testen einer Regel können Sie entweder genügend Testnachrichten senden, um zu bestätigen, dass das Erwartete passiert, oder die Nachrichtenablaufverfolgung auf Nachrichten überprüfen, die Personen in Ihrer Organisation senden. Überprüfen Sie auf jeden Fall die folgenden Arten von Nachrichten:

- Nachrichten, von denen Sie erwarten, dass sie der Regel entsprechen
- Nachrichten, von denen Sie nicht erwarten, dass sie der Regel entsprechen
- Nachrichten, die von und an Personen in Ihrer Organisation gesendet wurden
- Nachrichten, die von und an Personen außerhalb Ihrer Organisation gesendet wurden
- Antworten auf Nachrichten, die der Regel entsprechen
- Nachrichten, die zu Interaktionen zwischen mehreren Regeln führen können

### Tipps für das Senden von Testnachrichten

Eine Möglichkeit zum Testen ist, sich als Absender und Empfänger einer Testnachricht anzumelden.

- Wenn Sie über keinen Zugriff auf mehrere Konten in Ihrer Organisation verfügen, können Sie den Test mit einem [Office 365-Testkonto](#) durchführen oder temporär einige gefälschte Benutzer in Ihrer Organisation erstellen.
- Da es ein Webbrowser in der Regel nicht zulässt, dass Sie auf dem gleichen Computer bei mehreren Konten gleichzeitig angemeldet sind, können Sie für jeden Benutzer das [Internet Explorer InPrivate-Browsen](#) oder einen anderen Computer, Webbrowser oder ein anderes Gerät verwenden.

### Untersuchen der Nachrichtenablaufverfolgung

Die Nachrichtenablaufverfolgung enthält einen Eintrag für jede Regel, die für die Nachricht gefunden wird, und einen Eintrag für jede von der Regel ausgeführte Aktion. Dies ist nützlich zum Nachverfolgen, was mit Testnachrichten geschieht, und auch zum Nachverfolgen, was mit tatsächlichen Nachrichten passiert, die Ihre Organisation durchlaufen.

sales quote 200			
Sender:	spand@contoso.com	Recipient:	anrep@contoso.org
Message size:	5.43		
Message ID:	<0a0f564044661bae07ff102462bfef@E102801948396.usmof01.offexchange01.com>	To IP:	68.17.214.52
From IP:	97.113.24.97		
Delivery status:	Delivered		
DATE	EVENT	ACTION	DETAIL
6/6/2014 8:02...	RECEIVE		Message received by #E102801948396
6/6/2014 8:02...	SUBMIT		Message received by #E102801948396
6/6/2014 8:02...	Transport rule	GenerateIncidentReport	The message is awaiting submission to the mailbox store.
6/6/2014 8:02...	Transport rule	Moderate message by mana...	Transport rule: 'Sales quote approval', ID: E00469508-7...
6/6/2014 8:02...	Transport rule	Apply HTML disclaimer	Transport rule: 'Sales quote approval', ID: E00469508-7...
6/6/2014 8:02...	SEND		Transport rule: 'Add a disclaimer to all' (rule operator: ID: ...)
			Message transferred from To_DefaultOpportunity@L5
Transport rule	GenerateIncidentReport	Transport rule: 'Sales quote approval'	
Transport rule	Moderate message by mana...	Transport rule: 'Sales quote approval'	
Transport rule	Apply HTML disclaimer	Transport rule: 'Add a disclaimer to all'	

1. Wechseln Sie im EAC zu **Nachrichtenfluss > Nachrichtenablaufverfolgung**.
2. Suchen Sie die Nachrichten, die Sie nachverfolgen möchten, mithilfe von Kriterien wie z. B. Absender und Sendedatum. Hilfe beim Angeben von Kriterien finden Sie unter [Run a Message Trace and View Results](#).
3. Nach dem Auffinden der Nachricht, die Sie nachverfolgen möchten, doppelklicken Sie darauf, um Details zur Nachricht anzeigen.
4. Suchen Sie in der Spalte **Ereignis** nach **Transportregel**. In der Spalte **Aktion** wird die spezifisch erfolgte Aktion angezeigt.

## Schritt 3: Festlegen der zu erzwingenden Regel im Anschluss an den Test

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Regeln**.
2. Wählen Sie eine Regel aus, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf **Erzwingen**.
4. Wenn Sie eine Aktion zum Generieren eines Schadensberichts verwendet haben, wählen Sie die Aktion aus, und klicken Sie dann auf **Entfernen**.
5. Klicken Sie auf **Speichern**.

### TIP

Um Überraschungen zu vermeiden, informieren Sie die Benutzer über neue Regeln.

## Vorschläge zur Problembehandlung

Hier nun einige gängige Probleme und Lösungen:

- **Alles sieht wie gewünscht aus, doch die Regel funktioniert nicht.**  
Gelegentlich dauert es länger als 15 Minuten, bis ein neuer E-Mail-Fluss zur Verfügung steht. Warten Sie ein paar Stunden, und wiederholen Sie den Test. Überprüfen Sie auch, ob ggf. eine andere Regel störend wirkt. Versuchen Sie, die Priorität dieser Regel in 0 zu ändern, indem Sie sie an den Anfang der Liste verschieben.
- **Der Haftungsausschluss wird an die ursprüngliche Nachricht und alle Antworten und nicht nur an die ursprüngliche Nachricht angefügt.**  
Um dies zu vermeiden, können Sie eine Ausnahme für die Haftungsausschlussregel hinzufügen, dass nach einem eindeutigen Ausdruck im Haftungsausschluss gesucht werden soll.

- **Meine Regel enthält zwei Bedingungen, und ich möchte, dass die Aktion erfolgt, wenn eine der Bedingungen erfüllt ist. Sie erfolgt aber nur, wenn beide Bedingungen zutreffen.**

Sie müssen zwei Regeln erstellen, eine für jede Bedingung. Sie können die Regel problemlos kopieren, indem Sie **Kopieren** auswählen und eine Bedingung aus dem Original und die andere Bedingung aus der Kopie entfernen.

- **ich arbeite mit Verteilergruppen und Der Absender ist ( SentTo) nicht funktionsfähig zu sein scheinen.**

**SentTo** entspricht Nachrichten, bei denen einer der Empfänger ein Postfach, E-Mail-aktivierter Benutzer oder Kontakt ist. Sie können jedoch keine Verteilergruppe mit dieser Bedingung angeben. Verwenden Sie stattdessen **Feld „An“ enthält ein Mitglied dieser Gruppe ( SentToMemberOf)**.

## Weitere Testoptionen

Wenn Sie Exchange Online oder Exchange Online Protection verwenden, können Sie mithilfe eines Regelberichts prüfen, wie oft jede Regel erfüllt wird. Damit eine Regel in den Berichten eingeschlossen wird, muss bei der Regel das Kontrollkästchen **Diese Regel mit Schweregrad überwachen** aktiviert sein. Dank dieser Berichte können Sie Trends bei der Verwendung von Regeln ausmachen und Regeln bestimmen, die nicht erfüllt werden.

Wählen Sie zum Anzeigen eines Regelberichts im Office 365 Admin Center die Option **Berichte** aus.

### NOTE

Die meisten Daten werden innerhalb von 24 Stunden im Bericht erfasst. Bei einigen Daten kann es bis zu 5 Tage dauern, bis sie angezeigt werden.



Weitere Informationen finden Sie unter [Anzeigen von Berichten zum E-Mail-Schutz](#).

## Benötigen Sie weitere Hilfe?

[Verwalten von Nachrichtenflussregeln](#)

[E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online \(Exchange Online\)](#)

[Transport rules \(Exchange Online Protection\)](#)

## Transportregeln (Exchange Server)

# Verwenden von Nachrichtenflussregeln zum Umgehen von unwichtigen Elementen durch Nachrichten

18.12.2018 • 3 minutes to read

Wenn Sie darauf achten, dass Sie bestimmte Nachrichten erhalten möchten, können Sie eine Exchange Mail Flow Regel (auch bekannt als eine Transportregel) erstellen, die sichergestellt wird, dass diese Nachrichten Ordner Unübersichtlichkeit umgehen. Checken Sie weitere Informationen zu Unübersichtlichkeit [Verwendung Unübersichtlichkeit Nachrichten in Outlook niedriger Priorität sortiert](#).

Checken Sie weitere Verwaltungsaufgaben im Zusammenhang mit e-Mail-Flussregeln [e-Mail-Flussregeln \(Transportregeln\) in Exchange Online](#) und das [New-TransportRule PowerShell](#) Thema. Wenn Sie Exchange Online PowerShell noch nicht kennen, sehen Sie sich [mit Exchange Online PowerShell verbinden](#).

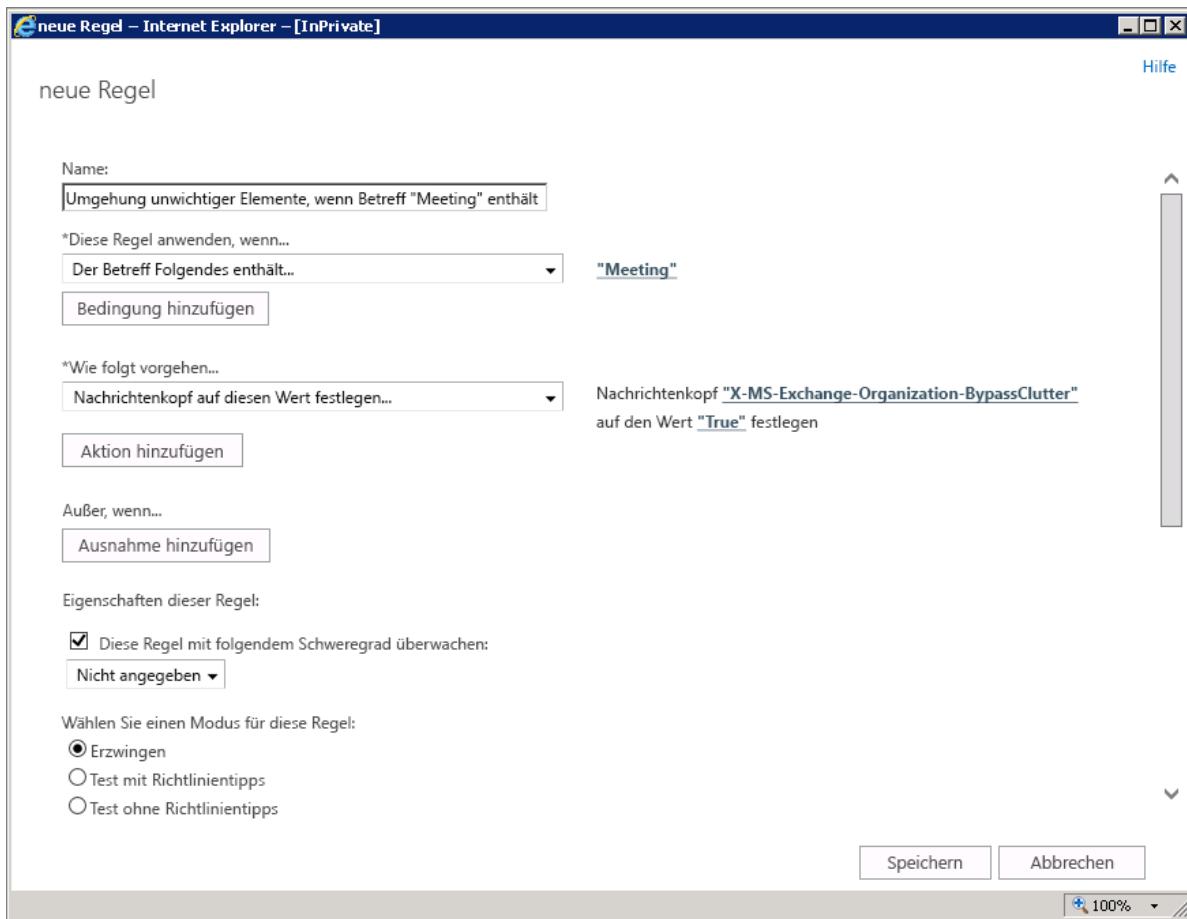
## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Transportregeln" im Thema [Berechtigungen für Messagingrichtlinien und -kompatibilität](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## Verwenden Sie die Exchange-Verwaltungskonsole zum Erstellen einer Mail Flow Regel für die Umgehung den Übersichtlichkeit-Ordner

In diesem Beispiel sind alle Nachrichten mit dem Titel „Meeting“ zulässig, um die unwichtigen Elemente zu umgehen.

1. Navigieren Sie im Exchange Administrationscenter (EAC) zu **Nachrichtenfluss > Regeln**. Klicken Sie auf **neu**  und wählen Sie dann auf **neue Regel erstellen**.



2. Nach Besprechungsende Erstellen einer neuen Regel, klicken Sie auf **Speichern**, um die Regel zu starten.

## Verwenden Sie zum Erstellen einer Mail Flow-Regel für das Umgehen des Ordners Unübersichtlichkeit Exchange Online PowerShell

In diesem Beispiel sind alle Nachrichten mit dem Titel „Meeting“ zulässig, um die unwichtigen Elemente zu umgehen.

```
New-TransportRule -Name "<Unique rule name>" -SubjectContainsWords "Meeting" -SetHeaderName "X-MS-Exchange-Organization-BypassClutter" -SetHeaderValue "true"
```

### IMPORTANT

In diesem Beispiel wird sowohl `X-MS-Exchange-Organization-BypassClutter` und `true` wird die Groß-/Kleinschreibung beachtet.

Detaillierte Informationen zur Syntax und den Parametern finden Sie unter [New-TransportRule](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Sie können die e-Mail-Nachrichtenheader zu sehen, ob die e-Mail-Nachrichten im Posteingang aufgrund der Unübersichtlichkeit Mail Flow Regel Zielseite sind umgehen überprüfen. Wählen Sie eine e-Mail-Nachricht von einem Postfach in Ihrer Organisation, die die Unübersichtlichkeit umgehen der e-Mail-Flussregel angewendet wurde. Sehen Sie sich die Kopfzeilen der Nachricht versehen und sollte die **X-MS-Exchange-Organization-BypassClutter: true** Kopfzeile. Dies bedeutet, dass die Umgehung funktionsfähig ist. Checken Sie die [Ansicht der Internet-Headerinformationen für eine e-Mail-Nachricht](#) Thema Informationen zur Suche nach die Kopfzeileninformationen.

**NOTE**

Kalenderelemente (akzeptierte, gesendete oder abgelehnt Besprechungen Benachrichtigungen) enthalten keine Kopfzeile sein. Wir arbeiten auf Erweitern der Funktionen von Unübersichtlichkeit zu diesen Kalenderelementen bald.

# Verwenden von Nachrichtenflussregeln zum Routen von E-Mails basierend auf einer Liste von Wörtern, Begriffen oder Mustern

18.12.2018 • 3 minutes to read

Mit denen die Benutzer Ihrer Organisation e-Mail-Richtlinien entsprechen, können Sie Exchange Mail Flow Regeln (auch als Transportregeln bezeichnet) verwenden, um zu bestimmen, wie e-Mail-Nachrichten mit bestimmten Wörtern oder Muster weitergeleitet wird. Für eine kleine Gruppe von Wörtern oder Ausdrücken können Sie die Exchange-Verwaltungskonsole (EAC) verwenden. Eine längere Liste möchten Sie möglicherweise Exchange Online PowerShell verwenden, um der Liste aus einer Textdatei zu lesen.

Wenn Ihre Organisation Verhinderung von Datenverlust (Data Loss Prevention, DLP) verwendet, finden Sie unter [Verhinderung von Datenverlust](#) weitere Optionen für die Identifizierung und das Routing von E-Mails mit vertraulichen Informationen.

## Beispiel 1: Verwenden einer kurzen Liste mit nicht zulässigen Wörtern

Wenn die Liste der Wörter oder Ausdrücke kurz ist, können Sie eine Regel mithilfe des Exchange Admin Centers erstellen. Wenn Sie z. B. sicherstellen möchten, dass keine E-Mails mit Schimpfwörtern oder mit falscher Schreibweise Ihres Unternehmensnamens, mit internen Akronymen oder Produktnamen gesendet werden, können Sie eine Regel erstellen, mit der solche Nachrichten blockiert werden und eine Benachrichtigung an den Absender geschickt wird. Beachten Sie, dass die Groß-/Kleinschreibung bei Wörtern, Ausdrücken und Mustern nicht berücksichtigt wird.

In diesem Beispiel werden Nachrichten mit häufig vorkommenden Tippfehlern blockiert.

The screenshot shows the 'Nachrichten mit internen Akronymen oder Produktnamen sperren' (Block messages with internal acronyms or product names) rule configuration in the Exchange Admin Center. The 'Name:' field contains 'Nachrichten mit internen Akronymen oder Produktnamen sperren'. Under 'Diese Regel anwenden, wenn...', the conditions are set to 'Der Empfänger befindet sich in... Außerhalb der Organisation' and 'Der Betreff oder Nachrichtentext enthält...' with the value '„microsoft“ oder „micrsoft“ oder „msoft“ oder „msft“'. A 'Bedingung hinzufügen' button is visible. In the 'Gehen Sie folgendermaßen vor...' section, the action is set to 'Nachricht mit Erklärung ablehnen...' with the reason '„Keine internen Akryome, Produktnamen oder Rechtschreibfehler in externer Kommunikation“'.

## Beispiel 2: Verwenden einer langen Liste mit nicht zulässigen Wörtern

Wenn die Liste der Wörter, Ausdrücke oder Muster lang ist, können Sie sie in eine Textdatei mit jedem Wort, Ausdruck oder Muster in einer eigenen Zeile platzieren. Mit Exchange Online PowerShell, lesen in der Liste der Schlüsselwörter in eine Variable, erstellen Sie eine e-Mail-Fluss-Regel, und weisen Sie die Variable mit den Schlüsselwörtern der e-Mail-Fluss regelbedingung. Das folgende Skript verwendet beispielsweise eine Liste von

Rechtschreibfehlern aus einer Datei namens C:\My Documents\misspelled\_companyname.txt.

```
$Keywords=Import-Content "C:\My Documents\misspelled_companyname.txt"
New-TransportRule -Name "Block messages with unacceptable words" -SubjectOrBodyContainsWords $Keywords -
SentToScope "NotInOrganization" -RejectMessageReasonText "Do not use internal acronyms, product names, or
misspellings in external communications."
```

## Verwenden von Ausdrücken und Mustern in der Textdatei

Die Textdatei kann reguläre Ausdrücke für Muster enthalten. Für diese Ausdrücke wird nicht zwischen Groß- und Kleinschreibung unterschieden. Allgemeine reguläre Ausdrücke umfassen Folgendes:

|:----|:----| | **Ausdruck | Übereinstimmungen**|| .| Ein beliebiges einzelnes Zeichen || \*| Alle zusätzlichen Zeichen || \d| Alle Dezimalzahl || [Zeichengruppe] | Ein beliebiges einzelnes Zeichen in *Zeichengruppe*. |

Diese Datei enthält beispielsweise die häufigsten falschen Schreibweisen von Microsoft.

```
[mn]sft
[mn]icrosft
[mn]icro soft
[mn].crosoft
```

Informationen zum Angeben von Mustern mithilfe von regulären Ausdrücken finden Sie unter [Referenz zu regulären Ausdrücken](#).

# Verwenden von Nachrichtenflussregeln zum automatischen Hinzufügen von Besprechungen zu Kalendern in Exchange Online

18.12.2018 • 10 minutes to read

Mit dem Feature Direkt in Kalender in Exchange Online können Administratoren Nachrichtenflussregeln (auch als Transportregeln bezeichnet) konfigurieren, die bestimmten Benutzern das Hinzufügen von Besprechungen zu Kalendern erlauben. Direkt in Kalender bietet die folgenden Vorteile:

- Das Ereignis wird automatisch zum Kalender des Empfängers hinzugefügt, ohne dass dieser eine Aktion ausführen muss. Wenn der Benutzer die Besprechungseinladung erhalten hat, steht sie in seinem Kalender.
- Der Absender erhält keine Abwesenheits- oder anderen unerwünschten Antwortnachrichten, die die Folge sind, wenn Besprechungsanfragen an eine große Anzahl von Empfängern gesendet werden.
- Die Teilnehmer sehen keine besprechungsbezogenen Nachrichten, es sei denn, die Besprechung wird abgesagt.

Direkt in Kalender erfordert zwei Nachrichtenflussregeln mit bestimmten Bedingungen und Aktionen. Diese Regeln werden in der folgenden Tabelle beschrieben:

REGELBESCHREIBUNG	BEDINGUNG	ACTION	KOMMENTARE
Diese Nachrichtenflussregel wandelt reguläre Besprechungseinladungen in Direkt in Kalender-Besprechungseinladungen um.	<b>Ist der Absender oder Absender &gt; ist diese Person</b> (der vom Parameter). Diese Bedingung identifiziert die Benutzer, die zum Senden von Direct in Kalender-Besprechungseinladungen berechtigt sind. Sie können zwar andere Bedingungen verwenden, das Einschränken der Einladungen nach Absender verhindert jedoch die nicht autorisierte Verwendung von Direct in Kalender-Besprechungseinladungen.	<b>Der Nachrichtenkopf auf diesen Wert festlegen</b> oder ändern die <b>Nachrichteneigenschaften &gt; einen Nachrichtenkopf festgelegt</b> (die Parameter <code>SetHeaderName</code> und <code>SetHeaderValue</code> ). Diese Aktion wird die <b>X-MS-Exchange-Organization-CalendarBooking-Response</b> Kopfzeile auf den Wert <code>Accept</code> . Andere gültige Werte sind <code>Tentative</code> und <code>Decline</code> .	Es wird empfohlen für die Verwendung dedizierter Postfächer (freigegebene Postfächer sind OK) zum Senden von Direct in Kalender-Besprechungseinladungen, da Alle Besprechungsanfragen dieser Absender Empfänger Kalender automatisch hinzugefügt werden soll. Die dedizierten Postfächer erfordern keine besonderen Berechtigungen zu Senden von Direct in Kalender-Besprechungseinladungen.

REGELBESCHREIBUNG	BEDINGUNG	AKTION	KOMMENTARE
Diese Nachrichtenflussregel verhindert, dass Direkt in Kalender-Besprechungseinladungen im Posteingang der Empfänger angezeigt werden.	Ist der Absender oder Absender > ist diese Person (der vom Parameter).	Der Nachrichtenkopf auf diesen Wert festlegen oder ändern die Nachrichteneigenschaften > einen Nachrichtenkopf festgelegt (die Parameter SetHeaderName und SetHeaderValue ). Diese Aktion wird die X-MS-Exchange-Organization-CalendarBooking-TriageAction Kopfzeile auf den Wert MoveToDeleteItems . Gültiger Wert ist None .	Technisch gesehen ist diese Regel optional (ohne sie werden Besprechungen weiterhin automatisch zu den Kalendern der Empfänger hinzugefügt). Beachten Sie, dass mit dieser Regel nicht die Anzeige von Nachrichten mit Besprechungsabsagen für Direkt in Kalender-Besprechungen im Posteingang der Empfänger verhindert wird.

Weitere Informationen zu Nachrichtenflussregeln finden Sie unter [Mail flow rules \(transport rules\) in Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 10 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Nachrichtenübermittlung" im Thema [Featureberechtigungen in Exchange Online](#).
- Die festgelegten Konten zum Senden von Direkt in Kalender-Besprechungseinladungen müssen vorhanden sein.
- Weitere Informationen zum Öffnen und Verwenden der Exchange-Verwaltungskonsole (EAC) finden Sie unter [Exchange Admin center in Exchange Online](#).
- Wie Sie mit Windows PowerShell eine Verbindung mit Exchange Online herstellen, können Sie unter [Herstellen einer Verbindung mit Exchange Online PowerShell](#) nachlesen.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden des Exchange-Verwaltungskonsole zum Erstellen von Direkt in Kalender-Nachrichtenflussregeln

1. Öffnen Sie das EAC, und wechseln Sie zu **Nachrichtenfluss > Regeln**.
2. Klicken Sie auf **Neu** (), und wählen Sie dann **Neue Regel erstellen** aus.
3. Klicken Sie auf der daraufhin geöffneten Seite **Neue Regel** auf **Weitere Optionen**.

new rule

Name:

\*Apply this rule if...

\*Do the following...

Properties of this rule:

Audit this rule with severity level:

Choose a mode for this rule:  
 Enforce  
 Test with Policy Tips  
 Test without Policy Tips

4. Konfigurieren Sie die folgenden zusätzlichen Einstellungen auf der Seite **Neue Regel**:

- **Name:** direkt zu Kalender-Antwort (oder einen beliebigen beschreibenden).
- **Wenn diese Regel anwenden > Der Absender > ist diese Person:** Wählen Sie einen oder mehrere Benutzer direkt an Kalender Besprechungsanfragen senden.
- **Gehen Sie folgendermaßen vor > Ändern die Nachrichteneigenschaften > einen Nachrichtenkopf festgelegt:** Geben Sie die folgenden Werte:
- **Nachrichtenkopf festlegen**
- **auf den Wert**

Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

new rule

Name:

\*Apply this rule if...

\*Do the following...  
 Set the message header X-MS-Exchange-Organization-CalendarBooking-Response to the value 'Accept'

Except if...

5. Zurück zur **E-Mail-Fluss > Regeln**, klicken Sie auf **neu** (neue Regel erstellen.
6. Klicken Sie auf der daraufhin geöffneten Seite **Neue Regel** auf **Weitere Optionen**.

new rule

Name:

\*Apply this rule if...

\*Do the following...

Properties of this rule:

Audit this rule with severity level:

Choose a mode for this rule:  
 Enforce  
 Test with Policy Tips  
 Test without Policy Tips

7. Konfigurieren Sie die folgenden zusätzlichen Einstellungen auf der Seite **Neue Regel**:

- **Name:** direkt zu Kalender Ursachenanalyse Aktion (oder einen beliebigen beschreibenden).
- **Wenn diese Regel anwenden > Der Absender > ist diese Person:** Wählen Sie die gleichen Benutzer wie in Schritt 3.
- **Gehen Sie folgendermaßen vor > Ändern die Nachrichteneigenschaften > einen Nachrichtenkopf festgelegt:** Geben Sie die folgenden Werte:
- **Nachrichtenkopf festlegen**
- **auf den Wert**

Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

new rule

Name:

\*Apply this rule if...

\*Do the following...  
 Set the message header ["X-MS-Exchange-Organization-CalendarBooking-TriageAction"](#) to the value ["MoveToDeleteItems"](#).

## Verwenden von Exchange Online PowerShell zum Erstellen von Direkt in Kalender-Nachrichtenflussregeln

1. Um die Nachrichtenflussregel zu erstellen, die reguläre Besprechungseinladungen in Direkt in Kalender-Besprechungseinladungen umwandelt, verwenden Sie die folgende Syntax:

```
New-TransportRule -Name "Direct to Calendar response" -From "<designated sender 1>","<designated sender 2>"...  
-SetHeaderName "X-MS-Exchange-Organization-CalendarBooking-Response" -SetHeaderValue Accept
```

<span data-ttu-id="3df55-171">In diesem Beispiel wird die Regel mit dem dedizierten Postfach namens „'Direkt in Kalender' Einladungen“ konfiguriert.</span><span class="sxs-lookup"><span data-stu-id="3df55-171">This example configures the rule using the dedicated mailbox named Direct to Calendar invites.</span></span>

```
New-TransportRule -Name "Direct to Calendar response" -From "Direct to Calendar invites" -SetHeaderName "X-MS-Exchange-Organization-CalendarBooking-Response" -SetHeaderValue Accept
```

2. Um die Nachrichtenflussregel zu erstellen, die verhindert, dass Direkt in Kalender-Besprechungseinladungen im Posteingang der Empfänger angezeigt werden, verwenden Sie die folgende Syntax:

```
New-TransportRule -Name "Direct to Calendar triage action" -From "<designated sender 1>","<designated sender 2>"... -SetHeaderName "X-MS-Exchange-Organization-CalendarBooking-TriageAction" -SetHeaderValue MoveToDeletedItems
```

<span data-ttu-id="3df55-173">In diesem Beispiel wird die Regel mit dem dedizierten Postfach namens „'Direkt in Kalender' Einladungen“ konfiguriert.</span><span class="sxs-lookup"><span data-stu-id="3df55-173">This example configures the rule using the dedicated mailbox named Direct to Calendar invites.</span></span>

```
New-TransportRule -Name "Direct to Calendar triage action" -From "Direct to Calendar invites" -SetHeaderName "X-MS-Exchange-Organization-CalendarBooking-TriageAction" -SetHeaderValue MoveToDeletedItems
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-TransportRule](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um die erfolgreiche Konfiguration von Direkt in Kalender-Besprechungseinladungen zu überprüfen, senden Sie unter Verwendung des Postfach des festgelegten Absenders eine Testbesprechungseinladung an eine kleine Anzahl von Empfängern. Überprüfen Sie, ob die Besprechung automatisch in den Kalendern der Empfängern angezeigt wird, und stellen Sie sicher, dass der Posteingang keine besprechungsbezogenen Nachrichten enthält (die zweite Regel sollte diese Nachrichten automatisch in den Ordner „Gelöschte Elemente“ verschieben).

## Weitere Informationen

- Das Postfach des festgelegten Absenders empfängt Antworten zur Besprechungsannahme für Direkt in Kalender-Besprechungen. Verwenden Sie die folgenden Strategien, um die Auswirkungen dieser Nachrichten auf den festgelegten Absender so weit wie möglich zu minimieren:
  - Aktivieren Sie in Outlook die Einstellungen **Verlaufsinformationen aktualisieren und dann Antworten ohne Kommentare löschen** und **Nach dem Aktualisieren der Verlaufsinformationen Bestätigungen verschieben nach: <Gelöschte Elemente>** unter **E-Mail > Verlauf** für das Postfach des festgelegten Absenders. Weitere Informationen finden Sie unter [Change how meeting requests, polls, and read or delivery receipts are processed](#).
  - Das Deaktivieren der Einstellung **Bitte um Antwort** in Direkt in Kalender-Besprechungseinladungen verhindert nicht, dass Antworten an das Postfach des festgelegten Absenders gesendet werden.
- Wenn das festgelegte Postfach eine Besprechungsabsage für eine Direkt in Kalender-Besprechung sendet, wird der Titel der abgesagten Besprechung immer in **ABGESAGT: <vorheriger Besprechungstitel>**

geändert, und die abgesagte Besprechung verbleibt in den Kalendern der Teilnehmer, bis diese sie manuell entfernen.

- Besprechungsabsagen für Direkt in Kalender-Besprechungen werden immer im Posteingang der Empfänger angezeigt.

# Verwalten von nachrichtengenehmigung in Exchange Online

18.12.2018 • 7 minutes to read

Manchmal ist es sinnvoll, eine Nachricht von einer zweiten Person überprüfen zu lassen (Vier-Augen-Prinzip), bevor sie zugestellt wird. Als Exchange-Administrator können Sie dies festlegen. Dieses Verfahren wird als Moderation bezeichnet, und die genehmigende Person ist der Moderator. Je nachdem, welche Nachrichten genehmigt werden müssen, können Sie zwei verschiedene Ansätze zugrunde legen:

- Ändern der Verteilergruppeneigenschaften
- Erstellen einer Nachrichtenflussregel

In diesem Artikel wird Folgendes erläutert:

- [Entscheiden, welche Vorgehensweise für die Genehmigung verwendet werden soll](#)
- [Funktionsweise des Genehmigungsvorgangs](#)

Informationen zum Implementieren gängiger Szenarien finden Sie unter [Gängige Szenarien der Nachrichtengenehmigung](#).

## Entscheiden, welche Vorgehensweise für die Genehmigung verwendet werden soll

Es folgt ein Vergleich der beiden Ansätze für die Nachrichtengenehmigung.

WAS MÖCHTEN SIE MACHEN?	ANSATZ	ERSTER SCHITT
Erstellen einer moderierten Verteilergruppe, wobei alle Nachrichten an die Gruppe moderiert werden müssen	Einrichten der Nachrichtengenehmigung für die Verteilergruppe	Wechseln Sie zu der Exchange-Verwaltungskonsole (EAC) > <b>Empfänger</b> > <b>Gruppen</b> , die Verteilergruppe zu bearbeiten, und wählen Sie <b>nachrichtengenehmigung</b> .
Festlegen, dass Nachrichten genehmigt werden müssen, die bestimmten Kriterien entsprechen oder an eine bestimmte Person gesendet werden	Erstellen Sie eine Transportregel mithilfe der Aktion <b>Die Nachricht zur Genehmigung weiterleiten</b> . Sie können Kriterien für Nachrichten angeben, wie beispielsweise Textmuster, Absender und Empfänger. Die Kriterien können auch Ausnahmen enthalten.	Navigieren Sie zum EAC > <b>Nachrichtenfluss</b> > <b>Regeln</b> .

## Funktionsweise des Genehmigungsvorgangs

Wenn jemand eine Nachricht an eine Person oder Gruppe, die genehmigt werden muss, sendet Wenn sie Outlook im Web (vormals Outlook Web App) verwenden, werden sie benachrichtigt, dass ihre Nachricht verzögert werden kann.

✉ SEND ✎ DISCARD ⌂ INSERT ⌂ APPS ⌂

● Messages sent to All Employees are moderated. They may be rejected or delayed. [Remove recipient](#)

● This message will be sent to 26 recipients. [Show details](#)

To:  All Employees

Cc: [+](#)

Subject: Company meeting

Der Moderator erhält eine E-Mail mit der Aufforderung, die Nachricht zu genehmigen oder abzulehnen. Die Nachricht enthält Schaltflächen, über die die Nachricht genehmigt oder abgelehnt werden kann, und die ursprüngliche Nachricht ist zur Überprüfung in der Anlage enthalten.

 Microsoft Exchange on behalf of Allie Bellew  
Tue 9/9/2014 9:57 AM

APPROVE  REJECT

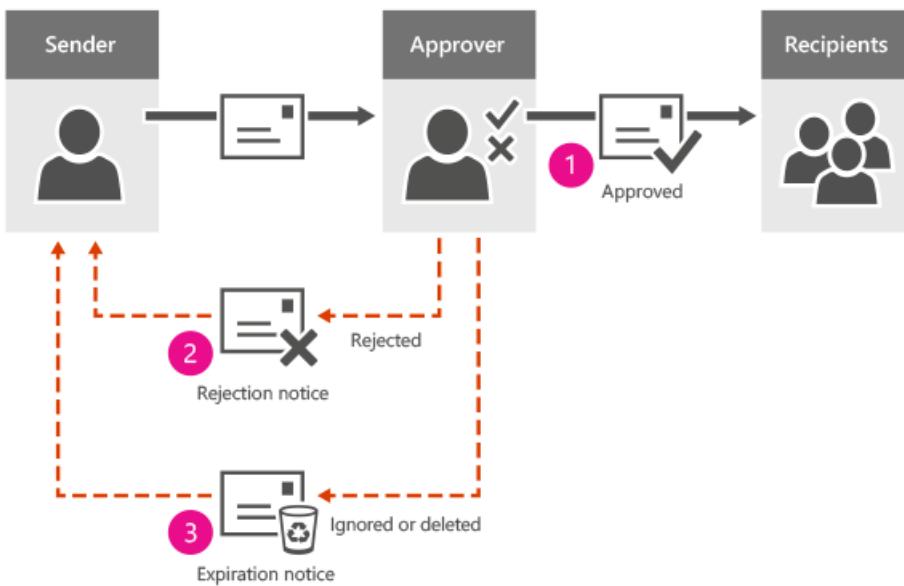
To:  Rob Young;  Bonnie Kearney;  
● Please respond.

✉ 1 attachment  
 Company meeting  
6 KB [...](#)

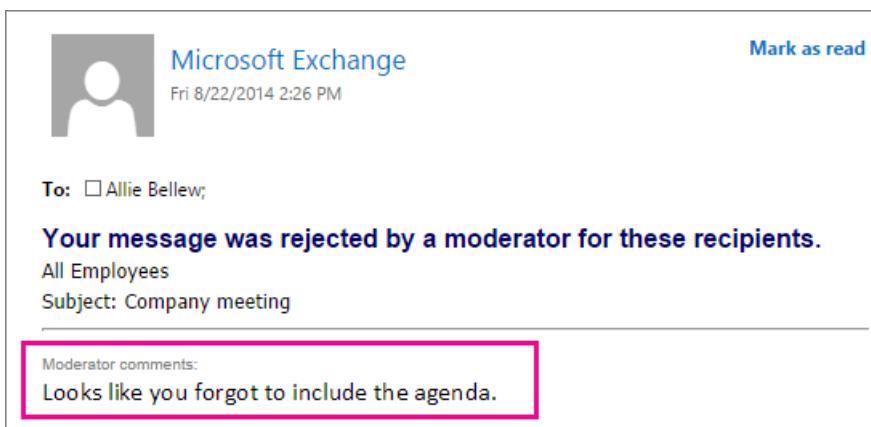
**Your decision is requested.**  
Allie Bellew has asked you to approve the attached message for delivery to:  
All Employees

A preview of the message is below. To view the complete message, open the attachment.

Der Moderator kann eine der drei folgenden Maßnahmen ergreifen:



1. Wenn die Nachricht genehmigt wurde, wird sie an die ursprünglich vorgesehenen Empfänger zugestellt.  
Der ursprüngliche Absender wird nicht benachrichtigt.
2. Wenn die Nachricht abgelehnt wurde, wird eine Ablehnungsnachricht an den Absender gesendet. Der Moderator kann eine Erklärung hinzufügen:



3. Wenn die genehmigenden Person löscht, oder die Genehmigungsnachricht ignoriert, wird eine Nachricht Ablauf an den Absender gesendet. In diesem Fall nach zwei Tagen im Exchange Online und nach fünf Tagen im Exchange Server. (In Exchange Server, können Sie in diesem Zeitraum ändern).

Die zur Genehmigung anstehende Nachricht wird vorübergehend in einem als Vermittlungspostfach bezeichneten Systempostfach gespeichert. Die ursprüngliche Nachricht wird so lange im Vermittlungspostfach aufbewahrt, bis der Moderator die Nachricht genehmigt oder ablehnt, die Genehmigungsnachricht löscht oder zulässt, dass die Genehmigungsnachricht abläuft.

## Fragen und Antworten

### **Welcher Unterschied besteht zwischen der genehmigenden Person und dem Besitzer einer Verteilergruppe?**

Der Besitzer einer Verteilergruppe ist verantwortlich für die Verwaltung der Gruppenmitgliedschaft Verteilung. Beispielsweise eine Person in IT möglicherweise der Besitzer einer Verteilergruppe aufgerufen werden alle Mitarbeiter, jedoch nur Leiter der Personalabteilung möglicherweise als Moderator eingerichtet werden. Darüber hinaus müssen Nachrichten, die der Besitzer an die Verteilergruppe sendet nicht von einem Moderator genehmigt werden.

## **Was geschieht, wenn der Moderator oder die genehmigende Person eine Nachricht an die Verteilergruppe sendet?**

Die Nachricht wird unter Umgehung des Genehmigungsvorgangs direkt an die Gruppe gesendet.

## **Was geschieht, wenn nur für einen Teil der Empfänger eine Genehmigung erforderlich ist?**

Sie können eine Nachricht an eine Gruppe von Empfängern senden, wenn nur für eine Teilmenge der Empfänger eine Genehmigung benötigt wird. Betrachten Sie beispielsweise eine Nachricht, die an 12 Empfänger gesendet wird, von denen einer eine moderierte Verteilergruppe ist. Die Nachricht wird automatisch in zwei Kopien aufgeteilt. Eine Nachricht wird sofort an die 11 Empfänger gesendet, für die keine Genehmigung erforderlich ist, während die zweite Nachricht an den Genehmigungsvorgang für die moderierte Verteilergruppe übermittelt wird. Ist eine Nachricht für mehrere moderierte Empfänger vorgesehen, wird automatisch eine separate Kopie der Nachricht für jeden moderierten Empfänger erstellt, und jede Kopie durchläuft den entsprechenden Genehmigungsvorgang.

## **Was muss ich tun, wenn meine Verteilergruppe moderierte Empfänger enthält, für die eine Genehmigung erforderlich ist?**

Eine Verteilergruppe kann moderierter Empfänger enthalten, die auch genehmigt werden müssen. In diesem Fall nachdem die Nachricht an die Verteilergruppe genehmigt wurde, tritt ein separater Genehmigungsprozess für jeden moderierter Empfänger, der Mitglied der Verteilergruppe ist. Jedoch können Sie auch die automatische Genehmigung für die Mitglieder der Verteilergruppe nach aktivieren die Nachricht an die moderierte Verteilergruppe genehmigt wird. Zu diesem Zweck verwenden Sie den Parameter *BypassNestedModerationEnabled* im Cmdlet [Set-DistributionGroup](#).

## **Ist das Verfahren ein anderes, wenn wir über unsere eigenen Exchange-Server verfügen?**

Standardmäßig wird für jede Exchange-Organisation ein Vermittlungspostfach verwendet. Wenn Sie über eigene Exchange-Server verfügen und für den Lastenausgleich weitere Vermittlungspostfächer benötigen, befolgen Sie die Anweisungen zum Hinzufügen von Vermittlungspostfächern unter [Verwalten und Problembearbeitung der Nachrichtengenehmigung](#). Vermittlungspostfächer sind Systempostfächer, für die keine Exchange-Lizenz erforderlich ist.

## **Benötigen Sie weitere Informationen?**

[Verwalten von Nachrichtenflussregeln](#)

[Exchange Online PowerShell](#)

# Gängige Szenarien der Nachrichtengenehmigung

18.12.2018 • 9 minutes to read

Möglicherweise benötigt Ihre Organisation bestimmte Arten von Nachrichten genehmigt werden, um die rechtlichen oder Compliance-Anforderungen erfüllen oder bestimmte Geschäftsworkflows implementieren. In diesem Artikel werden Beispiele für häufige Szenarien, in denen Sie mithilfe von Exchange einrichten können.

## Beispiel 1: Vermeiden eines Nachrichtenansturms auf eine große Verteilergruppe

Zum Steuern der Nachrichten, die an eine große Verteilergruppe gesendet werden, können Sie festlegen, dass ein Moderator die an diese Gruppe gesendeten Nachrichten genehmigen muss. Wenn keine Kriterien dafür angegeben wurden, welche Nachrichten genehmigt werden müssen, können Sie dies am einfachsten festlegen, indem Sie die Gruppe so konfigurieren, dass Nachrichten genehmigt werden müssen.

In diesem Beispiel müssen alle Nachrichten genehmigt werden, die an die Gruppe "All Employees" gesendet werden. Ausgenommen davon sind Absender, die Mitglieder der Verteilergruppe "Legal Team" sind.

The screenshot shows the 'All Employees' distribution group settings in the EAC. Under 'general ownership membership', there is a checked checkbox for 'Messages sent to this group have to be approved by a moderator'. Below this, under 'Group moderators:', there is a list box containing 'Bonnie Kearney' and 'Rob Young'. There are also '+' and '-' buttons to manage the list. Below the list, there is a section for 'Senders who don't require message approval:' which contains a list box for 'Legal Team'. There are also '+' and '-' buttons for this list. At the bottom, there is a section for 'Select moderation notifications:' with a list box containing 'None'.

Um festzulegen, dass an eine bestimmte Verteilergruppe gesendete Nachrichten genehmigt werden müssen, navigieren Sie im Exchange Admin Center (EAC) zu **Empfänger > Gruppen**, bearbeiten Sie die Verteilergruppe, und wählen Sie dann **Nachrichtengenehmigung** aus.

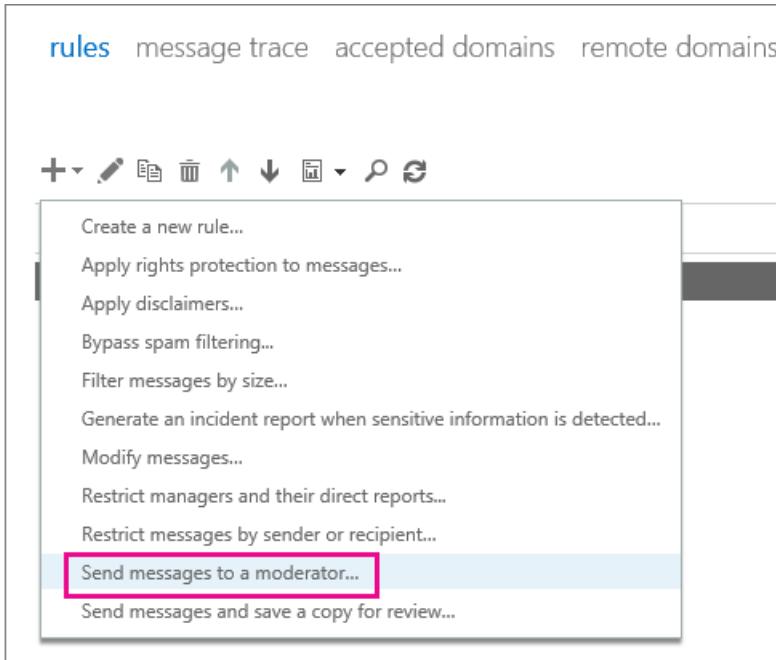
## Beispiel 2: Weiterleiten von Nachrichten zur Genehmigung an den Vorgesetzten eines Absenders

Im Folgenden sind einige gängige Nachrichtentypen aufgeführt, für die möglicherweise die Genehmigung des Vorgesetzten erforderlich ist:

- Von einem Benutzer an bestimmte Verteilergruppen oder Empfänger gesendete Nachrichten

- An externe Benutzer oder Partner gesendete Nachrichten
- Zwischen zwei Gruppen gesendete Nachrichten
- Gesendete Nachrichten mit bestimmten Inhalten, beispielsweise dem Namen eines bestimmten Kunden
- Von einem Praktikanten gesendete Nachrichten

Um festzulegen, dass eine Nachricht zur Genehmigung übermittelt werden muss, erstellen Sie zuerst eine Regel mithilfe der Vorlage **Nachrichten an einen Moderator senden**, und geben Sie dann an, dass die Nachrichten an den Vorgesetzten des Absenders geleitet werden müssen, wie in den folgenden Screenshots dargestellt.



Legen Sie anschließend fest, welche Nachrichten genehmigt werden müssen.

Hier finden Sie ein Beispiel, bei dem für alle von einem Praktikanten namens Garth Fort an Empfänger außerhalb der Organisation gesendeten Nachrichten die Genehmigung des Vorgesetzten erforderlich ist.

The screenshot shows the configuration of a rule named 'Review messages sent from trainee'. The 'Name:' field contains the name of the rule. Under the heading '\*Apply this rule if...', there are two conditions: 'The sender is...' set to 'Garth Fort' and 'The recipient is located...' set to 'Outside the organization'. Under the heading '\*Do the following...', there is one action: 'Forward to the sender's manager for approval'.

Navigieren Sie zuerst zum EAC > **Nachrichtenfluss** > **Regeln**, und erstellen Sie dann eine neue Regel mithilfe der Vorlage **Nachrichten an einen Moderator senden**.

#### IMPORTANT

Einige Bedingungen und Aktionen, einschließlich der Weiterleitung von Nachrichten an den Vorgesetzten des Absenders, sind auf der Seite **Neue Regel** standardmäßig ausgeblendet. Wählen Sie **Weitere Optionen** aus, um alle Bedingungen und Aktionen anzuzeigen.

## Beispiel 3: Einrichten einer Nachrichtengenehmigungskette

Sie können mehrere Genehmigungsstufen für Nachrichten festlegen. Beispielsweise können Sie festlegen, dass Nachrichten an einen bestimmten Kunden zuerst vom Kundenbeziehungs-Manager und danach von einem Compliance Officer genehmigt werden müssen. Oder Sie legen fest, dass Spesenabrechnungen von Vorgesetzten auf zwei Ebenen genehmigt werden müssen.

Erstellen Sie eine Transportregel für jede Genehmigungsstufe, um diesen Typ mehrstufiger Genehmigung zu erstellen. Jede Regel erkennt die gleichen Muster in den Nachrichten, wie nachfolgend erläutert:

- Die erste Regel leitet die Nachricht an die erste genehmigende Person weiter. Wenn die erste genehmigende Person die Nachricht akzeptiert, wird die Nachricht automatisch an die genehmigende Person in der zweiten Regel geleitet.
- Wenn alle genehmigenden Personen in der Kette bei Erhalt der Genehmigungsanforderung **Genehmigen** auswählen, wird die ursprüngliche Nachricht, nachdem die letzte Genehmigung in der Kette abgeschlossen wurde, an die vorgesehenen Empfänger gesendet.
- Wählt eine Person in der Genehmigungskette bei Erhalt der Genehmigungsanforderung **Ablehnen** aus, erhält der Absender eine Ablehnungsmeldung.
- Wenn keines der Genehmigung Anforderungen innerhalb der Ablaufzeit (2 Tage für Exchange Online, 5 Tage für Exchange Server) genehmigt werden nicht, erhält der Absender eine Nachricht Ablauf.

Im folgenden Beispiel wird davon ausgegangen, dass Sie einen Kunden namens Blue Yonder Airlines haben. Sowohl der Kundenbeziehungs-Manager als auch der Compliance Officer soll alle Nachrichten an diesen Kunden genehmigen. Sie erstellen zwei Regeln, eine für jede genehmigende Person. Die erste Regel ist für die genehmigende Person der ersten Stufe. Die zweite Regel ist für die genehmigende Person der zweiten Stufe.

ON	RULE	PRIORITY
<input checked="" type="checkbox"/>	Blue Yonder Airlines: Approval #1 Relationship Manager	0
<input checked="" type="checkbox"/>	Blue Yonder Airlines: Approval #2 Compliance Manager	1

Die erste Regel ermittelt alle Nachrichten, bei denen der Firmenname Blue Yonder Airlines im Betreff oder im Nachrichtentext enthalten ist, und sendet diese Nachrichten dann an den internen Kundenbeziehungs-Manager für Blue Yonder Airlines, Garret Vargas.

## Blue Yonder Airlines: Approval #1 Relationship Manager

Name:

\*Apply this rule if...

The sender is located... [Inside the organization](#)

and

The subject or body matches... ['B.Y.A.' or 'BYA' or 'Blue Yonder Airlines' or 'Blue Yonder'](#)

[add condition](#)

\*Do the following...

['Garret Vargas'](#)

[add action](#)

Die zweite Regel sendet diese Nachrichten an den Compliance Officer Tony Krijnen.

Blue Yonder Airlines: Approval #2 Compliance Manager 2

Name:

\*Apply this rule if...

The sender is located... [Inside the organization](#)

and

The subject or body matches... ['B.Y.A.' or 'BYA' or 'Blue Yonder Airlines' or 'Blue Yonder'](#)

[add condition](#)

\*Do the following...

['Tony Krijnen'](#)

[add action](#)

## Beispiel 4: Weiterleiten von Nachrichten, die eines von mehreren Kriterien erfüllen

Innerhalb einer Transportregel müssen alle in der Regel konfigurierten Bedingungen zutreffen, damit die Regel erfüllt ist. Wenn die gleichen Aktionen einzelnen Bedingungen zugeordnet werden sollen, müssen Sie für jede eine eigene Regel erstellen.

Erstellen Sie hierzu im EAC auf der Seite **Regeln** eine Regel für die erste Bedingung. Wählen Sie dann die Regel aus, wählen Sie **Kopieren** aus, und ändern Sie die Bedingungen in der neuen Regel, sodass sie mit der zweiten Bedingung übereinstimmen.

Gehen Sie sorgfältig vor, wenn Sie mehrere Regeln mit Bedingungen vom Typ ODER erstellen, damit eine Nachricht nicht letztlich mehrere Male an die genehmigende Person gesendet wird. Um dies zu vermeiden, fügen Sie der zweiten Regel eine Ausnahme hinzu, sodass Nachrichten ignoriert werden, die die Bedingungen in der ersten Regel erfüllen.

Beispiel: Mit einer einzelnen Regel kann nicht geprüft werden, ob in einer Nachricht der Text "Verkaufsangebot" im Betreff vorkommt oder der Titel der Anlage ist. Damit die Nachricht nicht mehrmals an die genehmigende Person gesendet wird, ist Folgendes erforderlich: Wenn die erste Regel prüft, ob der Text "Verkaufsangebot" im

Betreff oder im Nachrichtentext enthalten ist, wird für die zweite Regel, die prüft, ob der Text "Verkaufsangebot" in der Anlage vorkommt, eine Ausnahme benötigt, die die Kriterien der ersten Regel enthält.

Sales quote appoval: Rule 2

Name:

\*Apply this rule if...  
 ['Sales quote'](#)

\*Do the following...

Except if...  
  ['Sales quote'](#)

**NOTE**

Ausnahmen werden standardmäßig auf der Seite **Neue Regel** ausgeblendet. Wählen Sie **Weitere Optionen** aus, um alle Bedingungen und Aktionen anzuzeigen.

## Beispiel 5: Weiterleiten einer Nachricht, die vertrauliche Informationen enthält

Wenn Sie über das Feature [Verhinderung von Datenverlust](#) (DLP) verfügen, sind zahlreiche vertrauliche Informationstypen vordefiniert. Bei Verwendung von DLP wird Ihnen angezeigt, dass die Nachricht eine Bedingung für vertrauliche Informationen enthält. Unabhängig davon, ob Sie über DLP verfügen oder nicht, können Sie Bedingungen erstellen, die bestimmte vertrauliche Informationsmuster ausschließlich für Ihre Organisation ermitteln.

Hier finden Sie ein Beispiel, bei dem Nachrichten mit vertraulichen Informationen genehmigt werden müssen. In diesem Beispiel müssen Nachrichten genehmigt werden, die eine Kreditkartennummer enthalten.

new rule

Name:

\*Apply this rule if...  
 ['Credit Card Number'](#)

\*Do the following...

## See also

## Verwalten der Nachrichtengenehmigung

# Wiederherstellbare Elemente Ordner in Exchange Online

18.12.2018 • 19 minutes to read

Zum Schutz vor versehentlichen oder böswilligen Löschvorgängen verwenden Suche nach Daten zur häufig durchgeführten vor oder während Rechtsstreitigkeiten oder Untersuchungen zu erleichtern Exchange Online und "wiederherstellbare Elemente". Ordner "wiederherstellbare Elemente" ersetzt die Funktion, die als bezeichnet wurde *die Dumpster* in früheren Versionen von Exchange. Die folgenden Exchange-Features Verwenden des Ordners wiederherstellbare Elemente:

- Aufbewahrungszeit für gelöschte Elemente
- Wiederherstellung einzelner Elemente
- Compliance-Archiv
- Aufbewahrung für eventuelle Rechtsstreitigkeiten
- eDiscovery-Archiv
- Office 365-Aufbewahrungsrichtlinien
- Postfachüberwachungsprotokollierung
- Kalenderprotokollierung

## Terminologie

Sie sollten die folgenden Begriffe kennen, um den Inhalt in diesem Thema verstehen zu können.

### **Löschen**

Beschreibt den Vorgang, bei dem ein Element aus einem Ordner gelöscht und im Standardordner "Gelöschte Elemente" platziert wird.

### **Vorläufig löschen**

Beschreibt den Vorgang, bei dem ein Element aus dem Ordner „Gelöschte Elemente“ gelöscht und im Standardordner „Wiederherstellbare Elemente“ platziert wird. Beschreibt außerdem den Vorgang, bei dem ein Benutzer von Outlook ein Element durch Drücken von UMSCHALT+ENTF löscht, wodurch der Ordner „Gelöschte Elemente“ umgangen und das Element direkt im Ordner „Wiederherstellbare Elemente“ platziert wird.

### **Dauerhaft löschen**

Beschreibt, wenn ein Element aus der Postfachdatenbank geleert, markiert ist. Dies ist auch bekannt als einer *harte Informationsspeicher zu löschen*.

## Ordner „Wiederherstellbare Elemente“

Jedes Benutzerpostfach ist in zwei Unterstrukturen unterteilt: die Unterstruktur IPM (zwischen Personen messaging), die enthält die normale, sichtbare Ordner wie Posteingang, Kalender und gesendete Objekte und der IPM-Unterstruktur, die interne Daten, Einstellungen und andere enthält operative Daten über das Postfach. Ordner "wiederherstellbare Elemente" befindet sich in der IPM Unterstruktur der einzelnen Postfächer. Diese Teilstruktur ist nicht für Benutzer mit Outlook, Outlook im Web (vormals Outlook Web App) oder anderen e-Mail-Clients

angezeigt.

Durch diese Änderung der Architektur ergeben sich die folgenden Vorteile:

- Wird ein Postfach in eine andere Postfachdatenbank verschoben, wird der Ordner "Wiederherstellbare Elemente" ebenfalls verschoben.
- Ordner "wiederherstellbare Elemente" wird von der Exchange-Suche indiziert und mithilfe von Compliance-eDiscovery oder Content-Suche in der Office 365-Sicherheit und Compliance Center ermittelt werden kann.
- Der Ordner "Wiederherstellbare Elemente" besitzt ein eigenes Speichercontingent.
- Exchange kann verhindern, dass Daten aus dem Ordner "Wiederherstellbare Elemente" dauerhaft gelöscht werden.
- Exchange kann Bearbeitungsvorgänge für bestimmte Inhalte nachverfolgen.

Der Ordner "Wiederherstellbare Elemente" enthält die folgenden Unterordner:

- **Löschvorgänge:** Dieser Unterordner enthält alle Elemente aus dem Ordner Gelöschte Elemente gelöscht. (In Outlook kann ein Benutzer löschen welche ein Element durch Drücken von UMSCHALT + ENTF.) In diesem Unterordner steht Benutzern über das Feature gelöschte Elemente wiederherstellen in Outlook und Outlook im Web.
- **Versionen:** Compliance-Archiv, Aufbewahrung für eventuelle Rechtsstreitigkeiten oder einer Aufbewahrungsrichtlinie für Office 365 aktiviert ist, wird dieser Unterordner enthält die ursprünglichen und geänderten Kopien der gelöschten Elemente. Dieser Ordner ist nicht sichtbar für Endbenutzer.
- **Löscht ein:** Aufbewahrung für eventuelle Rechtsstreitigkeiten oder Wiederherstellung einzelner Elemente aktiviert ist, wird dieser Unterordner enthält alle Elemente, die schwerer gelöscht werden. Dieser Ordner ist nicht sichtbar für Endbenutzer.
- **Überwachungen:** Wenn postfachüberwachungsprotokollierung Protokollierung für ein Postfach aktiviert ist, werden diesem Unterordner enthält die Überwachungsprotokolleinträge. Dass weitere Informationen zum Postfach-überwachungsprotokollierung finden Sie unter [Export Postfach Überwachungsprotokolle im Exchange Online](#).
- **DiscoveryHolds:** Wenn Compliance-Archiv aktiviert ist oder wenn eine Aufbewahrungsrichtlinie für Office 365 an das Postfach zugewiesen ist, enthält dieser Unterordner aller Objekte, die die Abfrageparameter halten und die Festplatte gelöscht sind entsprechen.
- **Protokollierung Kalender:** diesem Unterordner enthält Änderungen der Kalender, die innerhalb eines Postfachs auftreten. Dieser Ordner ist nicht für Benutzer verfügbar.

Die folgende Abbildung zeigt die Unterordner in den Ordnern "Wiederherstellbare Elemente" Außerdem zeigt die Abbildung die Workflowprozesse der Aufbewahrung gelöschter Elemente, Wiederherstellung einzelner Elemente und Archivierung, die in den folgenden Abschnitten beschrieben werden.



### Aufbewahrungszeit für gelöschte Elemente

In folgenden Fällen gilt ein Element als vorläufig gelöscht:

- Ein Benutzer löscht ein Element oder leert alle Elemente aus dem Ordner "Gelöschte Elemente".
- Ein Benutzer drückt UMSCHALT+ENTF, um ein Element aus einem anderen Postfachordner zu löschen.

Vorübergehend gelöschte Elemente werden in den Unterordner "Löschvorgänge" des Ordners "Wiederherstellbare Elemente" verschoben. Dies bietet zusätzliche Sicherheit, sodass Benutzer gelöschte Elemente wiederherstellen können, ohne den Helpdesk konsultieren zu müssen. Benutzer können das Feature "Gelöschte

Elemente wiederherstellen" in Outlook oder Outlook im Web verwenden, um ein gelöschtes Element wiederherzustellen. Benutzer können dieses Feature auch verwenden, um ein Element dauerhaft zu löschen. Weitere Informationen finden Sie unter:

- [Wiederherstellen gelöschter Elemente in Outlook 2013 oder Outlook 2016](#)
- [Wiederherstellen gelöschter Elemente oder E-Mails in Outlook im Web](#)

Elemente verbleiben im Unterordner "löschen", bis die Aufbewahrungszeit für gelöschte erreicht wird. Die Aufbewahrungszeit für gelöschte Standard für eine Postfachdatenbank ist 14 Tage. Sie können diesen Zeitraum für Postfächer bis maximal 30 Tage zu ändern. Zusätzlich zu einer Aufbewahrungszeit unterliegt "wiederherstellbare Elemente" auch Kontingente. Finden Sie weitere Informationen finden Sie weiter unten in diesem Thema unter [Postfachkontingente wiederherstellbare Elemente](#).

Nach Ablauf die Aufbewahrungszeit für gelöschte das Element wird in den Ordner Benutzerkontenverwaltung verschoben und ist nicht mehr für den Benutzer sichtbar. Wenn die verwaltete Ordner-Assistent (mehrstufiger Authentifizierung das) das Postfach verarbeitet, werden Objekte im Unterordner Benutzerkontenverwaltung aus Exchange Online gelöscht.

### **Wiederherstellung einzelner Elemente**

Wenn ein Element aus dem Löschvorgänge Unterordner, entweder von einem Benutzer das Element löschen, indem das Feature gelöschte Elemente wiederherstellen oder ein automatisierter Prozess wie Assistenten für verwaltete Ordner, entfernt wird werden nicht vom Benutzer das Element wiederhergestellt. Beim Assistenten für verwaltete Ordner "wiederherstellbare Elemente" für ein Postfach, die Wiederherstellung einzelner Elemente aktiviert hat verarbeitet, wird keines Element im Unterordner "bereinigt" gelöscht, wenn die Aufbewahrungszeit für gelöschte Elemente für dieses Element abgelaufen ist. Dies bedeutet, dass ein Administrator das Element mit einer eDiscovery-Tool wie In-Place eDiscovery oder Inhaltssuche jedoch nach wie vor wiederherstellen kann.

In der folgenden Tabelle sind die Inhalte und Aktionen aufgelistet, die im Ordner "Wiederherstellbare Elemente" durchgeführt werden können, wenn die Wiederherstellung einzelner Elemente aktiviert ist.

### **Ordner "Wiederherstellbare Elemente" und Wiederherstellung einzelner Elemente**

STATUS DER WIEDERHERSTELLUNG EINZELNER ELEMENTE	DER ORDNER "WIEDERHERSTELLBARE ELEMENTE" ENTHÄLT VORÜBERGEHEND GELÖSCHTE ELEMENTE	DER ORDNER "WIEDERHERSTELLBARE ELEMENTE" ENTHÄLT DAUERHAFT GELÖSCHTE ELEMENTE	DIE BENUTZER KÖNNEN ELEMENTE IM ORDNER "WIEDERHERSTELLBARE ELEMENTE" DAUERHAFT LÖSCHEN	DER ASSISTENT FÜR VERWALTETE ORDNER LÖSCHT ELEMENTE AUTOMATISCH DAUERHAFT AUS DEM ORDNER "WIEDERHERSTELLBARE ELEMENTE"
Aktiviert	Ja	Ja	Nein	Ja. Standardmäßig werden alle Elemente nach 14 Tagen dauerhaft gelöscht, mit Ausnahme von Kalendereinträgen, die nach 120 Tagen dauerhaft gelöscht werden.

STATUS DER WIEDERHERSTELLUNG EINZELNER ELEMENTE	DER ORDNER "WIEDERHERSTELLBARE ELEMENTE" ENTHÄLT VORÜBERGEHEND GELÖSCHTE ELEMENTE	DER ORDNER "WIEDERHERSTELLBARE ELEMENTE" ENTHÄLT DAUERHAFT GELÖSCHTE ELEMENTE	DIE BENUTZER KÖNNEN ELEMENTE IM ORDNER "WIEDERHERSTELLBARE ELEMENTE" DAUERHAFT LÖSCHEN	DER ASSISTENT FÜR VERWALTETE ORDNER LÖSCHT ELEMENTE AUTOMATISCH DAUERHAFT AUS DEM ORDNER "WIEDERHERSTELLBARE ELEMENTE"
Deaktiviert	Ja	Nein	Ja	Ja. Standardmäßig werden alle Elemente nach 14 Tagen dauerhaft gelöscht, mit Ausnahme von Kalendereinträgen, die nach 120 Tagen dauerhaft gelöscht werden. Wenn der Warngrenzwert für "Wiederherstellbare Elemente" vor Ablauf der Aufbewahrungszeit für gelöschte Elemente erreicht wird, werden Nachrichten nach der FIFO-Methode (First In, First Out) gelöscht, d. h. nach der Reihenfolge, in der sie im Ordner gespeichert wurden.

### In-Situ-Speicher und Beweissicherungsverfahren

In Exchange Online können Discovery-Managern Compliance-eDiscovery mit delegierten Berechtigungen für [Discoveryverwaltung](#) Sie eDiscovery-Suchen von Inhalt von Postfächern ausführen. In Exchange Online können Sie Compliance-Archiv verwenden Postfachelemente beibehalten, die Abfrageparameter übereinstimmen und schützen Sie die Elemente vor Löschung durch Benutzer oder automatisierte Prozesse. Sie können auch Aufbewahrung für eventuelle Rechtsstreitigkeiten beibehalten aller Elemente in Benutzerpostfächern und schützen Sie die Elemente vor Löschung durch Benutzer oder automatisierte Prozesse.

Platzieren eines Postfachs auf Compliance-Archiv oder Aufbewahrung für eventuelle Rechtsstreitigkeiten beendet den Assistenten für verwaltete Ordner aus automatisch löschen von Nachrichten aus den Unterordnern DiscoveryHolds und bereinigt. Kopie bei Schreibvorgang Seitenschutz ist darüber hinaus auch für das Postfach aktiviert. Kopie bei Schreibvorgang Seite Protection erstellt eine Kopie des ursprünglichen Elements, bevor Modifikationen geschrieben werden auf dem Exchange-Speicher. Nachdem das Postfach aus dem Haltebereich entfernt wurde, fortgesetzt Assistenten für verwaltete Ordner automatische Löschung.

#### NOTE

Wenn Sie ein Postfach auf Compliance-Archiv und Aufbewahrung für eventuelle Rechtsstreitigkeiten versetzen, dauert Aufbewahrung für eventuelle Rechtsstreitigkeiten Option Sie bevorzugen, da dadurch das gesamte Postfach gehalten wird.

In der folgenden Tabelle sind die Inhalte und Aktionen aufgelistet, die im Ordner "Wiederherstellbare Elemente" durchgeführt werden können, wenn die Aufbewahrung für das Beweissicherungsverfahren aktiviert ist.

### Ordner "Wiederherstellbare Elemente" und Archive

STATUS DER AUFBEWAHRUNG	DER ORDNER "WIEDERHERSTELLBARE ELEMENTE" ENTHÄLT VORÜBERGEHEND GELÖSCHTE ELEMENTE	DER ORDNER "WIEDERHERSTELLBARE ELEMENTE" ENTHÄLT GEÄNDERTE UND DAUERHAFT GELÖSCHTE ELEMENTE	DIE BENUTZER KÖNNEN ELEMENTE IM ORDNER "WIEDERHERSTELLBARE ELEMENTE" DAUERHAFT LÖSCHEN	DER ASSISTENT FÜR VERWALTETE ORDNER LÖSCHT ELEMENTE AUTOMATISCH DAUERHAFT AUS DEM ORDNER "WIEDERHERSTELLBARE ELEMENTE"
Aktiviert	Ja	Ja	Nein	Nein
Deaktiviert	Ja	Nein	Ja	Ja

Weitere Informationen zur Compliance-eDiscovery, zum Compliance-Archiv und zum Beweissicherungsverfahren finden Sie in den folgenden Themen:

- [Compliance-eDiscovery in Exchange Online](#)
- [Compliance-Archiv und Aufbewahrung für eventuelle Archiv in Exchange Online](#)

### Schutz durch Kopie bei Schreibvorgang und geänderte Elemente

Nimmt ein Benutzer, für den das Compliance-Archiv oder das Beweissicherungsverfahren aktiviert ist, Änderungen an bestimmten Eigenschaften eines Postfachelements vor, wird vor dem Schreiben des geänderten Elements eine Kopie des ursprünglichen Postfachelements erstellt. Die ursprüngliche Kopie wird im Ordner "Versionen" gespeichert. Dieser Prozess ist als *Schutz durch Kopie bei Schreibvorgang* bezeichnet. Der Schutz durch Kopie bei Schreibvorgang gilt für Elemente, die sich in einem beliebigen Postfachordner befinden. Der Ordner "Versionen" ist für Benutzer nicht sichtbar.

In der folgenden Tabelle sind die Nachrichteneigenschaften aufgelistet, die den Schutz durch Kopie bei Schreibvorgang auslösen.

### Eigenschaften, die den Schutz durch Kopie bei Schreibvorgang auslösen

ELEMENTTYP	EIGENSCHAFTEN, DIE DEN SCHUTZ DURCH KOPIE BEI SCHREIBVORGANG AUSLÖSEN
Nachrichten (IPM.Note*)	<ul style="list-style-type: none"> <li>• Betreff</li> <li>• Textkörper</li> <li>• Anlagen</li> <li>• Absender und Empfänger</li> <li>• Gesendet und Empfangen von Datumsangaben</li> </ul>
Beiträge (IPM.Post*)	
Andere Elemente als Nachrichten und Beiträge	Jede Änderung an einer sichtbaren Eigenschaft mit folgenden Ausnahmen: <ul style="list-style-type: none"> <li>• Speicherort des Elements (wenn ein Element zwischen Ordnern verschoben wird)</li> <li>• Änderung des Elements (gelesen oder ungelesen)</li> <li>• Änderungen an einer zu einem Element zugewiesenen Aufbewahrungstag</li> </ul>
Elemente im Standardordner "Entwürfe"	Keine. Elemente im Ordner "Entwürfe" sind von dem Schutz durch Kopie bei Schreibvorgang ausgenommen.

#### IMPORTANT

Beim Schutz durch Kopie bei Schreibvorgang wird keine Version einer Besprechung gespeichert, wenn der Organisator einer Besprechung Antworten von Teilnehmern enthält und die Überwachungsinformationen der Besprechung aktualisiert werden. Auch Änderungen an RSS-Feeds werden nicht vom Kopie-bei-Schreibvorgang-Schutz erfasst.

Wenn ein Postfach nicht mehr auf Compliance-Archiv oder Aufbewahrung für eventuelle Rechtsstreitigkeiten ist, werden Kopien der geänderten Elemente im Versionsordner gespeichert entfernt.

## Postfachkontingente für "Wiederherstellbare Elemente"

Wenn ein Element in den Ordner wiederherstellbare Elemente verschoben wird, ist die Größe von Postfachkontingent abgezogen und die Größe des Ordners "wiederherstellbare Elemente" hinzugefügt. In Exchange Online werden die vorgegebenen Grenzwerte für das Kontingent wiederherstellbare Elemente: Weiche maximal 20 GB und einer harte Grenze von 30 GB. Allerdings werden die Kontingente für den Ordner wiederherstellbare Elemente automatisch auf 90 und 100 GB, die jeweils erhöht beim Platzieren eines Postfachs Beweissicherungsverfahren oder Compliance-Archiv oder wenn eine Office 365-Aufbewahrungsrichtlinie auf das Postfach angewendet wird.

Erreicht der Ordner "Wiederherstellbare Elemente" für ein Postfach das Kontingent für wiederherstellbare Elemente, können keine weiteren Elemente im Ordner gespeichert werden. Dies hat folgende Auswirkungen auf die Postfachfunktionen:

- Postfachbenutzer können keine Elemente löschen.
- Der Assistent für verwaltete Ordner kann keine Elemente auf der Grundlage von Aufbewahrungstags oder Einstellungen für verwaltete Ordner löschen.
- Bei Postfächern, für die die Wiederherstellung einzelner Elemente, das Compliance-Archiv oder das Beweissicherungsverfahren aktiviert ist, kann der Prozess zum Schutz durch Kopie bei Schreibschutz keine Versionen von Elementen verwalten, die vom Benutzer bearbeitet wurden.
- Bei Postfächern, für die die Postfachüberwachungsprotokollierung aktiviert ist, können keine Postfachüberwachungsprotokolle im Unterordner "Überwachungen" gespeichert werden.

Bei Postfächern, für die der In-Situ-Speicher oder das Beweissicherungsverfahren nicht aktiviert ist, löscht der Assistent für verwaltete Ordner die Elemente aus dem Ordner „Wiederherstellbare Elemente“ bei Ablauf der Aufbewahrungszeit für gelöschte Elemente automatisch. Wenn der Ordner den Warnwert für wiederherstellbare Elemente erreicht, löscht der Assistent Elemente automatisch nach dem FIFO-Verfahren.

Wenn das Postfach auf Compliance-Archiv oder Aufbewahrung für eventuelle Rechtsstreitigkeiten platziert oder um eine Aufbewahrungsrichtlinie für Office 365 zugeordnet ist, kann nicht Kopie bei Schreibvorgang Seite Protection Versionen geänderter Objekte verwalten. Um Versionen geänderter Objekte zu verwalten, müssen Sie die Größe des Ordners wiederherstellbare Elemente zu reduzieren. Sie können verwenden Sie das Cmdlet [Search-Mailbox](#) beim Kopieren von Nachrichten aus dem Ordner wiederherstellbare Elemente eines Postfachs in ein discoverypostfach, und klicken Sie dann die Elemente aus dem Postfach löschen. Alternativ können Sie auch das Kontingent wiederherstellbare Elemente für das Postfach auslösen. Weitere Informationen hierzu finden Sie unter [bereinigen oder Delete Elemente aus dem Ordner wiederherstellbare Elemente](#).

## Weitere Informationen

- Die Kopie-bei-Schreibvorgang-Funktion ist nur dann aktiviert, wenn für ein Postfach das Compliance-Archiv oder das Beweissicherungsverfahren aktiviert ist.
- Sollte ein Benutzer gelöschte Elemente aus dem Ordner "Wiederherstellbare Elemente" wiederherstellen müssen, verweisen Sie ihn auf die folgenden Themen:
  - [Wiederherstellen gelöschter Elemente in Outlook für Windows](#)
  - [Wiederherstellen gelöschter Elemente oder E-Mails in Outlook im Web](#)

# Bereinigen oder Löschen von Elementen aus dem Ordner wiederherstellbare Elemente im Exchange Online

18.12.2018 • 5 minutes to read

Ordner "wiederherstellbare Elemente" (in früheren Versionen von Exchange als bekannte *die Dumpster*) vorhanden ist, zum Schutz vor versehentlichen oder böswilligen Löschvorgängen und Suche nach Daten zur häufig durchgeführten vor oder während Rechtsstreitigkeiten oder Untersuchungen zu erleichtern.

Wie bereinigen oder Löschen von Elementen aus eines Benutzers wiederherstellbare Elemente Ordner abhängig, ob das Postfach gebracht Compliance-Archiv oder Aufbewahrung für eventuelle Rechtsstreitigkeiten oder hatte Wiederherstellung einzelner Elemente aktiviert:

- Wenn ein Postfach ist nicht für Compliance-Archiv oder Aufbewahrung für eventuelle Rechtsstreitigkeiten oder anderen Typen von Haltestatus in Office 365 platziert, oder wenn ein Postfach Wiederherstellung einzelner Elemente aktiviert hat, Sie einfach können Löschen von Elementen aus dem Ordner wiederherstellbare Elemente. Nachdem Elemente gelöscht werden, können Sie die Wiederherstellung einzelner Elemente zum wiederherstellbar verwenden.
- Elementwiederherstellung ist deaktiviert, wenn das Postfach für Compliance-Archiv oder Aufbewahrung für eventuelle Rechtsstreitigkeiten oder anderen Typen von Haltestatus in Office 365 platziert wird oder wenn die Wiederherstellung einzelner Elemente aktiviert ist, Sie die Postfachdaten beizubehalten sollten, bis die Sperre entfernt oder einzelne ist. In diesem Fall müssen Sie weitere detaillierte Schritte zum Bereinigen des Ordners wiederherstellbare Elemente ausführen.

Weitere Informationen zu Compliance-Archiv und Aufbewahrung für eventuelle Rechtsstreitigkeiten finden Sie unter [Compliance-Archiv und Aufbewahrung für eventuelle Rechtsstreitigkeiten in Exchange Online](#). Weitere Informationen zum Wiederherstellung einzelner Elemente finden Sie unter [Wiederherstellung einzelner Elemente](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Standardmäßig ist nicht die Postfach Import/Export-Rolle alle Rollengruppen in Exchange Online zugewiesen. Wenn Sie keine Cmdlets verwenden, die Postfach Import/Export-Rolle erforderlich, müssen Sie die Rolle zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie unter [Manage Role Gruppen in Exchange Online](#)
- Da falsch Bereinigen des Ordners wiederherstellbare Elemente Datenverlusten führen kann, ist es wichtig, dass Sie mit dem Ordner "wiederherstellbare Elemente" und die Auswirkungen des Entfernen von seinen Inhalt vertraut sind. Bevor Sie dieses Verfahren durchführen, wird empfohlen, dass Sie die Informationen im [Ordner wiederherstellbare Elemente in Exchange Online](#) lesen.
- Exchange Online PowerShell können nur die Verfahren in diesem Thema ausführen. Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter: [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell Elemente aus dem Ordner "wiederherstellbare Elemente" für Postfächer zu löschen, werden nicht in die Warteschleife gestellt oder keinen Wiederherstellung einzelner Elemente aktiviert

In diesem Beispiel werden die Elemente dauerhaft aus der Benutzer Gurinder Singh Ordner "wiederherstellbare Elemente" gelöscht und auch die Elemente in den Ordner GurinderSingh RecoverableItems, in dem Discoverysuchpostfach (ein integrierter Postfach in Exchange Online) kopiert.

```
Search-Mailbox -Identity "Gurinder Singh" -SearchDumpsterOnly -TargetMailbox "Discovery Search Mailbox" -TargetFolder "GurinderSingh-RecoverableItems" -DeleteContent
```

### NOTE

Verwenden Sie, um Elemente aus dem Postfach zu löschen, ohne sie auf anderes Postfach kopieren, mit dem vorstehenden Befehl ohne den Parameter *TargetMailbox* und *TargetFolder*.

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Search-Mailbox](#).

## Verwenden von Exchange Online PowerShell Bereinigen des Ordners "wiederherstellbare Elemente" für Postfächer, die in der Warteschleife befinden oder Wiederherstellung einzelner Elemente aktiviert

In diesem Szenario wird vollständig in das [Löschen von Elementen im Ordner des cloudbasierten Postfächer auf halten wiederherstellbaren Elementen](#) Thema behandelt.

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie erfolgreich bereinigt oder Elemente aus dem Ordner wiederherstellbare Elemente eines Postfachs gelöscht haben, verwenden Sie [Get-mailboxfolderstatistics abrufen](#) -Cmdlet die Kontrollkästchen der Größe des Ordners "Wiederherstellbare Elemente".

Bei diesem Beispiel wird die Größe des Ordners "Wiederherstellbare Elemente" und seiner Unterordner sowie die Anzahl der Elemente im Ordner und den einzelnen Unterordnern abgerufen.

```
Get-MailboxFolderStatistics -Identity "Gurinder Singh" -FolderScope RecoverableItems | Format-Table Name,FolderAndSubfolderSize,ItemsInFolderAndSubfolders -Auto
```

# Bewährte Methoden für die Nachrichtenübermittlung für Exchange Online und Office 365 (Übersicht)

18.12.2018 • 16 minutes to read

Verwenden Sie Microsoft Exchange Online und Office 365 zur Verwaltung Ihres Nachrichtenflusses: In diesem Artikel erfahren Sie, wie es geht, und finden Tipps sowie bewährte Methoden für die E-Mail-Einrichtung und -Verwaltung.

**Dieser Artikel richtet sich an IT-Experten. Sie benötigen andere Informationen?**

**Lesen Sie den Artikel [Einrichten von Office 365 Business](#) oder den Artikel [Bereitstellen von Office 365 Enterprise für Ihre Organisation](#).**

Office 365 bietet Ihnen Flexibilität bei der Wahl des besten Setups für die Übermittlung von E-Mails an die Postfächer Ihrer Organisation. Der Weg, den eine E-Mail aus dem Internet bis zu einem Postfach und umgekehrt durchläuft, wird Nachrichtenfluss genannt. Für die meisten Organisationen ist es ausreichend, wenn sowohl die Verwaltung aller Postfächer als auch die E-Mail-Filterung über Office 365 läuft. Einige Organisationen benötigen jedoch einen komplexeren Nachrichtenfluss, um bestimmte gesetzliche Vorschriften oder geschäftliche Anforderungen zu erfüllen. Kleinunternehmen oder Organisationen, die möchten, dass Office 365 die Verwaltung sämtlicher Postfächer sowie des Nachrichtenflusses übernimmt, empfehlen wir den Artikel [Einrichten von Office 365 Business](#). Sie finden dort eine vollständige Checkliste für die Einrichtung von Office 365-Diensten und -Programmen, einschließlich der Einrichtung von Nachrichtenflüssen und E-Mail-Clients.

Informationen dazu, wie Ihre E-Mails mit EOP geschützt werden, finden Sie unter [Exchange Online Protection Overview](#).

## TIP

Sind Sie neu in Office 365-Nachrichtenfluss? Sehen Sie sich das Thema [externe DNS-Einträge für Office 365](#) . Wir empfehlen insbesondere das Webpart zu SPF-Datensätze lesen, da Kunden häufig falsche Werte in ihre SPF-Eintrag aufgelistet, bei die Mail Flow Problemen führen kann.

Für den Office 365-Nachrichtenfluss sind folgende Szenarien möglich:

EINRICHTEN DES NACHRICHTENFLUSSES	SZENARIO IN IHRER ORGANISATION	KOMPLEXITÄT
<a href="#">Verwalten aller Postfächer und des Nachrichtenflusses mithilfe von Office 365</a>	<b>Szenario 1</b> Ich bin ein neuer Office 365-Kunde, und alle meine Benutzerpostfächer befinden sich in Office 365. Ich möchte alle von Office 365 bereitgestellten Filterlösungen verwenden. <b>Szenario 2</b> Ich bin ein neuer Office 365-Kunde. Ich verfüge über einen E-Mail-Dienst, möchte jedoch die vorhandenen Benutzerpostfächer gleichzeitig in die Cloud verschieben. Ich möchte alle von Office 365 bereitgestellten Filterlösungen verwenden.	Einfach

EINRICHTEN DES NACHRICHTENFLUSSES	SZENARIO IN IHRER ORGANISATION	KOMPLEXITÄT
Verwalten des E-Mail-Flusses mithilfe eines Drittanbieter-Clouddiensts mit Office 365	<p><b>Szenario 1</b>  Ich möchte, dass alle Postfächer meiner Organisation von Office 365 gehostet werden. Meine Organisation verwendet derzeit die (E-Mail-)Cloudlösung eines Drittanbieters zur Filterung von Spam und Malware bzw. plant, eine solche Drittanbieterlösung zu verwenden. Alle aus dem Internet gesendeten E-Mails müssen von diesem Drittanbieter-Clouddienst gefiltert werden.</p> <p><b>Szenario 2</b>  Ich möchte, dass alle Postfächer meiner Organisation von Office 365 gehostet werden. Meine Organisation muss alle E-Mails an einen Drittanbiertdienst senden, z. B. Archivierung oder Überwachung. Der Drittanbiertdienst stellt jedoch keine Spamfilterlösung bereit.</p>	Komplex

EINRICHTEN DES NACHRICHTENFLUSSES	SZENARIO IN IHRER ORGANISATION	KOMPLEXITÄT
<p>Verwalten des E-Mail-Flusses mit Postfächern an mehreren Speicherorten (Office 365 und lokal)</p> <p><b>Wichtig:</b> Office 365 lehnt In naher Zukunft, e-Mail-Nachrichten von unbekannten Absendern, die aus dem lokalen Server weitergeleitet werden. Das heißt, wenn die Domäne Absender oder Empfänger einer Nachricht nicht zu Ihrer Organisation gehört, Office 365 die Nachricht abgelehnt wird, wenn Sie eine Verbindung aus, um dies zu ermöglichen erstellt haben. Diese Änderung wird verhindert unbefugte verwenden Ihrer Organisation zum Senden von Spam oder Schadsoftware über Office 365.</p> <p>Diese Änderung wirkt sich möglicherweise auf Ihren E-Mail-Fluss aus, wenn Sie ein Szenario dieses Abschnitts verwenden. Für jedes dieser Szenarien sind bewährte Methoden vorhanden, mit denen sichergestellt wird, dass Ihr E-Mail-Fluss nicht unterbrochen wird.</p>	<p><b>Szenario 1</b> Ich möchte meine Postfächer zu Office 365 migrieren, dabei aber einige Postfächer weiterhin auf dem E-Mail-Server meiner Organisation (lokaler Server) belassen. Ich möchte Office 365 als Spamfilterlösung verwenden und Nachrichten von meinem lokalen Server über Office 365 ins Internet senden. Office 365 soll alle Nachrichten senden und empfangen.</p> <p><b>Szenario 2</b> Ich möchte meine Postfächer zu Office 365 migrieren, dabei aber einige Postfächer weiterhin auf dem E-Mail-Server meiner Organisation (lokaler Server) belassen. Ich möchte die Filter- und Compliancelösungen verwenden, die bereits in meiner lokalen Umgebung vorhanden sind. Alle Nachrichten, die aus dem Internet an meine Clouddpostfächer und aus meinen Clouddpostfächern ins Internet gesendet werden, müssen über meine lokalen Server laufen.</p> <p><b>Szenario 3</b> Ich möchte meine Postfächer zu Office 365 migrieren, dabei aber einige Postfächer weiterhin auf dem E-Mail-Server meiner Organisation (lokaler Server) belassen. Ich möchte die Filter- und Compliancelösungen verwenden, die bereits in meiner lokalen E-Mail-Umgebung vorhanden sind. Alle Nachrichten, die aus dem Internet an meine Clouddpostfächer und aus meinen Clouddpostfächern ins Internet gesendet werden, müssen über meine lokalen Server laufen. Außerdem muss der MX-Eintrag meiner Domäne auf meinen lokalen Server verweisen.</p> <p><b>Szenario 4</b> Ich möchte meine Postfächer zu Office 365 migrieren, dabei aber einige Postfächer weiterhin auf dem E-Mail-Server meiner Organisation (lokaler Server) belassen. Ich möchte die Filter- und Compliancelösungen verwenden, die bereits in meiner lokalen E-Mail-Umgebung vorhanden sind. Alle Nachrichten, die von meinen lokalen Servern gesendet werden, müssen über Office 365 ins Internet weitergeleitet werden. Außerdem muss der MX-Eintrag meiner Domäne auf meinen lokalen Server verweisen.</p>	<p>Sehr komplex</p>

EINRICHTEN DES NACHRICHTENFLUSSES	SZENARIO IN IHRER ORGANISATION	KOMPLEXITÄT
Verwalten des Mailflusses mithilfe eines Drittanbieter-Clouddiensts mit Postfächern in Office 365 und lokalen Postfächern	<b>Szenario</b> Ich möchte meine Postfächer zu Office 365 migrieren, dabei aber einige Postfächer weiterhin auf dem E-Mail-Server meiner Organisation (lokaler Server) belassen. Ich möchte den Clouddienst eines Drittanbieters zur Filterung von Spam aus dem Internet verwenden. Nachrichten ins Internet müssen über Office 365 laufen, damit die IP-Adressen meiner lokalen Server nicht zu externen Listen blockierter IP-Adressen hinzugefügt werden.	Komplexeste
Senden von E-Mails von Multifunktionsdruckern/Scannern/Faxgeräten/Anwendungen über Office 365 Weitere Informationen zu diesem Szenario finden Sie unter <a href="#">Einrichten eines Multifunktionsgeräts oder einer Anwendung zum Senden von E-Mails mit Office 365</a> .	<b>Szenario</b> Alle Postfächer meiner Organisation werden in Office 365, gehostet, ich verfüge jedoch über einen Multifunktionsdrucker, Scanner, ein Faxgerät oder eine Anwendung, von dem bzw. von der E-Mails gesendet werden.	Komplex
Verwenden von Exchange Online Protection (EOP) als eigenständige Lösung Informationen zu diesem Szenario finden Sie unter <a href="#">Mail Flow in EOP</a> und <a href="#">Wie funktionieren Office 365-Connectors mit meinen eigenen (lokalen) Servern?</a>	<b>Szenario</b> Ich habe eigene E-Mail-Server (lokale Server), und ich habe EOP nur für E-Mail-Schutzdienste abonniert.	Einfach

Informationen zur Migration Ihrer E-Mail-Konten zu Microsoft Exchange Online finden Sie unter [Methoden zum Migrieren mehrerer E-Mail-Konten zu Office 365](#).

## Einführung in die Grundlagen des Office 365-Nachrichtenflusses

verwendet Domänen wie contoso.com zum Weiterleiten von E-Mails. Bei der E-Mail-Einrichtung in wechseln Sie in der Regel von der Standarddomäne, die Sie bei der ersten Registrierung erhalten haben (die Domäne mit der Endung .onmicrosoft.com), zur Domäne Ihrer Organisation. Domänennamen wie contoso.com werden über ein weltweites System von Domänenregistrierungsstellen (z. B. GoDaddy, HostGator oder Moniker) und Datenbanken verwaltet, das als Domain Name System (DNS) bezeichnet wird. DNS regelt die Zuordnung von lesbaren Computerhostnamen zu den von Netzwerkgeräten verwendeten IP-Adressen. Wenn Sie noch nicht mit DNS vertraut sind, sollten Sie den Artikel [DNS-Grundlagen](#) lesen. Das folgende Video bietet eine kurze Übersicht über einige der wichtigsten Konzepte zur Definition und Funktionsweise von DNS.

### Verstehen, wie DNS-Einträge den Nachrichtenfluss steuern

Im -Nachrichtenfluss sind zwei DNS-Einträge besonders wichtig: MX-Einträge und SPF-Einträge.

**MX-Einträge (Mail Exchanger)** sind eine einfache Möglichkeit für E-Mail-Server, um zu erfahren, wo die E-Mail gesendet werden soll. Sie können sich den MX-Eintrag als eine Art Postanschrift vorstellen. Wenn Office 365 alle an anyone@contoso.com gesendeten E-Mails erhalten soll, muss der MX-Eintrag für contoso.com auf verweisen und so aussehen wie im folgenden Beispiel:

```
Hostname: contoso-com.mail.protection.outlook.com
Priority: 0
TTL: 1 hour
```

**SPF (Sender Policy Framework)-Einträge** sind speziell formatierte TXT-Einträge in DNS. Sie stellen sicher, dass nur die Organisation, die tatsächlich Besitzer einer Domäne ist, E-Mails aus dieser Domäne versendet. SPF ist im Grunde eine Sicherheitsmaßnahme, um zu verhindern, dass sich Dritte als eine bestimmte Organisation ausgeben. (Eine solche Täuschung wird häufig als Spoofing bezeichnet.) Als Domänenbesitzer können Sie mithilfe eines SPF-Eintrags eine Liste aller IP-Adressen oder Subnetze veröffentlichen, die zur Versendung von E-Mails im Namen Ihrer Organisation autorisiert sind. Dies kann hilfreich sein, wenn Sie E-Mails von mehreren Servern oder Diensten mit unterschiedlichen IP-Adressen senden möchten. Der SPF-Eintrag einer Organisationsdomäne, die sämtliche E-Mails über sendet, sollte aussehen wie im folgenden Beispiel:

```
v=spf1 include:spf.protection.outlook.com -all
```

#### IMPORTANT

Es ist nur ein SPF-Eintrag pro Domäne zulässig. Beim Verwenden mehrerer SPF-Einträge werden alle SPF-Einträge ungültig und es kommt zu Problemen mit dem Nachrichtenfluss.

Die Konfiguration des SPF-Eintrags im Beispiel oben teilt den E-Mail-Servern der Empfänger mit, dass alle von -IP-Adressen gesendeten E-Mails für die Domäne autorisiert sind. Da die meisten E-Mail-Server heute zuerst den SPF-Eintrag einer Domäne abrufen, bevor sie E-Mails von ihr akzeptieren, ist es wichtig, bei der Ersteinrichtung des Nachrichtenflusses einen gültigen SPF-Eintrag in DNS einzurichten.

#### Auswirkungen von MX-Einträgen auf Spamfilter

Für einen optimale Nachrichtenfluss, insbesondere hinsichtlich der Spamfilterung, empfehlen wir, den MX-Eintrag für die Domäne Ihrer Organisation auf verweisen zu lassen. Die Überprüfung auf Spam ist der erste Verbindungspunkt mit dem -Dienst. Informationen wie der Absender der Nachricht, die IP-Adresse des Servers, von dem die Nachricht ursprünglich gesendet wurde, und das Verhalten des E-Mail-Servers, mit dem eine Verbindung hergestellt wird, helfen bei der Entscheidung, ob eine Nachricht legitim oder Spam ist. Wenn der MX-Eintrag Ihrer Domäne nicht auf verweist, arbeiten die Spamfilter weniger effektiv. Wenn Ihr MX-Eintrag nicht auf verweist, werden einige legitime Nachrichten vom Dienst fälschlicherweise als Spam klassifiziert und einige Spammnachrichten als legitime Nachrichten.

Dennoch gibt es einige legitime Geschäftsszenarien, in denen der MX-Eintrag Ihrer Domäne nicht auf verweisen darf. Beispiel: An Ihre Organisation gerichtete E-Mails müssen eventuell zunächst an ein anderes Ziel gesendet werden (z. B. die Archivierungslösung eines Drittanbieters) und dann über weitergeleitet werden. Von dort aus werden sie dann an die Postfächer auf dem E-Mail-Server Ihrer Organisation übermittelt. Ein solches Setup kann unter Umständen die beste Lösung für Ihre spezifischen Geschäftsanforderungen sein.

In diesem Handbuch erfahren Sie unabhängig von Ihren Anforderungen, wie MX-Einträge, SPF-Einträge und potenzielle Connectors eingerichtet werden müssen.

## Weitere Informationen

Im Folgenden sind zusätzliche Themen im Zusammenhang mit Nachrichtenfluss in Exchange Online aufgeführt:

[Testen der Nachrichtenübermittlung durch Überprüfen der Office 365-Connectors](#)

[Beheben von Problemen beim Office 365-Nachrichtenfluss](#)

[Verwenden Sie verzeichnisbasierte Edge-Blockierung zum Ablehnen von Nachrichten, die an ungültige](#)

[Empfänger gesendet](#)

[Verwalten akzeptierter Domänen in Exchange Online](#)

[Remotedomänen in Exchange Online](#)

[Nachrichtenformat und -übertragung in Exchange Online](#)

[Konfigurieren der externen Postmasteradresse in Exchange Online](#)

[Einrichten eines Multifunktionsgeräts oder einer Anwendung zum Senden von E-Mails mithilfe von Office 365](#)

# Testen der Nachrichtenübermittlung durch Überprüfen der Office 365-Connectors

18.12.2018 • 2 minutes to read

Prüfen Sie zur Überprüfung und Problembehandlung für den Nachrichtenfluss von Office 365 an den E-Mail-Server Ihrer Organisation (auch lokaler Server genannt) die Connectors. Sie können auf der Seite **Connectors** im Exchange-Verwaltungskonsole (EAC) Connectors einrichten und überprüfen. Mit der integrierten Überprüfung wird getestet, ob die Nachrichten von Office 365 an folgende Stellen übermittelt werden:

- E-Mail-Server Ihrer Organisation
- Eine Partnerorganisation.

Weitere Informationen finden Sie unter [Validieren von Connectors in Office 365](#)

Probleme mit dem Nachrichtenfluss können auch auftreten, wenn der MX-Eintrag nicht richtig eingerichtet ist. Weitere Informationen zum Überprüfen des MX-Eintrags finden Sie unter [Suchen und Beheben von Problemen, nachdem Ihre Domäne oder DNS-Einträge in Office 365 hinzugefügt wurden](#).

## NOTE

Mit diesen Tests wird die Office 365 Problembehandlung für Nachrichtenfluss ersetzt, die vorher im Rahmen der [Remoteverbindungsuntersuchung](#) verfügbar war.

## See also

[Configure mail flow using connectors in Office 365](#)

[Einrichten von Connectors zur Weiterleitung von E-Mails zwischen Office 365 und Ihren eigenen E-Mail-Servern](#)

[Fixing connector validation errors](#)

[Wann benötige ich einen Connector?](#)

# Beheben von Problemen beim Office 365-Nachrichtenfluss

18.12.2018 • 2 minutes to read

Sie können keine E-Mails senden oder empfangen? In Office 365 for Business gibt es verschiedene Möglichkeiten, um dieses Problem als Administrator zu beheben. Es wird empfohlen, die automatisierten Lösungen zu verwenden, da diese in der Regel einfacher und schneller als die manuelle Problembehandlung sind.

Anweisungen zur Problembehandlung bei Optionen finden Sie unter [feststellen und beheben Sie Probleme bei der e-Mail-Übermittlung als ein Office 365 für Unternehmen Admin](#).

## Behandlung von Problemen bei der Nachrichtenübermittlung, die durch Connectors verursacht werden

Zum Überprüfen und Beheben von e-Mail-Fluss von Office 365 an die e-Mail-Server in Ihrer lokalen Organisation (auch als den lokale Server bezeichnet), überprüfen Sie die Connectors. Sie können einrichten und Verbinden auf dem Zeichenblatt **Connectors** im Exchange Administrationscenter (EAC) überprüft. Die integrierten Validierungstests, die Ihre e-Mail-Fluss von Office 365 erreicht:

- E-Mail-Server Ihrer Organisation
- Eine Partnerorganisation.

Weitere Informationen finden Sie unter [Validieren von Connectors in Office 365](#).

## Behandlung von Problemen bei der Nachrichtenübermittlung, die durch falsche SPF- oder MX-Einträge verursacht werden

Unter [Problembehandlung: Bewährte Methoden für SPF in Office 365](#) erhalten Tipps zur Behebung verschiedener Fehler bei SPF-Einträgen. Am Anfang dieses Artikels finden Sie auch eine Erläuterung dazu, was SPF-Einträge sind und wie diese in Office 365 zur Vermeidung von Spoofing verwendet werden.

Probleme mit dem Nachrichtenfluss können auch auftreten, wenn der MX-Eintrag nicht richtig eingerichtet ist. Weitere Informationen zum Überprüfen des MX-Eintrags finden Sie unter [Suchen und Beheben von Problemen, nachdem Ihre Domäne oder DNS-Einträge in Office 365 hinzugefügt wurden](#).

## Weitere Informationen

[Bewährte Methoden für die Nachrichtenübermittlung für Exchange Online und Office 365 \(Übersicht\)](#)

[Mail Flow in EOP](#)

# Konfigurieren des Nachrichtenflusses mit Connectors in Office 365

18.12.2018 • 17 minutes to read

Verbinder sind eine Auflistung von Anweisungen, die Möglichkeit, Ihre e-Mail-Adresse fließt, zu und von Office 365-Organisation anpassen. Die meisten Office 365-Organisationen benötigen nicht tatsächlich, Connectors für reguläre e-Mail-Fluss. In diesem Thema werden die Szenarien für Nachrichtenübermittlung, die Connectors erfordern.

## Welchen Zweck haben Connectors?

Connectors verwendet werden:

- Aktivieren der Nachrichtenübermittlung zwischen Office 365 und einem beliebigen e-Mail-Server, die Ihnen in Ihrer lokalen Organisation (auch bekannt als lokale e-Mail-Servoren).
- Wenden Sie sicherheitseinschränkungen oder Steuerelemente für auf e-Mail-Austausch zwischen Office 365-Organisation und einer Business Partner oder Dienstanbieter an.
- Aktivieren Sie e-Mail-Benachrichtigungen von Druckern, Geräte oder andere nicht-Mailbox-Entitäten.
- Vermeiden Sie graue Liste, die andernfalls aufgrund der großen Anzahl von e-Mail-Nachrichten auftreten würden, die zwischen Office 365-Organisation regelmäßig ausgetauscht werden, und Ihre lokale e-Mail-Server oder Partnern.

### NOTE

Graue Liste ist eine Verzögerung Vorgehensweise, die zum Schutz von e-Mail-Systemen vor Spam verwendet wird. In Office 365 erfolgt die graue Liste durch Drosselung IPs Absender am Senden von Grund von einer zu großer Mengen an e-Mails zu beschränken. Office 365 reagiert auf diese ungewöhnliche Influxes von e-Mails durch eine temporäre Unzustellbarkeitsbericht-Fehler (auch bekannt als ein Unzustellbarkeitsbericht oder Springeffekt Nachricht) in den Bereich 451 4.7.500-699 zurückgeben (ASxxx). Weitere Informationen zu dieser Arten von Probleme bei der Übermittlung, finden Sie unter [beheben Sie Probleme bei der Übermittlung für Fehler 451 Code 4.7.500-699 e-Mail \(ASxxx\) in Office 365](#).

## Was ist mit den eingehenden und ausgehenden Connectors passiert?

Nothing zurück. Wir anzurufen nicht nur sie "Eingehend" und "Ausgehend" mehr (obwohl die PowerShell-Cmdlet-Namen weiterhin enthält diese Begriffe). Wenn Sie zuvor eingehenden und ausgehenden Connectors eingerichtet haben, werden sie jedoch auf genau die gleiche Weise funktionieren.

Der Prozess zum Einrichten von Connectors geändert hat. statt die Begriffe "Eingehend" und "Ausgehend" bitten wir Ihnen, anzugeben, die Anfangs- und Endpunkte, die Sie verwenden möchten. Die Arbeitsweise Connectors im Hintergrund ist dieselbe wie zuvor (eingehende bedeutet, dass in Office 365; bedeutet, dass ausgehende von Office 365 gesendet).

## Wann benötige ich einen Connector?

Exchange Online ist, zu senden und Empfangen von e-Mails aus dem Internet sofort bereit. Sie müssen nicht von Connectors festgelegt, es sei denn, Sie verfügen über Exchange Online Protection (EOP) oder anderen bestimmten Umständen, die in der folgenden Tabelle beschrieben werden:

SZENARIO	BESCHREIBUNG	IST EIN CONNECTOR ERFORDERLICH?	CONNECTOR-EINSTELLUNG
Sie haben eine eigenständige EOP-Abonnement.	<p>Sie haben Ihre eigene lokale e-Mail-Servern und EOP nur für e-Mail-Schutzdienste für Ihre lokale Postfächer (müssen keine Postfächer in Exchange Online) abonnieren.</p> <p>Weitere Informationen finden Sie im Thema <a href="#">Exchange Online Protection im Überblick</a> und die <a href="#">wie funktionieren Connectors mit meiner lokalen e-Mail-Servern?</a> weiter unten in diesem Thema.</p>	Ja	<p><b>Connector für eingehende e-Mail:</b></p> <ul style="list-style-type: none"> <li>• Klicken Sie <b>in:</b> das lokale e-Mail-Server</li> <li>• <b>An:</b> Office 365</li> </ul> <p><b>Connector für ausgehende e-Mail:</b></p> <ul style="list-style-type: none"> <li>• <b>Aus:</b> Office 365</li> <li>• Klicken Sie <b>zum:</b> das lokale e-Mail-Server</li> </ul>
Einige Ihrer Postfächer befinden sich auf Ihre lokalen e-Mail-Server, und einige sind in Exchange Online.	<p>Bevor Sie Connectors manuell konfigurieren, überprüfen Sie, ob eine hybride Exchange-Bereitstellung besser auch Ihre geschäftsanforderungen erfüllt.</p> <p>Weitere Informationen hierzu finden Sie unter der <a href="#">Was passiert, wenn ich meinen eigenen e-Mail-Servern haben?</a> weiter unten in diesem Topicand im Thema <a href="#">Exchange Server Hybrid Deployments</a>.</p>	Ja	<p><b>Connector für eingehende e-Mail:</b></p> <ul style="list-style-type: none"> <li>• Klicken Sie <b>in:</b> das lokale e-Mail-Server</li> <li>• <b>An:</b> Office 365</li> </ul> <p><b>Connector für ausgehende e-Mail:</b></p> <ul style="list-style-type: none"> <li>• <b>Aus:</b> Office 365</li> <li>• Klicken Sie <b>zum:</b> das lokale e-Mail-Server</li> </ul>
Alle Ihre Postfächer sind in Exchange Online, aber Sie müssen zum Senden von e-Mails aus Quellen in Ihrer lokalen Organisation.	<p>Sie müssen keine eigenen e-Mail-Servern, sondern auch zum Senden von e-Mail-Postfächern der nicht benötigten: Drucker, Fax-, apps oder andere Geräte.</p> <p>Weitere Informationen hierzu finden Sie unter <a href="#">Option 3: Konfigurieren Sie einen Connector zum Senden von e-Mail-Nachrichten mithilfe von Office 365 SMTP-Relay</a></p>	Optional	<p><b>Nur ein Connector für eingehende e-Mail:</b></p> <ul style="list-style-type: none"> <li>• Klicken Sie <b>in:</b> Ihrer Organisation e-Mail-Server</li> <li>• <b>An:</b> Office 365</li> </ul>

SZENARIO	BESCHREIBUNG	IST EIN CONNECTOR ERFORDERLICH?	CONNECTOR-EINSTELLUNG
Tauschen Sie häufig vertraulichen Informationen mit Geschäftspartnern und Sicherheitseinschränkungen gelten sollen.	<p>Transport Layer Security (TLS) zum Verschlüsseln von vertraulichen Informationen verwenden soll, oder Sie für e-Mail-Nachrichten von der Partnerdomäne die Quelle (IP-Adressen) beschränken möchten.</p> <p>Weitere Informationen hierzu finden Sie unter <a href="#">Einrichten von Connectors für die sichere Nachrichtenübermittlung mit einer Partnerorganisation</a>.</p>	Optional	<p><b>Connector für eingehende e-Mail:</b></p> <ul style="list-style-type: none"> <li>• Klicken Sie in: Partner-Organisation</li> <li>• An: Office 365</li> </ul> <p><b>Connector für ausgehende e-Mail:</b></p> <ul style="list-style-type: none"> <li>• Aus: Office 365</li> <li>• Klicken Sie zum: Partner-Organisation</li> </ul>

#### TIP

Wenn Sie keinen Zugriff haben, Exchange Online oder EOP interessieren sich für Informationen zu Sendeconnectors und Empfangsconnectors in Exchange 2016 oder Exchange 2019, finden Sie unter [Connectors](#).

## Was geschieht, wenn ich meinen eigenen e-Mail-Servern haben?

Wenn Sie Exchange Online oder EOP und Ihre eigene lokale e-Mail-Server, benötigen Sie definitiv Connectors. Dies ist komplizierter und weitere Optionen wie in der folgenden Tabelle beschrieben:

SIE SIND LOKALE E-MAIL-ORGANISATION IST	IHR DIENSTABONNEMENT IST	HABEN SIE EINE EXCHANGE-HYBRIDBEREITSTELLUNG DURCHGEFÜHRT?	BENÖTIGE ICH VON CONNECTORS MANUELL FESTLEGEN?
Exchange 2010 oder höher	Exchange Online Protection	Nicht verfügbar	Ja. Befolgen Sie die Anweisungen in <a href="#">Connectors zum Weiterleiten von e-Mails zwischen Ihrem eigenen e-Mail-Servern und Office 365 einrichten</a> .

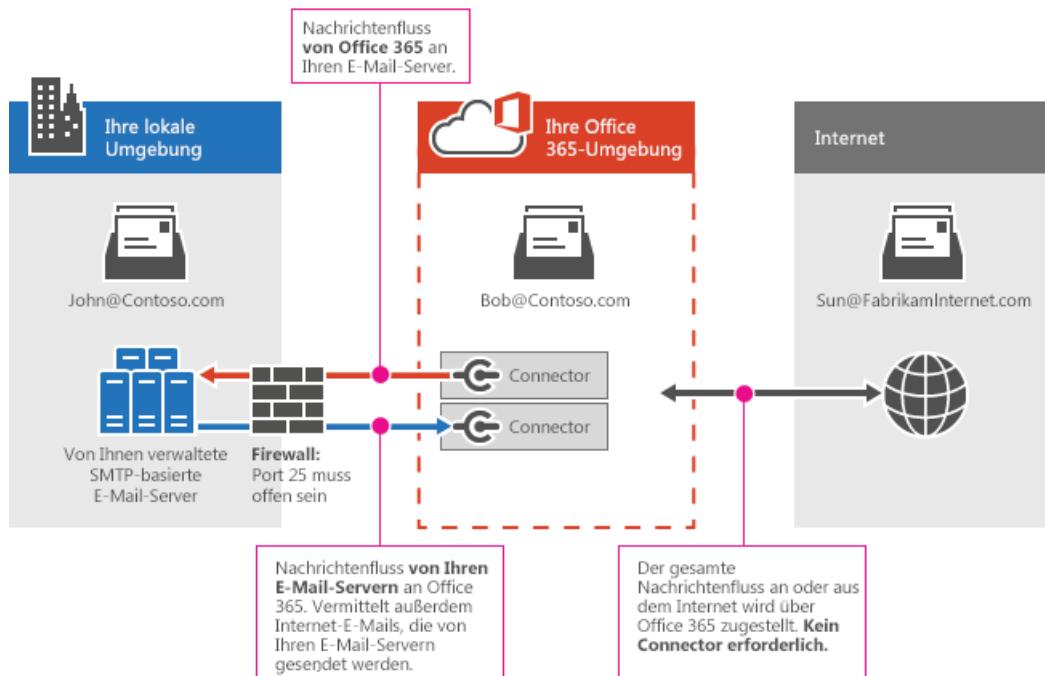
SIE SIND LOKALE E-MAIL-ORGANISATION IST	IHR DIENSTABONNEMENT IST	HABEN SIE EINE EXCHANGE-HYBRIDBEREITSTELLUNG DURCHGEFÜHRT?	BENÖTIGE ICH VON CONNECTORS MANUELL FESTLEGEN?
Exchange 2010 oder höher	Exchange Online	Nein	<p>Überlegen Sie, ob eine hybride Exchange-Bereitstellung besser der Anforderungen Ihrer Organisation erfüllen durch die Überprüfung des Themas, das die aktuelle Situation in <a href="#">Hybridbereitstellungen in Exchange Server</a> übereinstimmt.</p> <p>Wenn eine hybridbereitstellung die richtige Option für Ihre Organisation ist, mithilfe des <a href="#">Hybrid-Konfigurations-Assistenten für Exchange</a> Online in Ihrer lokalen Exchange-Organisation zu integrieren.</p> <p>Wenn Sie nicht, dass eine hybridbereitstellung möchten, und Sie nur Connectors, die e-Mail-routing aktivieren möchten, befolgen Sie die Anweisungen in <a href="#">Connectors zum Weiterleiten von e-Mails zwischen Ihrem eigenen e-Mail-Servern und Office 365 einrichten</a>.</p>
Exchange 2010 oder höher	Exchange Online	Ja	Nein. Assistenten für die Hybridkonfiguration erstellt Connectors. Anzeigen oder bearbeiten diese Connectors, wechseln Sie zur Seite <b>Connectors</b> im Exchange Administrationscenter (EAC), oder führen Sie den Assistenten für Hybridkonfigurationen erneut aus.

SIE SIND LOKALE E-MAIL-ORGANISATION IST	IHR DIENSTABONNEMENT IST	HABEN SIE EINE EXCHANGE-HYBRIDBEREITSTELLUNG DURCHGEFÜHRT?	BENÖTIGE ICH VON CONNECTORS MANUELL FESTLEGEN?
Exchange 2007 oder älter	Exchange Online Protection oder Exchange Online	Nicht verfügbar	<p>Ja. Führen Sie die Anweisungen in <a href="#">Connectors zum Weiterleiten von e-Mails zwischen Ihrem eigenen e-Mail-Servers und Office 365 einrichten.</a></p> <p>Bei bestimmten Umständen müssen Sie möglicherweise eine hybridkonfiguration mit Exchange Server 2007 und Office 365. Überprüfen Sie, ob Verbinder bereits für Ihre Organisation eingerichtet werden durch Aufrufen der Seite <a href="#">Connectors</a> in der Exchange-Verwaltungskonsole.</p>
Anderer als Microsoft-SMTP-Server	Exchange Online Protection oder Exchange Online	Nicht verfügbar	<p>Ja. Befolgen Sie die Anweisungen in <a href="#">Connectors zum Weiterleiten von e-Mails zwischen Ihrem eigenen e-Mail-Servers und Office 365 einrichten.</a></p>

### Wie funktionieren Connectors mit meiner lokalen e-Mail-Server?

Connectors Aktivieren der Nachrichtenübermittlung in beide Richtungen (zu Office 365 und vom Office 365). Sie können die Nachrichtenübermittlung mit einem SMTP-Server (beispielsweise Microsoft Exchange oder einem Drittanbieter-e-Mail-Server) aktivieren.

Im folgenden Diagramm veranschaulicht, wie Connectors in Exchange Online oder EOP arbeiten mit Ihren eigenen e-Mail-Servern.



In diesem Beispiel werden John und Bob beide Mitarbeiter in Ihrem Unternehmen. John hat ein Postfach auf einem e-Mail-Server, den Sie verwalten, und Bob verfügt über ein Postfach in Exchange Online. John und Bob exchange Mail mit Sun, ein Kunde mit einem Internet Mail-Konto:

- Wenn zwischen John und Bob e-Mail gesendet wird, werden die Konnektoren benötigt.
- Wenn zwischen John und Sun e-Mail gesendet wird, werden die Konnektoren benötigt. (Alle Internet-e-Mail wird über Office 365 übermittelt).
- Zum Senden von E-Mails zwischen Bob und Sun ist kein Connector erforderlich.

#### **IMPORTANT**

Immer bestätigen Sie, dass Ihre Internet verbundenen e-Mail-Server werden nicht versehentlich offenes Relay konfiguriert. *Offenes Relay* ermöglicht es e-Mail-Nachrichten von einer beliebigen Quelle (Spammer) transparent über den offenen Relayserver weitergeleitet werden sollen. Dieses Verhalten die ursprüngliche Quelle der Nachrichten maskiert und erleichtert die e-Mail-Nachricht stammt vom Server offenes Relay aussehen.

#### **Was geschieht, wenn ich bereits the Hybrid Configuration Wizard ausgeführt haben?**

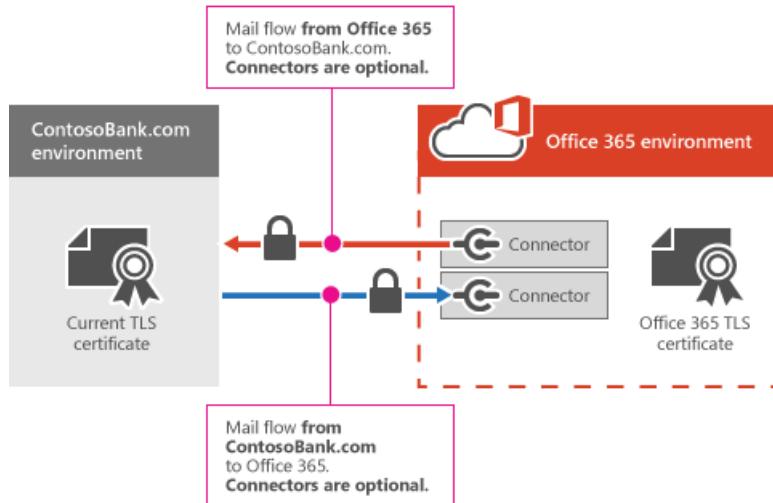
Wenn Sie den Assistenten für die Hybridkonfiguration bereits ausgeführt haben, sind die erforderlichen Connectors bereits für Sie konfiguriert. Sie können Ihre Hybriden Connectors auf der Seite **Connectors** in der Exchange-Verwaltungskonsole anzeigen. Können Sie anzeigen, Problembehandlung und aktualisieren diese Connectors verwenden die Verfahren unter [Einrichten von Connectors zum Weiterleiten von e-Mails zwischen Ihrem eigenen e-Mail-Servern und Office 365](#), oder Sie können den Hybrid-Konfigurations-Assistenten, um die Änderungen vornehmen erneut ausführen.

## **Connectors für den E-Mail-Fluss mit einer Partnerorganisation**

Sie können Connectors zum Hinzufügen von zusätzlichen sicherheitseinschränkungen für gesendete zwischen Office 365 und einer Partnerorganisation erstellen. Ein Partner kann eine Organisation, die Sie Geschäfte mit, wie etwa eine Bank sein. Sie können auch einen Cloud-e-Mail-Dienstanbieter sein, der Diensten wie etwa Archivierung, Antispam usw. bereitstellt. Sie können einen Partner-Connector erstellen, der Grenzen und Einschränkungen für e-Mail gesendet oder Empfangen von Ihren Partnern, einschließlich Festlegen des Bereichs für des Connectors Empfang von e-Mail von bestimmten IP-Adressen oder TLS-Verschlüsselung erforderlich definiert.

#### **Beispiel der Verwendung von Connectors mit einer Partnerorganisation**

Im nachstehenden Diagramm zeigt ein Beispiel, in dem ContosoBank.com einen Geschäftspartner, den Sie per e-Mail finanzielle Details mit freigeben wird. Da Sie Finanzdaten freigeben, möchten Sie die Integrität der e-Mail-Fluss zwischen Ihrem Unternehmen zu schützen. Connectors mit TLS-Verschlüsselung aktivieren einen sicheren und vertrauenswürdigen DDE-Kanal für die Kommunikation mit ContosoBank.com. In diesem Beispiel werden zwei Verbinder in Office 365 erstellt. TLS ist für die Nachrichtenübermittlung in beide Richtungen erforderlich, damit ContosoBank.com ein gültiges Verschlüsselungszertifikat sein muss. Ein Zertifikat von einer kommerziellen Zertifizierungsstelle (CA), die beide Parteien automatisch als vertrauenswürdig ist, wird empfohlen.



### Weitere Connectoroptionen für Partnerorganisationen: Angeben einer Domäne oder von IP-Adressbereichen

Wenn Sie einen Connector erstellen, können Sie auch angeben, die Domäne oder IP-Adressbereiche, denen Ihre Partner Mail aus sendet. Wenn Sie e-Mail-Nachrichten die Sicherheit Bedingungen nicht erfüllen, die Sie für den Connector festlegen, wird die Nachricht abgelehnt. Weitere Informationen zum Erstellen von Connectors, um sichere e-Mail mit einer Partnerorganisation austauschen finden Sie unter [Einrichten von Connectors für die sichere Nachrichtenübermittlung mit einer Partnerorganisation](#).

## Konnektoren für e-Mail-Benachrichtigungen von Druckern und Geräten

Dieses Szenario gilt nur für Organisationen, in denen alle ihre Postfächer in Exchange Online (keine lokalen e-Mail-Serven) und ermöglicht eine Anwendung oder ein Gerät, beispielsweise einen Drucker, Senden von e-Mails. Beispielsweise wenn Sie möchten einen Drucker Benachrichtigungen senden, wenn ein Druckauftrag bereit ist, oder Sie möchten Ihre Scanner Dokumente, e-Mail, verwenden Sie diese Option zum Senden von e-Mail-Nachrichten über Office 365 (jedoch andere Optionen, die Connectors nicht erforderlich ist). Weitere Informationen hierzu finden Sie unter [ein Multifunktionsgerät oder eine Anwendung zum Senden von E-mail über Office 365 unter Verwendung von SMTP zulassen](#).

## Wie richte ich Connectors ein?

Bevor Sie eine Verbindung eingerichtet haben, müssen Sie zum Konfigurieren von akzeptierten Domänen für Office 365. Weitere Informationen finden Sie unter [Manage akzeptierte Domänen im Exchange, Online](#).

Themen zur Einrichtung von Connectors:

- [Einrichten von Connectors zur Weiterleitung von E-Mails zwischen Office 365 und Ihren eigenen E-Mail-Serven](#)
- [Einrichten von Connectors für den sicheren Nachrichtenfluss mit einer Partnerorganisation](#)

## See also

[Einrichten von Connectors zur Weiterleitung von E-Mails zwischen Office 365 und Ihren eigenen E-Mail-Serven](#)

[Bewährte Methoden für die Nachrichtenübermittlung für Exchange Online und Office 365 \(Übersicht\)](#)

[Einrichten von Connectors für den sicheren Nachrichtenfluss mit einer Partnerorganisation](#)

[Was passiert, wenn ich über mehrere Connectors für das gleiche Szenario verfüge?](#)

# Muss ich einen Connector erstellen?

18.12.2018 • 3 minutes to read

Suchen Sie Ihr Szenario für die Nachrichtenübermittlung, um zu sehen, ob Sie für Ihre Organisation einen Connector erstellen müssen.

SZENARIO	WAS BEDEUTET DAS?	IST EIN CONNECTOR ERFORDERLICH?	WÄHLEN SIE BEIM ERSTELLEN DER CONNECTORS DIESE OPTIONEN AUS
Sie haben eine eigenständige Exchange Online Protection (EOP)-Abonnement.	Sie haben Ihre eigenen E-Mail-Server (auch als lokale Server bezeichnet), und Sie abonnieren EOP nur für E-Mail-Schutzdienste. Details finden Sie in <b>Exchange Online Protection im Überblick</b> und <a href="#">wie funktionieren Office 365-Connectors mit meinen eigenen e-Mail-Servern (auch als "lokale Server" bezeichnet)?</a> .	Ja	<b>Connector für eingehende e-Mail:</b> Von: Ihrer Organisation e-Mail-Server an: Office 365 <b>Connector für ausgehende e-Mail:</b> aus: Office 365 an: Ihrer Organisation e-Mail-Servers
Sie haben ein Exchange Online-Abonnement, und einige Ihrer Postfächer befinden sich auf Ihre e-Mail-Server.	Einige Ihrer Postfächer befinden sich in Microsoft Exchange Online, und einige auf Ihre e-Mail-Server (auch als der lokale Server bezeichnet). Bevor Sie Connectors eingerichtet haben, überprüfen Sie, ob Sie nur Connectors benötigen, oder wenn eine hybride Exchange-Bereitstellung besser auch Ihre geschäftsanforderungen erfüllt. Details finden <a href="#">Was passiert, wenn ich meinen eigenen e-Mail-Servern haben?</a> und <b>Hybridbereitstellungen in Exchange Server.</b>	Ja	<b>Connector für eingehende e-Mail:</b> Von: Ihrer Organisation e-Mail-Server an: Office 365 <b>Connector für ausgehende e-Mail:</b> Von: Office 365: Ihrer Organisation e-Mail-Server
Sie haben ein Exchange Online-Abonnement und Ihrer Organisation zum Senden von e-Mail-Nachrichten von nicht-Postfächern, wie der Drucker muss.	Sie haben keine E-Mail-Server (auch als lokale Server bezeichnet), möchten aber, dass Mitarbeiter E-Mail-Nachrichten aus Quellen wie Druckern, Faxgeräten oder Apps senden können. Weitere Informationen finden Sie unter <b>How to Allow a Multi-function Device or Application to Send E-mail through Office 365 Using SMTP.</b>	Optional	<b>Nur ein Connector benötigt:</b> Von: Ihrer Organisation e-Mail-Server an: Office 365

SZENARIO	WAS BEDEUTET DAS?	IST EIN CONNECTOR ERFORDERLICH?	WÄHLEN SIE BEIM ERSTELLEN DER CONNECTORS DIESE OPTIONEN AUS
Sie tauschen häufig E-Mails mit Geschäftspartnern aus und möchten bestimmte Sicherheitseinschränkungen anwenden.	<p>Wenn Ihre Benutzer e-Mail-Nachrichten mit Personen in Partnerorganisationen austauschen, um sicherzustellen, dass alle freigegebener vertraulicher Informationen geschützt ist werden soll. Sie können diese mithilfe von Transport Layer Security (TLS) oder durch Beschränken der Mail-Quelle Ziel Schritte durchführen.</p> <p>Weitere Informationen finden Sie unter <a href="#">Set up connectors for secure mail flow with a partner organization</a>.</p>	Optional	<p><b>Connector für eingehende e-Mail:</b> Aus: Partner-Organisation: Office 365</p> <p><b>Connector für ausgehende e-Mail:</b> Von: Office 365: Partner-Organisation</p>

#### NOTE

Weitere Informationen über diese Szenarien finden Sie unter [Configure mail flow using connectors in Office 365](#).

# Einrichten von Connectors zur Weiterleitung von E-Mails zwischen Office 365 und Ihren eigenen E-Mail-Servern

18.12.2018 • 24 minutes to read

Dieses Thema unterstützt Sie beim Einrichten von Connectors, die Sie für die folgenden zwei Szenarien benötigen:

- Sie haben Ihre eigenen E-Mail-Server (auch als lokale Server bezeichnet), und Sie abonnieren Exchange Online Protection (EOP) für E-Mail-Schutzdienste.
- Sie verfügen über (oder beabsichtigen) Postfächer an zwei Orten, einige Postfächer in Office 365, und einige auf E-Mail-Servern Ihrer Organisation (auch lokale Server bezeichnet).

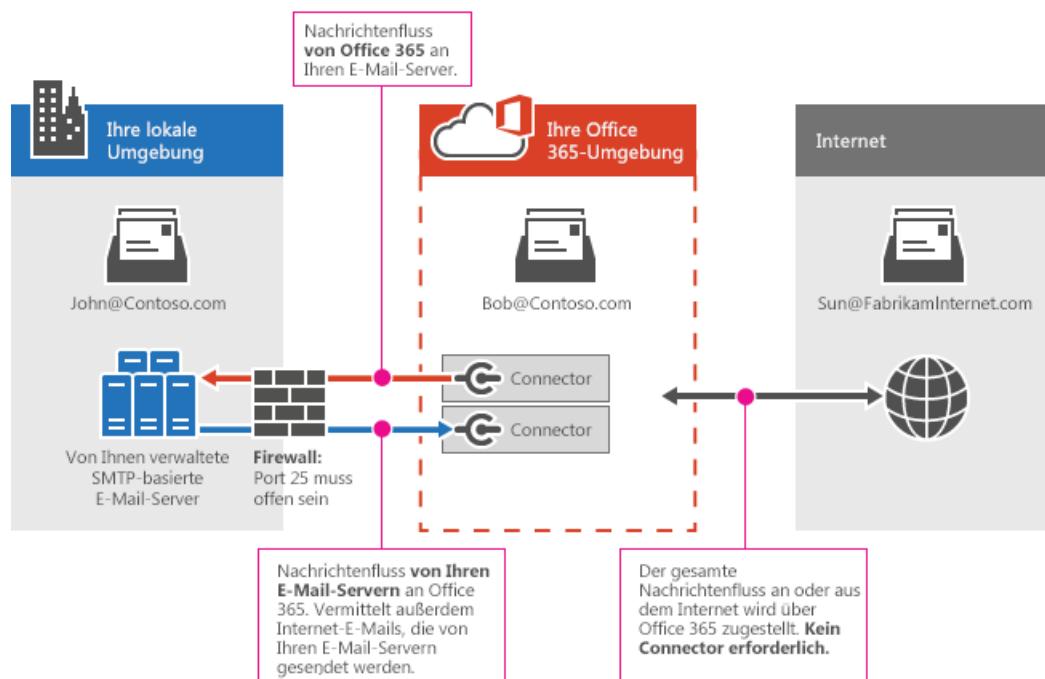
## NOTE

Bevor Sie beginnen, stellen Sie sicher, dass Sie auf Ihrer spezifischen Szenario in überprüfen [Was passiert, wenn ich meinen eigenen e-Mail-Servern haben?](#).

## Wie funktionieren Office 365-Connectors mit meinen eigenen (lokalen) Servern?

Wenn Sie über EOP und eigene E-Mail-Server verfügen oder sich einige Ihrer Postfächer in Office 365 und einige auf Ihren E-Mail-Servern befinden, können Sie Connectors einrichten, um den Nachrichtenfluss in beide Richtungen zu ermöglichen. Sie können den E-Mail-Fluss zwischen Office 365 und einem beliebigen SMTP-E-Mail-Server wie Exchange oder einem E-Mail-Server eines Drittanbieters aktivieren.

Die nachstehende Abbildung zeigt, wie Connectors in Office 365 (einschließlich Exchange Online oder EOP) mit Ihren eigenen E-Mail-Servern funktionieren.



In diesem Beispiel sind John und Bob Mitarbeiter in Ihrem Unternehmen. John hat ein Postfach auf einem E-Mail-Server, den Sie verwalten, und Bob verfügt über ein Postfach in Office 365. John und Bob tauschen E-Mails mit Sun aus, einem Kunden mit einem Internet-E-Mail-Konto:

- Zum Senden von E-Mails zwischen John und Bob sind Connectors erforderlich.
- Zum Senden von E-Mails zwischen John und Sun sind Connectors erforderlich. (Sämtliche Internet-E-Mails werden über Office 365 übermittelt.)
- Zum Senden von E-Mails zwischen Bob und Sun ist kein Connector erforderlich.

Wenn Sie über Ihre eigenen E-Mail-Server und Office 365 verfügen, müssen Sie Connectors einrichten. Ohne Connectors besteht kein E-Mail-Fluss zwischen Office 365 und den E-Mail-Servern Ihrer Organisation.

## Wie leiten Connectors E-Mails zwischen Office 365 und meinem eigenen E-Mail-Server weiter?

Sie benötigen zwei Connectors, um E-Mails wie folgt zwischen Office 365 und Ihren E-Mail-Servern zu leiten:

- **Ein Connector von Office 365 zu Ihrem eigenen E-Mail-Server**

Wenn Sie Office 365 so einrichten, dass alle E-Mails im Auftrag Ihrer Organisation akzeptiert werden, zeigen Sie mit dem MX-Eintrag (Mail Exchange) Ihrer Domäne auf Office 365. Zur Vorbereitung auf dieses E-Mail-Übermittelungsszenario müssen Sie einen alternativen Server (einen sogenannten Smarthost) festlegen, damit Office 365 E-Mails an den E-Mail-Server (den sogenannten lokalen Server) Ihrer Organisation senden kann. Zum Abschließen des Szenarios müssen Sie Ihren E-Mail-Server möglicherweise so konfigurieren, dass er Office 365 übermittelte Nachrichten akzeptiert.

- **Ein Connector von Ihrem eigenen E-Mail-Server zu Office 365**

Wenn dieser Connector eingerichtet ist, akzeptiert Office 365 Nachrichten vom E-Mail-Server Ihrer Organisation und sendet in Ihrem Auftrag Nachrichten an die entsprechenden Empfänger. Beim Empfänger kann es sich um ein Postfach für Ihre Organisation in Office 365 handeln. Alternativ kann sich ein Empfänger im Internet befinden. Zum Abschließen dieses Szenarios müssen Sie Ihren E-Mail-Server so konfigurieren, dass er E-Mails direkt an Office 365 sendet.

Dieser Connector ermöglicht Office 365, Ihre E-Mails auf Spam und Schadsoftware hin zu überprüfen, und er erzwingt Complianceanforderungen, beispielsweise das Ausführen von Richtlinien für die Verhinderung von Datenverlust. Wenn Ihr E-Mail-Server alle E-Mails direkt zu Office 365 sendet, sind Ihre IP-Adressen davor geschützt, zur Spamblockierliste hinzugefügt zu werden. Zum Abschließen des Szenarios müssen Sie Ihren E-Mail-Server möglicherweise so konfigurieren, dass er Nachrichten an Office 365 sendet.

### NOTE

Für dieses Szenario sind zwei Connectors erforderlich: einer von Office 365 zu Ihren E-Mail-Servern und einer zum Verwalten des E-Mail-Flusses aus der entgegengesetzten Richtung. Stellen Sie, bevor Sie anfangen, sicher, dass Sie über alle benötigten Informationen verfügen, und fahren Sie mit den Anweisungen fort, bis Sie beide Connectors eingerichtet und überprüft haben.

## Übersicht über die Schritte

Im Folgenden finden Sie eine Übersicht der Schritte:

- Schließen Sie die Voraussetzungen für Ihre E-Mail-Serverumgebung ab.
- **Teil 1:** Konfigurieren der e-Mail, um den Nachrichtenfluss von Office 365 zu Ihren e-Mail-Server.

- **Teil 2:** Konfigurieren von Mail flow von Ihrem e-Mail-Server zu Office 365.

## Voraussetzungen für Ihre E-Mail-Serverumgebung

Bereiten Sie Ihre Serverumgebung (auch als lokale Umgebung bezeichnet) vor, sodass eine Verbindung mit Office 365 hergestellt werden kann. Führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass Ihr E-Mail-Server (der sogenannte lokale E-Mail-Server) eingerichtet ist und E-Mails an das Internet senden und aus dem Internet empfangen kann.
2. Prüfen Sie, ob bei Ihrem lokalen E-Mail-Server Transport Layer Security (TLS) mit einem gültigen von einer Zertifizierungsstelle signierten Zertifikat aktiviert ist. Der Zertifikatantragstellername sollte den Domänennamen enthalten, der mit dem primären E-Mail-Server in Ihrer Organisation übereinstimmt. Kaufen Sie bei Bedarf ein digitales, von einer Zertifizierungsstelle signiertes Zertifikat, das mit dieser Beschreibung übereinstimmt.
3. Wenn Sie Zertifikate für die sichere Kommunikation zwischen Office 365 und Ihr e-Mail-Server verwenden möchten, aktualisieren Sie den Connector, den Ihre e-Mail-Server zum Empfangen von e-Mail verwendet werden. Dieser Connector muss das richtige Zertifikat erkennen, wenn Office 365, eine Verbindung mit dem Server versucht. Wenn Sie Exchange verwenden, finden Sie weitere Informationen unter [Receive Connectors](#). Konfigurieren Sie auf dem Edge-Transport-Server oder Client (Client Access Server, CAS) das Standardzertifikat für den Empfangsconnector. Aktualisieren des *TlsCertificateName* - Parameters im Cmdlet **Set-ReceiveConnector**, in der Exchange-Verwaltungsshell. Gewusst wie: Öffnen Sie die Exchange-Verwaltungsshell in Ihrer lokalen Exchange-Organisation finden Sie unter [der Exchange-Verwaltungsshell öffnen](#).
4. Notieren Sie sich den Namen oder die IP-Adresse Ihres außen zugänglichen E-Mail-Servers. Wenn Sie Exchange verwenden, ist dies der vollqualifizierte Domänenname Ihres Edge-Transport-Servers oder des Clientzugriffsservers, der E-Mails von Office 365 empfängt.
5. Öffnen Sie Port 25 in Ihrer Firewall, damit Office 365 eine Verbindung zu Ihren E-Mail-Servern herstellen kann.
6. Stellen Sie sicher, dass Ihre Firewall Verbindungen von allen Office 365-IP-Adressen akzeptiert. Unter [Exchange Online Protection IP addresses](#) erhalten Sie Informationen über den veröffentlichten IP-Adressbereich.
7. Notieren Sie sich eine E-Mail-Adresse für jede Domäne in Ihrer Organisation. Sie müssen später testen, ob Ihr Connector ordnungsgemäß funktioniert.

## Teil 1: Konfigurieren von E-Mails für den Fluss von Office 365 zu Ihrem E-Mail-Server

Dafür sind drei Schritte nötig:

1. Konfigurieren Sie Ihre Office 365-Umgebung.
2. Richten Sie einen Connector von Office 365 zu Ihrem E-Mail-Server ein.
3. Ändern Sie Ihren MX-Eintrag, um Ihren E-Mail-Fluss vom Internet zu Office 365 umzuleiten.

### 1. Konfigurieren Ihrer Office 365-Umgebung

Stellen Sie sicher, dass Sie Folgendes in Office 365 erledigt haben:

1. Wenn Sie Connectors einrichten, müssen Ihnen Berechtigungen zugewiesen sein, bevor Sie beginnen können. Welche Berechtigungen Sie benötigen, können Sie dem Eintrag „Office 365-Connectors“ im Thema [Feature permissions in EOP](#) entnehmen.

2. Wenn Sie möchten, dass EOP oder Exchange Online E-Mails von Ihren E-Mail-Servern an das Internet weiterleitet, gehen Sie wie folgt vor:

- Verwenden Sie ein Zertifikat, das mit einem Betreffnamen konfiguriert ist, der einer akzeptierte Domäne in Office 365 entspricht. Es wird empfohlen, dass der allgemeine Name des Zertifikats oder der alternative Antragstellername mit der primären SMTP-Domäne für Ihre Organisation übereinstimmt. Weitere Informationen hierzu finden Sie unter [Voraussetzungen für Ihre E-Mail-Serverumgebung](#).
- oder -
- Stellen Sie sicher, dass alle Absenderdomänen und -unterdomänen in Ihrer Organisation in Office 365 als akzeptierte Domänen konfiguriert sind.

Weitere Informationen zum Definieren von akzeptierten Domänen finden Sie unter [Verwalten akzeptierter Domänen in Exchange Online](#) und [Aktivieren der Nachrichtenübermittlung für Unterdomänen in Exchange Online](#).

3. Wählen Sie aus, ob Sie Transportregeln oder Domänennamen verwenden möchten, um E-Mails von Office 365 an Ihre E-Mail-Server zu übermitteln. Die meisten Unternehmen entscheiden sich dafür, E-Mails für alle akzeptierten Domänen zu übermitteln. Weitere Informationen finden Sie unter [Using a connector with a transport rule](#).

#### NOTE

Sie können die Transportregeln einrichten, wie in der [E-Mail-Fluss Regelaktionen in Exchange Online](#) beschrieben. Sie möchten beispielsweise Transportregeln mit Connectors verwenden, wenn Ihre Mail derzeit über Verteilerlisten zu mehreren Standorten gerichtet ist.

## 2. Einrichten eines Connectors von Office 365 zu Ihrem E-Mail-Server

Um in Office 365 einen Connector zu erstellen, wählen Sie **Administrator** aus, und klicken Sie dann auf **Exchange**, um zum Exchange-Verwaltungskonsole zu gelangen. Klicken Sie auf **E-Mail-Fluss** und auf **Connectors**.

Wenn bereits Connectors in Ihrer Organisation vorhanden sind, sind sie hier aufgelistet.

The screenshot shows the Exchange admin center interface. On the left, there's a navigation menu with items like dashboard, recipients, permissions, compliance management, organization, protection, and mail flow (which is highlighted with a pink box). The main content area has a header "Connectors" with a sub-header "Connectors help control the flow of email messages to and from your Office 365 organization. However, because most organizations don't need to use connectors, we recommend that you...". Below this is a "Want to help us improve connectors? Just send us feedback and let us know what you liked, didn't like, or what we can do to make your experience better." section. At the top right of the main area, there are four icons: a plus sign, a pencil, a trash bin, and a refresh symbol. Below these are two rows of connector details in a table:

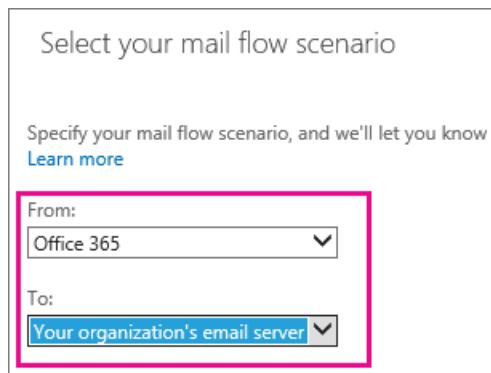
STATUS	NAME	FROM	TO
On	From Contoso Email server to Office 365	Your organization's email server	Office 365
On	From Office 365 to Contoso Email server	Office 365	Your organization's email server

At the bottom of the table area, there's a note: "Example connectors to and from Contoso email server".

Bevor Sie einen neuen Connector eingerichtet haben, überprüfen Sie alle Connectors, die für Ihre Organisation bereits hier aufgeführt sind. Angenommen, wenn Sie die Exchange- [Hybrid-Konfigurations-Assistenten](#) ausgeführt haben, werden Verbinder, die Nachrichtenübermittlung zwischen Office 365 und Exchange Server werden richten Sie bereits und hier aufgeführt. Sie müssen nicht neu einrichten, aber Sie können Bearbeiten Hier bei Bedarf. Richten Sie Wenn Sie nicht den Hybrid-Konfigurations-Assistenten

verwenden möchten oder wenn Sie Exchange Server 2007 oder früher ausführen oder wenn Sie einen nicht-Microsoft-SMTP-Mailserver ausführen, Connectors mithilfe des Assistenten.

Klicken Sie auf das Pluszeichen, +, um den Assistenten zu starten. Wählen Sie auf dem ersten Bildschirm die Optionen aus, die im folgenden Screenshot dargestellt sind:



Klicken Sie auf **Weiter**, und befolgen Sie die Anweisungen des Assistenten. Klicken Sie auf die Links **Hilfe** oder **Weitere Informationen**, wenn Sie weitere Informationen benötigen. Der Assistent führt Sie durch die Einrichtung. Stellen Sie am Ende sicher, dass Ihr Connector eine Bestätigung vornimmt. Wenn der Connector keine Bestätigung vornimmt, doppelklicken Sie auf angezeigte Meldung, um mehr Informationen zu erhalten, und lesen Sie [About fixing connector validation errors](#), um Hilfe zur Problembehebung zu erhalten.

### 3. Ändern Ihres MX-Eintrags zum Umleiten Ihres E-Mail-Flusses aus dem Internet zu Office 365

Ändern Sie zum Umleiten des E-Mail-Flusses zu Office 365 den MX-Eintrag (Mail Exchange) für Ihre Domäne. Informationen zur entsprechenden Vorgehensweise finden Sie unter [Hinzufügen eines MX-Eintrags](#).

## Teil 2: Konfigurieren von E-Mails für den Fluss von Ihrem E-Mail-Server zu Office 365

Dafür sind zwei Schritte nötig:

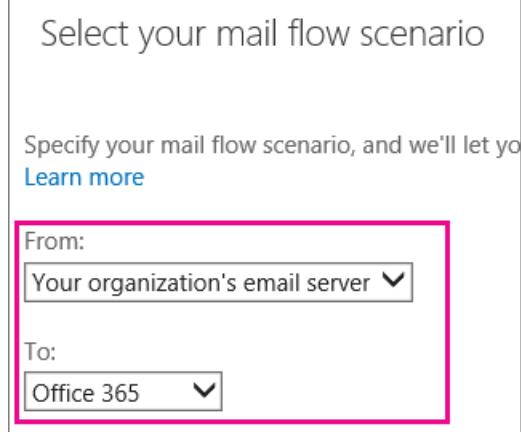
1. Richten Sie einen Connector von Ihrem E-Mail-Server zu Office 365 ein.
2. Richten Sie Ihren E-Mail-Server so ein, dass er E-Mails per Relay über Office 365 an das Internet weiterleitet.

Lesen Sie, sobald Sie Teil 2 abgeschlossen haben, die Anweisungen am Ende, um zu prüfen, ob Ihre Konfiguration konfiguriert.

### 1. Einrichten eines Connectors von Ihrem E-Mail-Server zu Office 365

Klicken Sie zum Erstellen eines Connectors im Office 365 auf **Administrator** und dann auf **Exchange**, um zum Exchange-Verwaltungskonsole zu gelangen. Klicken Sie dann auf **E-Mail-Fluss** und auf **Connectors**. Wenn bereits Connectors in Ihrer Organisation vorhanden sind, sind sie hier aufgelistet.

Klicken Sie auf das Pluszeichen, +, um den Assistenten zu starten. Wählen Sie auf dem ersten Bildschirm die Optionen aus, die im folgenden Screenshot dargestellt sind:



Klicken Sie auf **Weiter**, und befolgen Sie die Anweisungen des Assistenten Klicken Sie auf die Links **Hilfe** oder **Weitere Informationen**, wenn Sie weitere Informationen benötigen. Siehe insbesondere [Identifying email from your email server](#), um Informationen zur Konfiguration von Zertifikat- oder IP-Adresseneinstellungen für diesen Connector zu erhalten. Der Assistent führt Sie durch die Einrichtung. Speichern Sie abschließend Ihren Connector.

## 2. Einrichten Ihres E-Mail-Servers zum Weiterleiten Ihrer E-Mails per Relay über Office 365 an das Internet

Als Nächstes müssen Sie Ihren E-Mail-Server so vorbereiten, dass er E-Mails an Office 365 sendet. Dadurch wird der E-Mail-Fluss von Ihren E-Mail-Servern über Office 365 an das Internet ermöglicht.

Konfigurieren Sie auf Ihrem Exchange-Server einen Sendeconnector zum Senden von e-Mails über einen Smarthost zu Office 365. Anweisungen zur Verwendung mit Exchange Server dazu finden Sie unter [Erstellen eines Sendeconnectors zum Weiterleiten von ausgehenden e-Mails über einen Smarthost](#). Anweisungen zur Verwendung mit Exchange Server 2010 dazu finden Sie unter [Erstellen eines SMTP-Connectors senden](#).

Verwenden Sie die folgende Syntax in Exchange Online PowerShell, um den Sendeconnector in Exchange Server zu erstellen. Gewusst wie: Öffnen Sie Exchange Online PowerShell in Ihrer lokalen Exchange-Organisation finden Sie unter [Exchange Online PowerShell öffnen](#).

```
New-SendConnector -Name <DescriptiveName> -AddressSpaces * -CloudServicesMailEnabled $true -Fqdn <CertificateHostNameValue> -RequireTLS $true -DNSRoutingEnabled $false -SmartHosts <YourDomain>-com.mail.protection.outlook.com -TlsAuthLevel CertificateValidation
```

In diesem Beispiel wird ein neuer Sendeconnector mit den folgenden Eigenschaften erstellt:

- **Name:** Mein Unternehmen zu Office 365
- **FQDN** mail.contoso.com
- **SmartHosts** contoso-com.mail.protection.outlook.com

```
New-SendConnector -Name "My company to Office 365" -AddressSpaces * -CloudServicesMailEnabled $true -Fqdn mail.contoso.com -RequireTLS $true -DNSRoutingEnabled $false -SmartHosts contoso-com.mail.protection.outlook.com -TlsAuthLevel CertificateValidation
```

Nachfolgend finden Sie eine Beispiel- **PowerShell** -Cmdlets zur einfacheren den Sendeconnector in Exchange Server zu konfigurieren:

```
New-SendConnector -Name "My company to Office 365" -AddressSpaces * -CloudServicesMailEnabled $true -Fqdn "cert domain name, such as mail.contoso.com" -RequireTLS $true -SmartHosts yourdomain-com.mail.protection.outlook.com -TlsAuthLevel CertificateValidation
```

Wie weiß ich, ob die Connectors meine Organisations-E-Mails richtig

## weiterleiten?

Wenn Sie all diese Schritte ordnungsgemäß vorgenommen haben, werden Ihre gesamten E-Mails nun über Office 365 übermittelt.

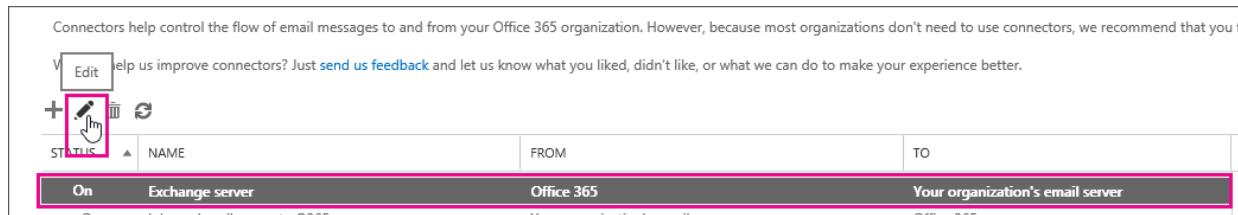
So nehmen Sie eine Funktionsprüfung vor

1. Senden Sie E-Mails von einem Postfach auf Ihrem E-Mail-Server an ein Internetpostfach.
2. Senden Sie E-Mails von einem Internetpostfach an ein Postfach auf Ihrem E-Mail-Server.

Stellen Sie sicher, dass beide E-Mails empfangen werden.

## Ändern eines von Office 365 für den Nachrichtenfluss verwendeten Connectors

Wählen Sie zum Ändern der Einstellungen für einen Connector den gewünschten Connector aus, und wählen Sie dann das Symbol „Bearbeiten“, wie im folgenden Screenshot dargestellt.



Der Connector-Assistent wird geöffnet. Sie können nun die Änderungen an den vorhandenen Connectoreinstellungen vornehmen. In der Zeit, in der Sie Änderungen an den Connectoreinstellungen vornehmen, verwendet Office 365 weiterhin die vorhandenen Connectoreinstellungen für den Nachrichtenfluss. Beim Speichern der Änderungen an dem Connector beginnt Office 365, die neuen Einstellungen zu verwenden.

## Was passiert, wenn ich über mehrere Connectors für das gleiche Szenario verfüge?

Die meisten Kunden müssen keine Connectors einrichten. Für diejenigen, die Connectors einrichten müssen, ist in der Regel ein Connector pro Nachrichtenflussrichtung ausreichend. Sie können aber auch mehrere Connectors für eine Nachrichtenflussrichtung erstellen, z. B. für den Nachrichtenfluss von Office 365 an Ihren (lokalen) E-Mail-Server.

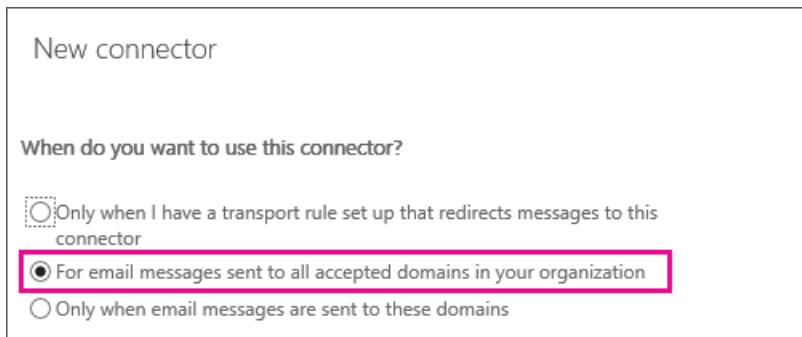
Wenn mehrere Connectors vorhanden sind, besteht der erste Schritt bei der Behebung von Problemen mit dem E-Mail-Fluss darin, herauszufinden, welchen Connector Office 365 verwendet. Office 365 verwendet die folgende Reihenfolge, um einen Connector zu Anwenden auf eine E-Mail auszuwählen:

1. Verwenden eines Connectors, der genau mit der Domäne des Empfängers übereinstimmt
2. Verwenden eines Connectors, der für alle akzeptierten Domänen gilt
3. Verwenden von Platzhalter-Mustervergleichen. \*. contoso.com würde z. B. mit mail.contoso.com sowie sales.contoso.com übereinstimmen.

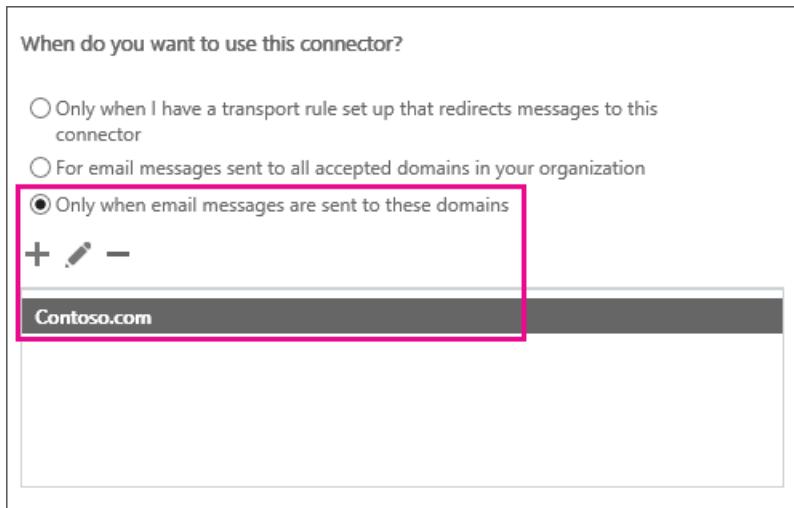
### Beispiel für die Verwendung mehrerer Connectors in Office 365

In diesem Beispiel verfügt Ihre Organisation über vier akzeptierte Domänen: contoso.com, sales.contoso.com, fabrikam.com und beispielsweise contoso.onmicrosoft.com. Sie verfügen über drei Connectors, die über Office 365 für den E-Mail-Server Ihrer Organisation konfiguriert wurden. In diesem Beispiel werden diese Connectors **Connector1**, **Connector2** und **Connector3** genannt.

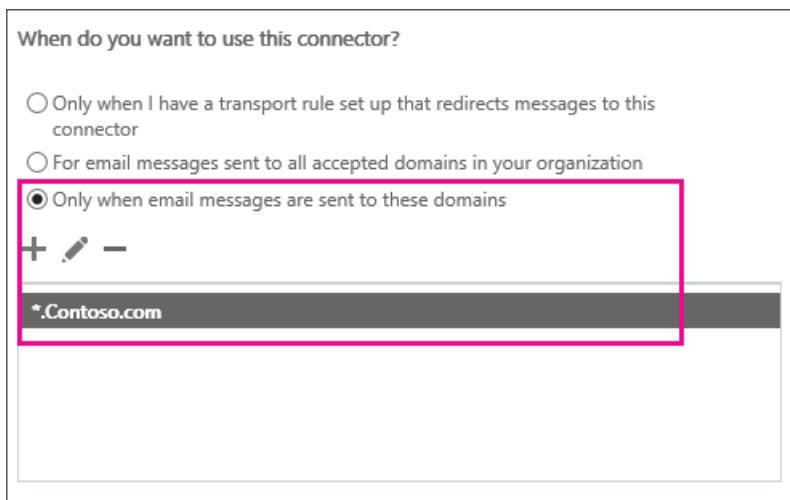
**Connector1** ist für alle akzeptierten Domänen in Ihrer Organisation konfiguriert. Der folgende Screenshot zeigt den Connector-Assistenten, in dem Sie die Domänen definieren, für die die Connectors verwendet werden sollen. In diesem Fall ist die folgende Einstellung ausgewählt: **Für an alle akzeptierten Domänen in Ihrer Organisation gesendete E-Mails.**



**Connector2** ist speziell für Ihre Unternehmensdomäne „contoso.com“ eingerichtet. Der folgende Screenshot zeigt den Connector-Assistenten, in dem Sie die Domänen definieren, für die die Connectors verwendet werden sollen. In diesem Fall ist die folgende Einstellung ausgewählt: **Nur, wenn E-Mails an diese Domänen gesendet werden.** Für **Connector2** ist Ihre Unternehmensdomäne „contoso.com“ angegeben.



**Connector3** ist ebenfalls durch die Verwendung der Option **Nur, wenn E-Mails an diese Domänen gesendet werden** eingerichtet. Anstelle der Domäne „Contoso.com“ verwendet der Connector einen Platzhalter: \*.Contoso.com, wie im folgenden Screenshot dargestellt.



Für jede von Office 365 an Postfächern auf Ihrem E-Mail-Server gesendete E-Mail wählt Office 365 den genauesten Connector aus. Für E-Mails an:

- john@fabrikam.com, Office 365 wählt den **Connector 1** aus.

- john@contoso.com, Office 365 wählt den **Connector 2** aus.
- john@sales.contoso.com wählt Office 365 den **Connector3**.

## See also

[Configure mail flow using connectors in Office 365](#)

[Bewährte Methoden für die Nachrichtenübermittlung für Exchange Online und Office 365 \(Übersicht\)](#)

[Validieren von Connectors in Office 365](#)

[Einrichten von Connectors für den sicheren Nachrichtenfluss mit einer Partnerorganisation](#)

# Einrichten von Connectors für den sicheren Nachrichtenfluss mit einer Partnerorganisation

18.12.2018 • 17 minutes to read

Sie können Connectors erstellen, um Sicherheitsbeschränkungen auf den E-Mail-Austausch mit einer Partnerorganisation oder einem Dienstanbieter anzuwenden. Ein Partner kann eine Organisation sein, mit der Sie in Geschäftsbeziehung stehen, z. B. eine Bank. Es kann sich auch um einen Clouddienst eines Drittanbieters handeln, der Dienste wie Archivierung, Spamschutz und Filterung bereitstellt.

Sie können einen Connector erstellen, um die Verschlüsselung über Transport Layer Security (TLS) zu erzwingen. Sie können auch andere Sicherheitsbeschränkungen anwenden, beispielsweise das Angeben von Domänennamen oder IP-Adressbereichen, aus denen Ihre Partnerorganisation E-Mails sendet.

## NOTE

Das Einrichten eines Connectors für den Austausch von E-Mails mit einer Partnerorganisation ist optional. Der Nachrichtenfluss zu und vor Ihrer Partnerorganisation erfolgt ohne Connectors.

Wenn Sie einen Drittanbieter-Cloud-Dienst für e-Mail-Filterung verwenden, benötigen Anweisungen zum Durchführen dieser Arbeit mit Office 365 finden Sie unter [Mail Flow best Practices für Exchange Online und Office 365 \(Übersicht\)](#).

## Verwenden von Connectors für den E-Mail-Verkehr mit einer Partnerorganisation

Standardmäßig sendet Office 365 E-Mail-Nachrichten mithilfe der TLS-Verschlüsselung, vorausgesetzt, dass der Zielserver auch TLS unterstützt. Wenn Ihre Partnerorganisation TLS unterstützt, müssen Sie nur einen Connector erstellen, wenn Sie bestimmte Sicherheitseinschränkungen erzwingen möchten - z. B. soll TLS immer angewendet werden, oder erfordern Sie eine Zertifikatsüberprüfung, wenn Nachrichten von Ihrem Partner an Ihre Organisation gesendet werden.

## NOTE

Informationen zu TLS finden Sie unter [Verwendung von TLS in Exchange Online für sichere E-Mail-Verbindungen in Office 365](#), und detaillierte technische Informationen darüber, wie Exchange Online die Reihenfolge der TLS-Verschlüsselungssammlungen verwendet, finden Sie unter [Verbesserung der E-Mail-Fluss-Sicherheit für Exchange Online](#).

Beim Festlegen eines Connectors werden alle E-Mails überprüft, um sicherzustellen, dass sie die von Ihnen angegebenen Sicherheitseinschränkungen erfüllen. Wenn E-Mails die von Ihnen angegebenen Sicherheitseinschränkungen nicht erfüllen, werden sie durch den Connector abgelehnt, wodurch diese Nachrichten nicht gesendet werden. Dadurch wird die Einrichtung eines sicheren Kommunikationskanals mit einer Partnerorganisation ermöglicht.

Sie können je nach Ihren Anforderungen entweder einen oder beide Schritte durchführen:

- [Einrichten eines Connectors zum Anwenden von Sicherheitseinschränkungen auf von Ihnen über Office 365 an Ihre Partnerorganisation gesendete E-Mails](#)
- [Einrichten eines Connectors zum Anwenden von Sicherheitseinschränkungen auf von Ihrer](#)

## Partnerorganisation über Office 365 an Sie gesendete E-Mails

Inhalt dieses Artikels:

- Ändern eines von Office 365 für den Nachrichtenfluss verwendeten Connectors
- Auf von einer Partnerorganisation gesendete E-Mails anwendbare Beispielsicherheitseinschränkungen

Lesen Sie diesen Abschnitt, um die bestimmten Einstellungen zu ermitteln, die Sie für Ihr Unternehmen benötigen.

## Einrichten eines Connectors zum Anwenden von Sicherheitseinschränkungen auf von Ihnen über Office 365 an Ihre Partnerorganisation gesendete E-Mails

Um einen Connector in Office 365 erstellen, klicken Sie auf **Administrator**, und klicken Sie auf **Exchange** um in die **Exchange-Verwaltungskonsole** zu wechseln. Im nächsten Schritt auf **e-Mail-Fluss**, und klicken Sie auf **Connectors**. Wenn Connectors für Ihre Organisation bereits vorhanden sind, können Sie sie die hier aufgeführten angezeigt.

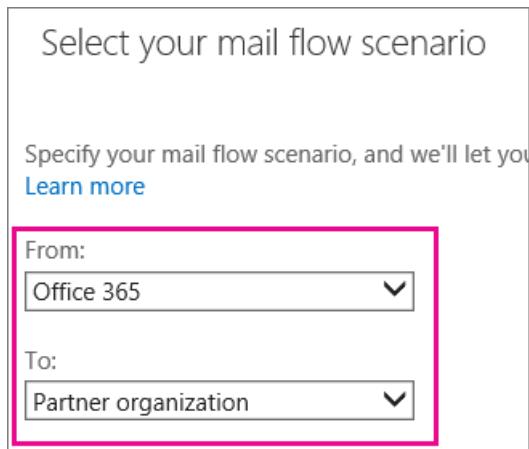
The screenshot shows the 'Connectors' section of the Microsoft Exchange Admin Center. At the top, there are navigation links: 'rules', 'message trace', 'accepted domains', 'remote domains', and 'connectors'. The 'connectors' link is highlighted with a red box. Below the links, there is a note about connectors helping to control email flow between the organization and external partners. A feedback link is provided. At the bottom, there is a table listing two existing connectors, both of which are currently active ('On'). The first connector, 'Receive From ContosoBank.com', maps 'Partner organization' to 'Office 365'. The second connector, 'Send To ContosoBank.com', maps 'Office 365' to 'Partner organization'. A red box highlights the entire table. A callout box at the bottom points to the table with the text 'Example Partner Organization connectors'.

STATUS	NAME	FROM	TO
On	Receive From ContosoBank.com	Partner organization	Office 365
On	Send To ContosoBank.com	Office 365	Partner organization

Example Partner Organization connectors

Prüfen Sie vor dem Einrichten eines neuen Connectors die Connectors, die hier bereits für Ihre Organisation aufgelistet sind. Wenn Sie beispielsweise über einen eingerichteten Connector für eine Partnerorganisation verfügen, wird er aufgelistet. Stellen Sie sicher, dass Sie keine doppelte Connectors für einen einzelnen Organisationspartner erstellen. Wenn dies geschieht, kann dies Fehler verursachen, wodurch Ihre E-Mails möglicherweise nicht übermittelt werden.

Klicken Sie auf das Pluszeichen, +, um den Assistenten zu starten. Wählen Sie auf dem ersten Bildschirm die Optionen aus, die im folgenden Screenshot dargestellt sind:

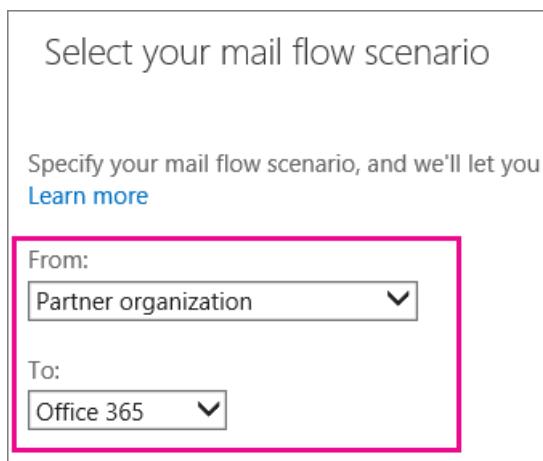


Klicken Sie auf **Weiter**, und befolgen Sie die Anweisungen des Assistenten Klicken Sie auf die Links **Hilfe** oder **Weitere Informationen**, wenn Sie weitere Informationen benötigen. Der Assistent führt Sie durch die Einrichtung. Stellen Sie am Ende sicher, dass Ihr Connector eine Bestätigung vornimmt. Wenn der Connector keine Bestätigung vornimmt, lesen Sie [About fixing connector validation errors](#), um Hilfe zur Behebung von Problemen zu erhalten.

Wenn Sie einen sicheren Kanal mit Ihrer Partnerorganisation in beiden Richtungen erstellen möchten, richten Sie einen Connector ein, der den E-Mail-Fluss von Ihrer Partnerorganisation zu Office 365 einschränkt.

## Einrichten eines Connectors zum Anwenden von Sicherheitseinschränkungen auf von Ihrer Partnerorganisation über Office 365 an Sie gesendete E-Mails

Sie können einen Connector einrichten, um Sicherheitseinschränkungen auf E-Mails anzuwenden, die Ihnen Ihre Partnerorganisation sendet. Klicken Sie zum Starten des Assistenten auf das Plussymbol +. Wählen Sie auf dem ersten Bildschirm die folgenden Optionen aus:

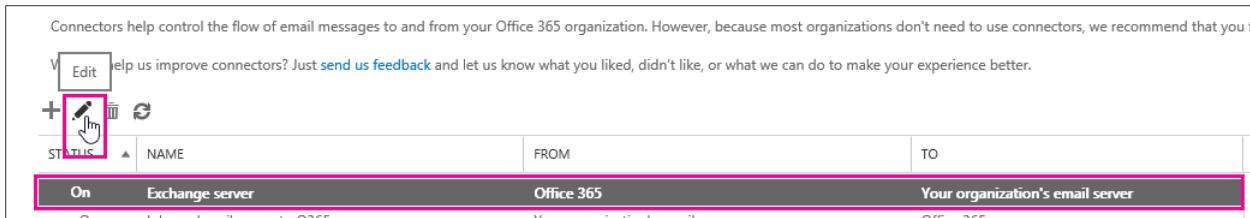


Klicken Sie auf **Weiter**, und befolgen Sie die Anweisungen des Assistenten Klicken Sie auf die Links **Hilfe** oder **Weitere Informationen**, wenn Sie weitere Informationen benötigen. Der Assistent führt Sie durch die Einrichtung. Speichern Sie abschließend Ihren Connector.

Bitten Sie Ihre Partnerorganisation, Ihnen eine Test-E-Mail zu senden. Stellen Sie sicher, dass die durch Ihre Partnerorganisation an Sie gesendete E-Mail dazu führt, dass der Connector angewendet wird. Wenn Sie beispielsweise Sicherheitseinschränkungen für E-Mails angegeben haben, die von einer bestimmten Partnerdomäne gesendet wurden, stellen Sie sicher, dass eine Test-E-Mail über diese Domäne gesendet wird. Prüfen Sie, ob die Test-E-Mail übermittelt wird, um sicherzustellen, dass der Connector ordnungsgemäß funktioniert.

# Ändern eines von Office 365 für den Nachrichtenfluss verwendeten Connectors

Wählen Sie zum Ändern der Einstellungen für einen Connector den gewünschten Connector aus, und wählen Sie dann das Symbol „Bearbeiten“, wie im folgenden Screenshot dargestellt.



Der Connector-Assistent wird geöffnet. Sie können nun die Änderungen an den vorhandenen Connectoreinstellungen vornehmen. In der Zeit, in der Sie Änderungen an den Connectoreinstellungen vornehmen, verwendet Office 365 weiterhin die vorhandenen Connectoreinstellungen für den Nachrichtenfluss. Beim Speichern der Änderungen an dem Connector beginnt Office 365, die neuen Einstellungen zu verwenden.

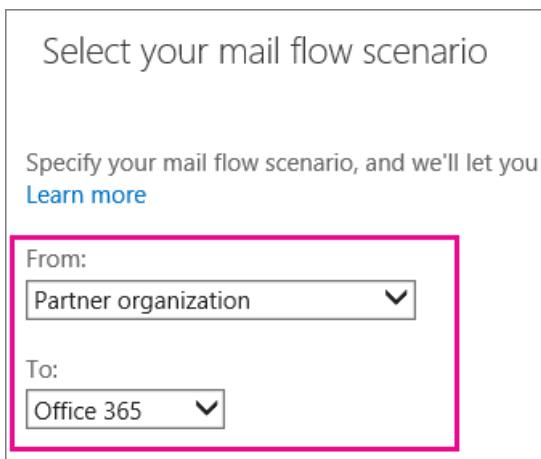
## Auf von einer Partnerorganisation gesendete E-Mails anwendbare Beispieldurchsetzungseinschränkungen

Lesen Sie diese Connectorbeispiele, die Ihnen bei der Entscheidung helfen, ob Sie Sicherheitseinschränkungen auf E-Mails anwenden möchten, die durch eine Partnerorganisation versendet wurden. Zudem helfen Ihnen die Beispiele beim Verstehen, welche Einstellungen Ihre Unternehmensanforderungen erfüllen.

### Erstellen eines Partnerorganisationsconnectors

Um einen Connector in Office 365 erstellen möchten, klicken Sie auf **Administrator**, und klicken Sie dann auf **Exchange** um in die **Exchange-Verwaltungskonsole** zu wechseln. Im nächsten Schritt auf **e-Mail-Fluss**, und klicken Sie auf **Connectors**. Wenn Connectors für Ihre Organisation bereits vorhanden sind, können Sie sie die hier aufgeführten anzeigen.

Klicken Sie zum Starten des Assistenten auf das Plussymbol +. Verwenden Sie zum Erstellen eines Connectors für von einer Partnerorganisation empfangene E-Mails die im folgenden Screenshot dargestellten Optionen:



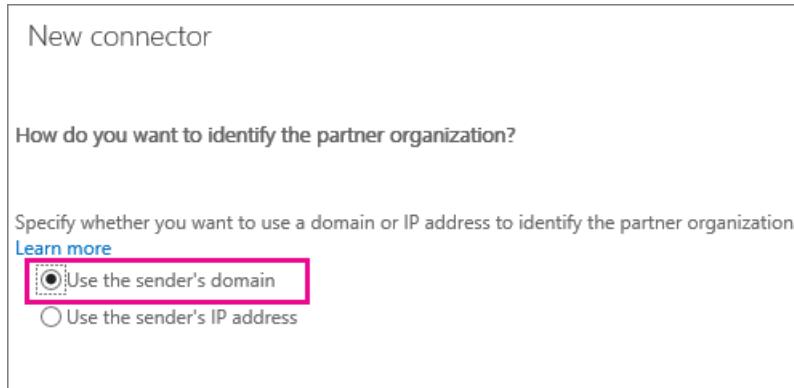
Nachdem Sie dieses E-Mail-Flussszenario ausgewählt haben, können Sie einen Connector einrichten, der Sicherheitseinschränkungen auf E-Mails anwendet, die von Ihnen von Ihrer Partnerorganisation gesendet werden. Aus einigen Sicherheitsgründen müssen Sie sich an Ihre Partnerorganisation wenden, um Informationen abzurufen, damit einige der Einstellungen abgeschlossen werden können. Lesen Sie die Beispiele, die Ihren Anforderungen am besten entsprechen. Diese helfen Ihnen beim Einrichten Ihres Partnerconnectors.

**NOTE**

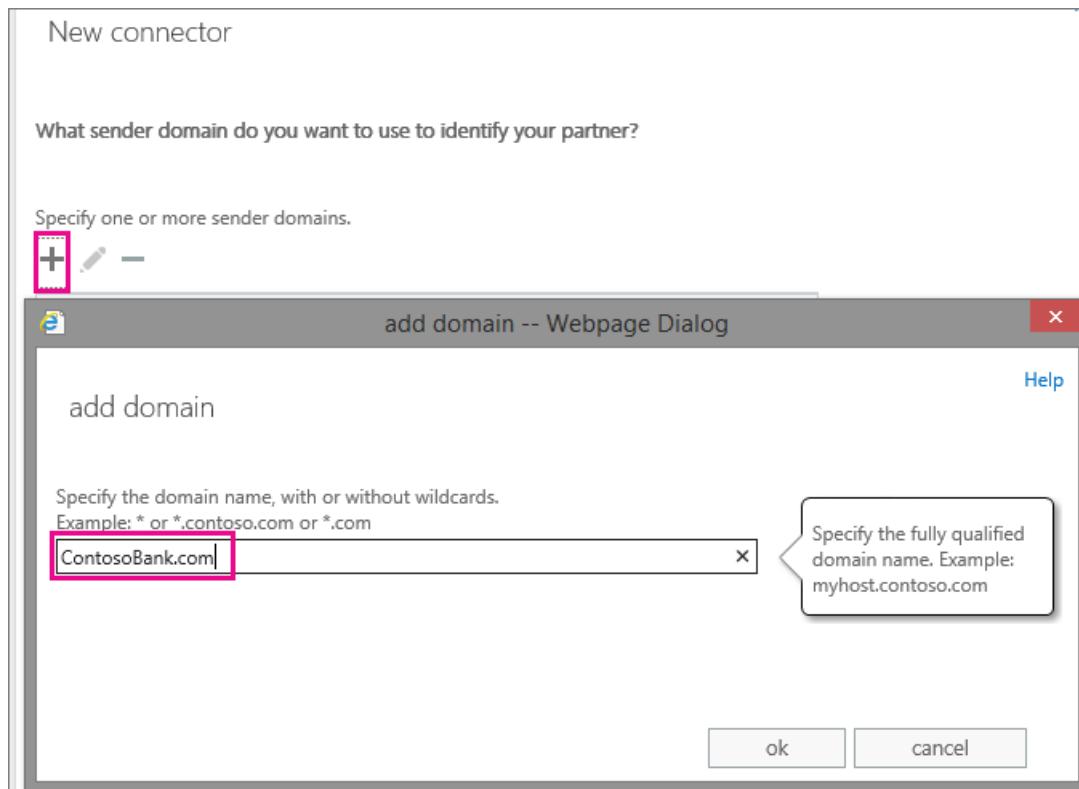
Von Ihrer Partnerorganisation gesendete E-Mails, die von Ihnen angegebenen Sicherheitseinschränkungen nicht erfüllen, werden nicht übermittelt.

**Beispiel 1: Von Ihrer Partnerorganisationsdomäne „contosobank.com“ gesendete E-Mails sollen verschlüsselt sein mithilfe von Transport Layer Security (TLS)**

Geben Sie dafür den Domänennamen Ihrer Partnerorganisation an, um E-Mails von diesem Partner zu bestimmen, und wählen Sie beim Erstellen Ihres Partners zum Office 365-Connector die TLS-Verschlüsselung (Transport Layer Security) aus. Verwenden Sie während der Einrichtung diese Optionen:



Verwenden Sie diesen Bildschirm, um den bzw. die Domänenname(n) Ihrer Partnerorganisation einzugeben, damit der Connector durch Ihren Partner gesendete E-Mails bestimmen kann:



Wählen Sie diese Einstellung aus, um die Verschlüsselung für alle E-Mails aus „ContosoBank.com“ mit TLS erforderlich zu machen:

## New connector

What security restrictions do you want to apply?

- Reject email messages if they aren't sent over TLS  
 And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name

Example: contoso.com or \*.contoso.com

Bei Auswahl dieser Einstellungen müssen alle E-Mails von der Domäne „ContosoBank.com“ Ihrer Partnerorganisation mit TLS verschlüsselt sein. Nicht verschlüsselte E-Mails werden abgelehnt.

### **Beispiel 2: Von der Domäne „ContosoBank.com“ Ihrer Partnerorganisation gesendete E-Mails sollen verschlüsselt sein und ihr Domänenzertifikat verwenden**

Verwenden Sie dafür alle in Beispiel 1 gezeigten Einstellungen. Fügen Sie zudem den Zertifikatsdomänennamen hinzu, den Ihre Partnerorganisation verwendet, um eine Verbindung mit Office 365 herzustellen. Verwenden Sie während der Einrichtung diese Option:

## New connector

What security restrictions do you want to apply?

- Reject email messages if they aren't sent over TLS  
 And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name

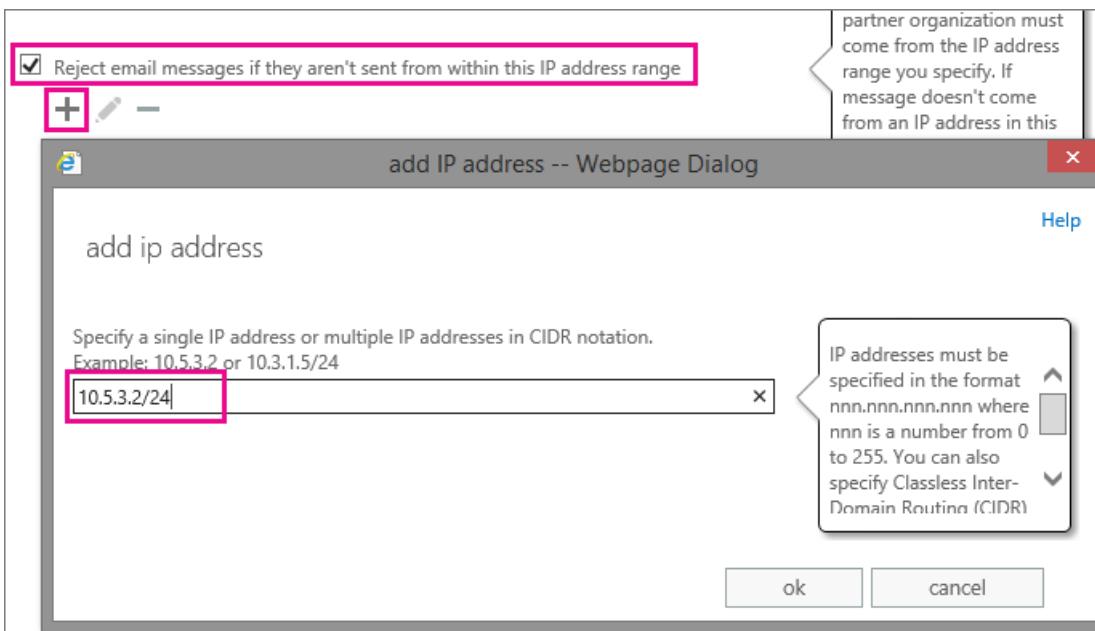
ContosoBank.com

Beim Festlegen dieser Einschränkungen müssen alle E-Mails aus der Domäne Ihrer Partnerorganisation mit TLS verschlüsselt werden und über einen Server mit dem von Ihnen angegebenen Zertifikatsnamen gesendet werden. E-Mails, die diese Bedingungen nicht erfüllen, werden abgelehnt.

### **Beispiel 3: Alle E-Mails müssen von einem bestimmten IP-Adressbereich gesendet werden**

Diese E-Mail könnte von einem Partnerunternehmen, wie z. B. ContosoBank.com, oder von Ihrer lokalen Umgebung stammen. Beispiel: Der MX-Eintrag für Ihre Domäne „contoso.com“ verweist auf die lokale Umgebung, und Sie möchten, dass alle an „contoso.com“ gesendeten Nachrichten nur von Ihren lokalen IP-Adressen stammen. Dadurch wird Spoofing verhindert und sichergestellt, dass die Compliancerichtlinien für alle Nachrichten erzwungen werden können.

Geben Sie dafür den Domänennamen Ihrer Partnerorganisation an, um E-Mails von diesem Partner zu bestimmen, und schränken Sie dann die IP-Adressen ein, von denen Sie E-Mails akzeptieren. Durch die Verwendung einer IP-Adresse wird der Connector spezifischer, da er eine einzelne Adresse oder einen Adressbereich bestimmt, von der bzw. von dem aus Ihrer Partnerorganisation E-Mails sendet. Geben Sie die Domäne Ihres Partners wie in Beispiel 1 beschrieben ein, und verwenden Sie diese Option während der Einrichtung:



Beim Festlegen dieser Einschränkungen müssen alle über die Domäne „ContosoBank.com“ Ihrer Partnerorganisation oder über die lokale Umgebung gesendete E-Mails über die IP-Adresse bzw. einen Adressbereich gesendet werden, die bzw. den Sie angeben. E-Mails, die diese Bedingungen nicht erfüllen, werden abgelehnt.

#### **Beispiel 4: Sämtliche über das Internet an Ihre Organisation gesendete E-Mails sollen über eine bestimmte IP-Adresse gesendet werden (Drittanbieter-E-Mail-Dienstszenario)**

E-Mail-Fluss zu Office 365 Works ohne eine Verbindung von einem Drittanbieter-e-Mail-Dienst. Jedoch in diesem Szenario können optional einen Connector Sie um alle e-Mail-Übermittlung an Ihrer Organisation zu beschränken. Wenn Sie die Einstellungen in diesem Beispiel beschrieben verwenden, gelten sie für *Alle e-Mails, die an Ihrer Organisation gesendet*. Wenn alle e-Mails an die Organisation gesendeten aus einem einzelnen Drittanbieter-e-Mail-Dienst stammt, können Sie optional eine Verbindung zum Einschränken von allen e-Mail-Übermittlung verwenden. nur Nachrichten aus einer einzelnen IP-Adresse oder Adressbereich gesendet wird übermittelt werden.

#### **NOTE**

Stellen Sie sicher, dass die den vollständigen Bereich der IP-Adressen bestimmen, von dem aus der Drittanbieter-E-Mail-Dienst E-Mails sendet. Wenn Sie eine IP-Adresse nicht berücksichtigen oder wenn eine ohne Ihr Wissen hinzugefügt wird, werden einige E-Mails nicht an Ihre Organisation übermittelt.

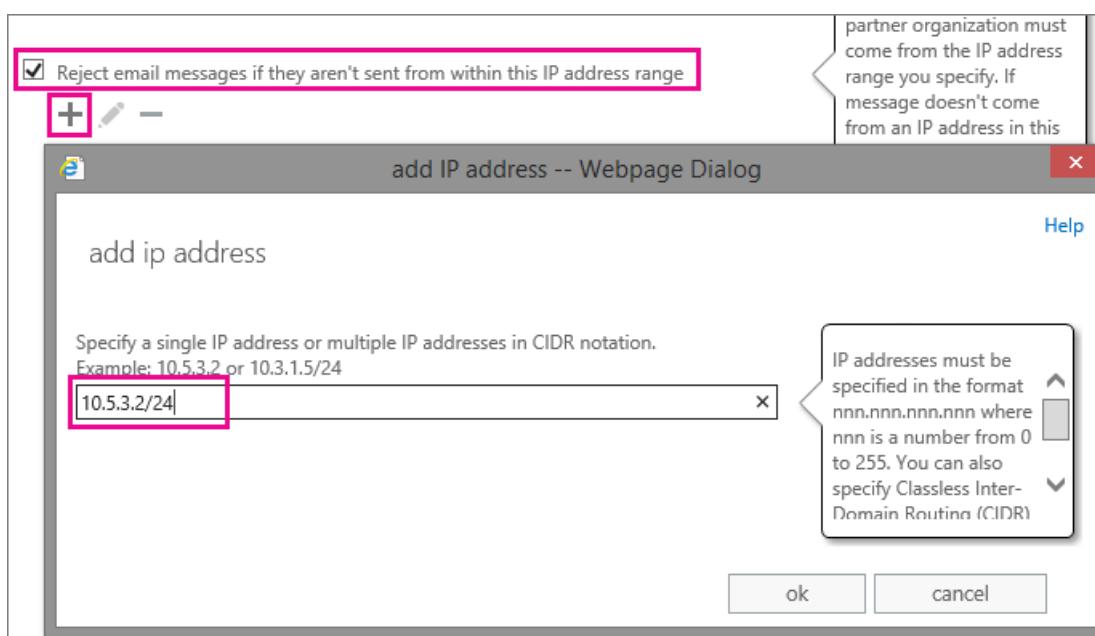
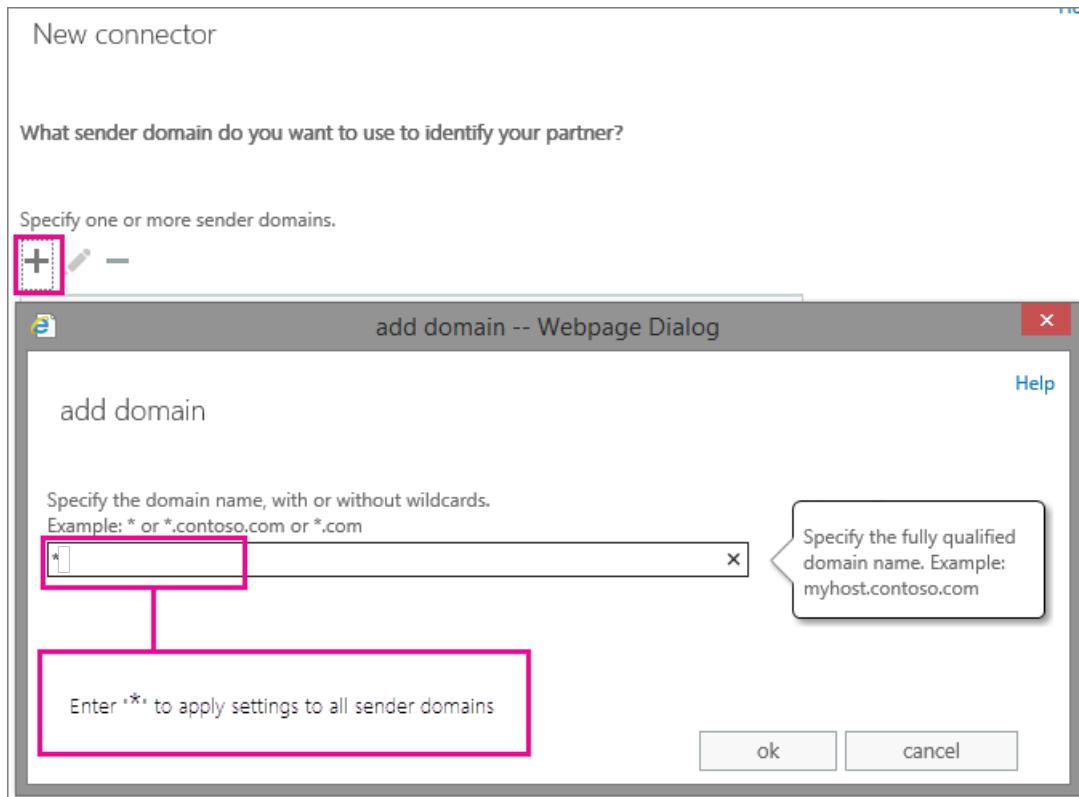
Verwenden Sie diese Optionen während der Einrichtung, um alle an Ihre Organisation gesendeten E-Mails auf eine bestimmte IP-Adresse oder einen -Adressbereich einzuschränken:

New connector

How do you want to identify the partner organization?

Specify whether you want to use a domain or IP address to identify the partner organization.  
[Learn more](#)

Use the sender's domain  
 Use the sender's IP address



Beim Festlegen dieser Einschränkungen müssen alle an Ihre Organisation gesendeten E-Mails über einen bestimmten IP-Adressbereich gesendet werden. Internet-E-Mails, die nicht aus diesem IP-Adressbereich stammen, werden abgelehnt.

**Beispiel 5: Alle über die IP-Adresse oder den -Adressbereich Ihrer Partnerorganisation gesendeten E-Mails sollen mit TLS verschlüsselt sein**

Verwenden Sie diese Optionen während der Einrichtung, um Ihre Partnerorganisation nach IP-Adresse zu bestimmen:

## New connector

How do you want to identify the partner organization?

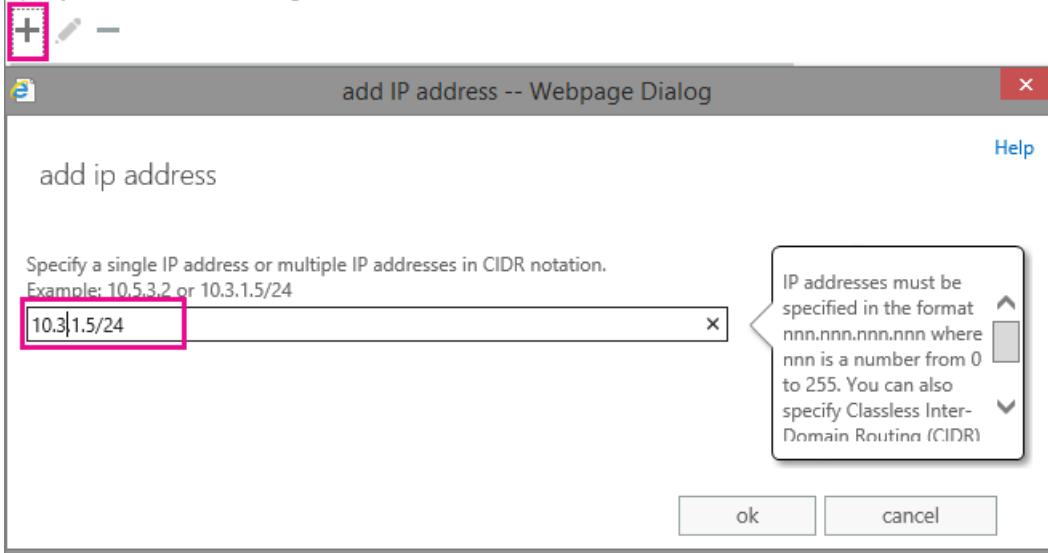
Specify whether you want to use a domain or IP address to identify the partner organization.  
[Learn more](#)

- Use the sender's domain  
 Use the sender's IP address

## New connector

What sender IP addresses do you want to use to identify your partner?

Specify the sender IP address range.



Fügen Sie die Anforderung für die TLS-Verschlüsselung mithilfe dieser Einstellung hinzu:

## New connector

What security restrictions do you want to apply?

- Reject email messages if they aren't sent over TLS  
 And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name

Example: contoso.com or \*.contoso.com

Beim Festlegen dieser Einschränkungen müssen alle über die IP-Adresse oder den -Adressbereich, die bzw. den Sie festlegen, von Ihrer Partnerorganisation gesendeten E-Mails mit TLS verschlüsselt sein. E-Mails, die diese Einschränkung nicht erfüllen, werden abgelehnt.

## Siehe auch

[Configure mail flow using connectors in Office 365](#)

[Bewährte Methoden für die Nachrichtenübermittlung für Exchange Online und Office 365 \(Übersicht\)](#)

About fixing connector validation errors

Was passiert, wenn ich über mehrere Connectors für das gleiche Szenario verfüge?

# Validieren von Connectors in Office 365

18.12.2018 • 5 minutes to read

Wenn Ihre Organisation über einen eigenen E-Mail-Server (auch als lokaler Server bezeichnet) verfügt, müssen Sie Connectors so einrichten, dass der E-Mail-Fluss zwischen Office 365 und Ihrem E-Mail-Server aktiviert wird. Für einen ordnungsgemäßen E-Mail-Fluss müssen die Connectors überprüft und aktiviert sein. Die Connectorüberprüfung wird als Teil des Connector-Einrichtungsprozesses ausgeführt. Dieser Artikel soll Ihnen helfen, wenn Sie Ihre Connectors zu einem anderen Zeitpunkt überprüfen möchten, oder wenn Sie weitere Informationen zu dem Prozess verstehen möchten. Verwenden Sie die integrierte Connectorüberprüfung, um zu testen, ob ein Connector ordnungsgemäß eingerichtet ist, und beheben Sie alle Probleme beim E-Mail-Fluss, bevor Sie den Connector aktivieren.

## NOTE

Wenn Sie Connectoreinstellungen ändern möchten, verwendet Office 365 die vorhandenen Connectoreinstellungen für den E-Mail-Fluss, bis Sie Ihre Änderungen speichern. Weitere Informationen finden Sie unter [Ändern eines von Office 365 für den Nachrichtenfluss verwendeten Connectors](#)

## Überprüfen und Aktivieren von Connectors

1. Melden Sie sich bei Office 365, wählen Sie **Admin**, und klicken Sie dann auf **Exchange** fahren Sie mit der Exchange-Verwaltungskonsole. Klicken Sie auf **E-Mail-Fluss**, und klicken Sie auf **Connectors**.

Office 365 Connectors, die für Ihre Organisation vorhanden sind, sind auf der Seite **Connectors** aufgeführt. Dazu gehören Connectors, die mithilfe des Hybrid Configuration Wizard oder PowerShell erstellt wurden. Sie können jeder Connector konfiguriert für die Nachrichtenübermittlung von Office 365 Ihrer Organisation e-Mail-Server oder einer Partnerorganisation überprüfen.

2. Wählen Sie den Connector, den Sie überprüfen oder aktivieren möchten. Informationen zu dem Connector werden, wie im folgenden Screenshot dargestellt, im Detailbereich angezeigt.

STATUS	Name	Von	An	
Ein	Eingehender E-Mail-Server für Office 365	E-Mail-Server Ihrer Organisation	Office 365	Exchange-Server
Ein	Eingehende Partner für Office 365	Partnerorganisation	Office 365	E-Mail-Fluss-Szenario
Ein	Contoso-Partnerorganisation	Office 365	Partnerorganisation	Von: Office 365 An: E-Mail-Server Ihrer Organisation
Aus	<b>Exchange-Server</b>	<b>Office 365</b>	<b>E-Mail-Server Ihrer Organisation</b>	<b>Beschreibung</b> Keine
				Status Aus <a href="#">Aktivieren</a>
				Überprüfung <a href="#">Diesen Connector prüfen</a> Ergebnis der letzten Überprüfung: Fehler Zeitpunkt der letzten Überprüfung: 9.9.2015 15:48 Uhr

3. Wenn Sie einen Connector für den E-Mail-Fluss auswählen, der aus Office 365 stammt, können Sie auf **Diesen Connector überprüfen** klicken. Wie im folgenden Screenshot dargestellt, können Sie auch feststellen, ob der Connector zuvor überprüft wurde.

Überprüfung

[Diesen Connector prüfen](#)

Ergebnis der letzten Überprüfung: Erfolgreich

Zeitpunkt der letzten Überprüfung: 11.03.2015 15:12 Uhr

4. Wählen Sie nach Auswahl des Connectors die Option **Diesen Connector überprüfen**. Das Dialogfeld **Diesen Connector überprüfen** wird geöffnet. Geben Sie mindestens eine E-Mail-Adresse ein, um mit der Überprüfung zu beginnen. Office 365 verwendet diese Adressen, um sicherzustellen, dass der E-Mail-Fluss ordnungsgemäß eingerichtet ist. Geben Sie, wenn Sie beispielsweise einen Connector für den E-Mail-Fluss von Office 365 an den E-Mail-Server Ihrer Organisation prüfen möchten, eine E-Mail-Adresse für ein Postfach auf dem E-Mail-Server ein.
5. Wählen Sie **Überprüfen**, um den Vorgang fortzusetzen. Detaillierte Informationen zu den dabei untersuchten Problemen und zur Problembehebung finden Sie unter [Fixing connector validation errors](#).
6. Überprüfen Sie, ob alle Connectors aktiviert sind. Wenn ein Connector, den Sie für den E-Mail-Fluss benötigen, nicht aktiviert ist, wählen Sie unter **Status Aktivieren** aus.

**NOTE**

Wenn Sie weiterhin Probleme mit dem E-Mail-Fluss haben, nachdem Sie einen Connector überprüft haben, überprüfen Sie, ob Sie mehrere Connectors eingerichtet haben, die möglicherweise auf ein einziges Szenario angewendet werden können. Es können beispielsweise Probleme auftreten, wenn Sie mehr als einen Connector für E-Mail-Verkehr von Office 365 zu Ihrem E-Mail-Server eingerichtet haben. Wenn Sie mehrere Connectors für E-Mail-Verkehr von Office 365 zu Ihrem E-Mail-Server (oder zu einem Partner) benötigen, stellen Sie sicher, dass Sie jeden Connector überprüfen und aktivieren. > Wenn Sie einen Connector ändern möchten, verwendet Office 365 die vorhandenen Connectoreinstellungen für den E-Mail-Fluss, bis Sie Ihre Änderungen speichern. Weitere Informationen finden Sie unter [Ändern eines von Office 365 für den Nachrichtenfluss verwendeten Connectors](#)

## See also

[Einrichten von Connectors zur Weiterleitung von E-Mails zwischen Office 365 und Ihren eigenen E-Mail-Servern](#)

[Configure mail flow using connectors in Office 365](#)

[Fixing connector validation errors](#)

[Wann benötige ich einen Connector?](#)

# Szenario: Bedingtes E-Mail-Routing

18.12.2018 • 5 minutes to read

Unter Umständen müssen Sie E-Mail abhängig vom Absender, Adressaten, Sendeort oder Inhalt der Nachricht unterschiedlich weiterleiten. Wenn Sie z. B. über mehrere Standorte auf der ganzen Welt verfügen, möchten Sie Mail möglicherweise an einen bestimmten Standort weiterleiten. Dazu können Sie Connectors und Nachrichtenflussregeln (auch als „Transportregeln“ bezeichnet) verwenden.

Wenn die folgenden Schritte abgeschlossen werden, werden Nachrichten an Benutzer, für die die Eigenschaft "Stadt" auf "New Orleans" gesetzt ist, von der Nachrichtenflussregel an die vom ausgehenden Connector angegebene IP-Adresse weitergeleitet.

## Schritt 1: Verwenden der Exchange-Verwaltungskonsole, um den Connector zu erstellen

Als Erstes müssen wir einen ausgehenden Connector erstellen. Dieser Connector wird von der Nachrichtenflussregel verwendet, die wir in Schritt 2 einrichten werden. In diesem Connector wählen Sie aus, woher empfangene Nachrichten stammen (z. B. ein Postfach in Ihrer Office 365-Organisation), die Art der Organisation, an die die Nachrichten gesendet werden (z. B. Ihre lokalen Server), die Sicherheit, die auf die Verbindung angewendet werden soll, und den Namen oder die IP-Adresse des Zielservers. Weitere Informationen zum Erstellen von Connectors finden Sie unter [Configure mail flow using connectors in Office 365](#).

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Connectors**. Klicken Sie auf **neu** zum Erstellen eines neuen Connectors.
2. Wählen Sie im Dropdown-Feld **Von:** die Option Office 365 aus.
3. Wählen Sie im Dropdown-Feld **An:** entweder E-Mail-Server Ihrer Organisation oder Partnerorganisation, wenn Sie mit einem anderen Server als dem Ihrer Organisation eine Verbindung herstellen möchten.

## Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.  
[Learn more](#)

From:

Office 365

To:

Your organization's email server ▾

You need to create a connector for this mail flow scenario. Because your domain's MX record points to Office 365, you must set up an alternative server (called a smart host) so that Office 365 can send email to your organization's email server (also called on-premises server). To complete the scenario, you might need to configure your email server to accept messages delivered by Office 365. [Learn more about configuring your email server](#)

Office 365: Your cloud email subscription.

Your organization's email server: This is an email server that you manage. It's often called an on-premises server.

Partner organization: A partner can be an organization you do business with, such as a bank. It can also be a cloud email service provider that provides services such as archiving, anti-spam, and so on.

Internet: For inbound email, this refers to email that's sent from the Internet to Office 365 (not to your email server or partner organization). For outbound email, it refers to email that's sent from Office 365 to the Internet (not to your email server or partner organization).

Next

Cancel

4. Benennen Sie den Connector, und fügen Sie eine Beschreibung hinzu. Wenn Sie den Connector sofort aktivieren möchten, wählen Sie die Option **Aktivieren**. Klicken Sie auf **Weiter**.

## New connector

This connector enforces routing and security restrictions for email messages sent from Office 365 to your partner organization or service provider.

\*Name:

Contosoco partners

Description:

Optionally include a description for this connector.

What do you want to do after connector is saved?

Turn it on

Next

Cancel

5. Wählen Sie **nur, wenn ich eine Transportregel... haben**, und klicken Sie auf **Weiter**.

## New connector

When do you want to use this connector?

- Only when I have a transport rule set up that redirects messages to this connector
- For email messages sent to all accepted domains in your organization
- Only when email messages are sent to these domains

Select this option only if you created a rule that redirects email messages to this connector.

[Learn more](#)



Back

Next

Cancel

6. Geben Sie einen oder mehrere Smartheads an, an die Office 365 E-Mail-Nachrichten übermitteln soll.

### New connector

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. [Learn more](#)

+ -

192.168.3.2

Back [Next](#) Cancel

7. Definieren Sie die TLS-Einstellungen (Transport Layer Security) entsprechend Ihren Sicherheitsanforderungen.

## New connector

How should Office 365 connect to your email server?

- Always use Transport Layer Security (TLS) to secure the connection (recommended)
- Connect only if the recipient's email server certificate matches this criteria
- Any digital certificate, including self-signed certificates
  - Issued by a trusted certificate authority (CA)
  - And the subject name or subject alternative name (SAN) matches this domain name:

Example: contoso.com or \*.contoso.com

TLS is a security protocol that helps to encrypt and deliver email messages securely so no one except the sender and recipient can access or tamper with the message. If you select this option, messages will be rejected if the TLS connection isn't successful.

[Back](#) [Next](#) [Cancel](#)

8. Überprüfen Sie die Konfiguration des neuen Connectors, und klicken Sie auf **Weiter**, um den Connector zu überprüfen.

## Schritt 2: Verwenden des EAC zum Erstellen einer E-Mail-Flussregel

Nachdem wir einen Connector erstellt haben, müssen wir eine E-Mail-Flussregel erstellen, die Mail basierend auf den von Ihnen definierten Kriterien sendet. Es stehen zahlreiche Bedingungen zur Wahl, mit denen Sie steuern können, wann Nachrichten zum Connector gesendet werden sollen.

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Regeln**. Klicken Sie auf **neu** [ ] , und wählen Sie **neue Regel erstellen**.
2. Benennen Sie die Regel, klicken Sie im Fenster **neue Regel** . Um alle für die Regel verfügbaren Optionen anzuzeigen, klicken Sie auf **Weitere Optionen** am unteren Rand der Seite.

**new rule**

Name:

\*Apply this rule if...

\*Do the following...

Properties of this rule:

Audit this rule with severity level:

Choose a mode for this rule:

Enforce  
 Test with Policy Tips  
 Test without Policy Tips

[More options...](#)

 Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. [Learn more](#)

3. Für \*\* \*diese Regel anwenden, wenn...\*\*, wählen Sie **den Empfänger...** und **hat bestimmte Eigenschaften einschließlich eines dieser Wörter.** Das **Auswählen von Benutzereigenschaften** angezeigt wird.

Klicken Sie auf , und klicken Sie unter **Benutzereigenschaften:** wählen Sie **Ort. Stadt** ist ein Active Directory-Attribut, das durch die Transportregel für die Verwendung zur Verfügung gestellt. Geben Sie den Namen der Stadt ein, beispielsweise New Orleans. Klicken Sie auf **OK**, und klicken Sie dann auf **OK**, um das Dialogfeld **Benutzereigenschaften auswählen** zu schließen.

**new rule**

Name:

\*Apply this rule if...  [\\*Select properties and words...](#)

[Properties of this rule.](#)

- ▶ is this person
- ▶ is external/internal
- ▶ is a member of this group
- ▶ address includes any of these words
- ▶ address matches any of these text patterns
- ▶ is on the sender's supervision list
- ▶ has specific properties including any of these words
- ▶ has specific properties matching these text patterns
- ▶ domain is

**IMPORTANT**

Überprüfen Sie die Benutzerattribute in Active Directory auf Genauigkeit, um sicherzustellen, dass die Nachrichtenflussregel so funktioniert wie beabsichtigt. > Beachten Sie, dass Änderungen am ausgehenden Connector möglicherweise einige Zeit für die Replikation benötigen.

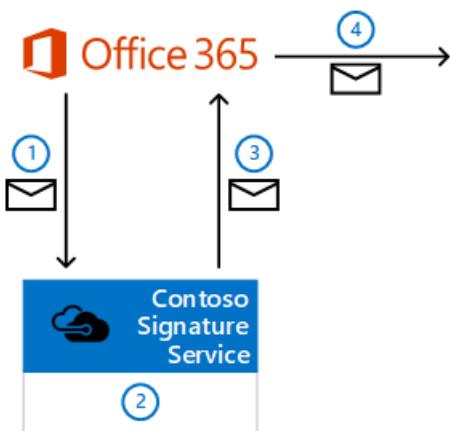
4. Für \*\* \*gehen...\*\*, wählen Sie **die Nachricht an... umleiten**, und geben Sie dann **die folgenden Connectors**. Das **Verbinden auswählen** wird angezeigt. Wählen Sie den ausgehenden Connector, den Sie zuvor erstellt haben.  
Sie können weitere Eigenschaften für die Regel auswählen, z. B. den Testmodus und wann die Regel aktiviert werden soll.
5. Klicken Sie auf **Speichern**, um den Connector zu speichern.

# Szenario: Integrieren von Office 365 mit einem E-Mail-Add-On-Dienst

18.12.2018 • 22 minutes to read

Viele Clouddienstlösungen von Drittanbietern stellen Add-On-Dienste für Office 365 bereit. Aus Sicherheitsgründen lassen wir nicht zu, dass E-Mail-Add-On-Dienste von Drittanbietern in Office 365 installiert werden. Sie können jedoch zusammen mit dem Dienstanbieter die Einstellungen in Ihrer Office 365-Organisation so konfigurieren, dass Sie den Dienst nutzen können.

In diesem Thema werden die optimalen Methoden für Ihre Organisation, um einen E-Mail-Add-On-Dienst eines Drittanbieters zu nutzen, anhand eines fiktiven Diensts namens „Contoso Signature Service“ beschrieben. Dieser fiktive Dienst wird in Azure ausgeführt und bietet benutzerdefinierte E-Mail-Signaturen (Beachten Sie, dass der Dienst in einer anderen Clouddumgebung als Azure bereitgestellt sein kann). Im folgenden Diagramm werden der E-Mail-Fluss und eine allgemeine Übersicht über den Dienst angezeigt.



1. Wenn ein Benutzer in Ihrer Office 365-Organisation eine Nachricht verfasst und sendet, wird die Nachricht mithilfe eines Connectors und einer E-Mail-Flussregel (auch bekannt als einer Transportregel), die Sie erstellen, an den Contoso Signature Service umgeleitet.

Verbindungen von Office 365 zum Contoso Signature Service werden durch TLS verschlüsselt, da Sie den Zertifikatdomänenamen für den Dienst in den Connectoreinstellungen konfigurieren (beispielsweise `smtp.contososignatureservice.com`).

2. Der Contoso Signature Service nimmt die Nachricht an und fügt der Nachricht eine E-Mail-Signatur hinzu. Der Dienst versieht die Nachricht zudem mit einer benutzerdefinierte Kopfzeile, um anzugeben, dass die Nachricht verarbeitet wurde.
3. Der Contoso Signature Service leitet die Nachricht zurück an Office 365. Ein Connector, den Sie erstellen, akzeptiert die eingehenden Nachrichten vom Contoso Signature Service.
  - Der Contoso Signature Service leitet Nachrichten mithilfe von Smarthostrouting zurück in die Region, in der sich Ihre Office 365-Organisation befindet. Ist Ihre Office 365-Domäne beispielsweise `fabrikam.onmicrosoft.com`, ist der Zielsmarthost `fabrikam.mail.protection.outlook.com`.
  - Der Contoso Signature Service stellt einen eindeutigen Zertifikatdomänenamen für jeden Kunden bereit. Sie konfigurieren diesen Domänenamen als eine akzeptierte Domäne in Ihrer Office 365-Organisation und in den Connectoreinstellungen (z. B.

S5HG3DCG14H8S1R2303RZHM4RX.smtp.contososignatureservice.com).

4. Office 365 sendet die Nachricht mit der angepassten Signatur an die ursprünglichen Empfänger.

Im Rest des Themas wird erläutert, wie der E-Mail-Fluss in Office 365 für die Zusammenarbeit mit dem E-Mail-Add-On-Dienst konfiguriert wird.

**NOTE**

Diese Elemente sind für alle E-Mail-Add-On-Dienste erforderlich, die Sie in Ihre Office 365-Organisation integrieren möchten. Sie müssen zusammen mit dem E-Mail-Add-On-Dienstanbieter die erforderlichen Einstellungen in Office 365 konfigurieren.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 15 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Nachrichtenübermittlung" im Thema [Featureberechtigungen in Exchange Online](#).
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). So verwenden Sie Windows PowerShell für die Verbindung zu Exchange Online finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

**TIP**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Schritt 1: Erstellen eines ausgehenden Connectors zum Weiterleiten von Nachrichten an den E-Mail-Add-On-Dienst

Die wichtigen Einstellungen für den Connector sind:

- Von Office 365 zum E-Mail-Add-On-Dienst
- Verwendung von Smarthostrouting zum E-Mail-Add-On-Dienst
- Verwendung von TLS zum Verschlüsseln der Verbindung basierend auf dem Domänennamen des E-Mail-Add-On-Diensts (Smarthost)

### **Erstellen des ausgehenden Connectors zum E-Mail-Add-On-Dienst mithilfe der Exchange-Verwaltungskonsole**

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Connectors**, und klicken Sie dann auf **New**

2. Der neue Connector-Assistent wird geöffnet. Konfigurieren Sie auf der Seite **Wählen Sie Ihr Nachrichtenübermittlungsszenario aus** die folgenden Einstellungen:

- **Von: Office 365**
- **An: Ihrer Organisation e-Mail-Server**

Klicken Sie nach Abschluss des Vorgangs auf **Weiter**.

3. Konfigurieren Sie auf der nächsten Seite die folgenden Einstellungen:

- **Name:** Geben Sie einen beschreibenden Namen (beispielsweise Office 365 Contoso Signatur Service).
- **Aufbewahren internen Exchange e-Mail-Header (empfohlen):** Konfigurieren Sie einen der folgenden Werte:
  - **Aktiviert:** behält interne Kopfzeilen in Nachrichten, die an die e-Mail-Add-on-Dienst, d. h. gesendet werden, die Nachrichten werden als vertrauenswürdige interne Nachrichten behandelt. Wenn Sie diesen Wert auswählen, müssen Sie auch den gleichen Wert für diese Einstellung für den eingehenden Connector verwenden, die Sie in Schritt 4 erstellen (andernfalls der eingehende Connector entfernt die internen Exchange-Kopfzeilen aus den zurückgegebenen Nachrichten).
  - **Deaktiviert:** interne Kopfzeilen von Nachrichten entfernt, vor dem Senden an den e-Mail-Add-on-Dienst befinden. Wenn Sie diesen Wert auswählen, ist der Wert dieser Einstellung für den eingehenden Connector, die Sie in Schritt 4 erstellen ohne Bedeutung (per Definition fallen keine internen Exchange-Header beibehalten oder Entfernen von Nachrichten zurückgeben).

Neuer Connector

Dieser Connector ermöglicht Office 365 das Zustellen von E-Mails an den E-Mail-Server Ihrer Organisation.

\*Name:  
Contoso Signature Service für Office 365

Beschreibung:

Was möchten Sie nach dem Speichern des Connectors tun?

Einschalten  
 Interne Exchange-E-Mail-Header beibehalten (empfohlen)

[Weiter](#)  [Abbrechen](#)

Klicken Sie nach Abschluss des Vorgangs auf **Weiter**.

- Wählen Sie auf der Seite **Wann möchten Sie diesen Connector verwenden?** die Option **Nur, wenn ich eine Transportregel eingerichtet habe, die Nachrichten an diesen Connector umleitet** aus, und klicken Sie dann auf **Weiter**.

Neuer Connector

Wann möchten Sie diesen Connector verwenden?

Nur, wenn ich eine Transportregel eingerichtet habe, die Nachrichten an diesen Connector umleitet  
 Für an alle akzeptierten Domänen in Ihrer Organisation gesendete E-Mails  
 Nur, wenn E-Mails an diese Domänen gesendet werden

+ / -

[Zurück](#)  [Weiter](#) [Abbrechen](#)

- Klicken Sie auf die **Wie möchten Sie den e-Mail-Nachrichten weitergeleitet?** Seite, klicken Sie auf **Hinzufügen**. Geben Sie im Dialogfeld **Smarthost hinzufügen**, das angezeigt wird den Smarthost-Wert für den e-Mail-Add-on-Dienst (beispielsweise smtp.contososignatureservice.com), klicken Sie auf **Speichern**, und klicken Sie dann auf **Weiter**.

Neuer Connector

Wie möchten Sie E-Mails weiterleiten?

Geben Sie mindestens einen Smarthost an, an den Office 365 E-Mails zustellen soll. Ein Smarthost ist ein alternativer Server und kann mithilfe eines vollqualifizierten Domänennamens (FQDN) oder einer IP-Adresse identifiziert werden. [Weitere Informationen](#)

+ / -

smtp.contososignatureservice.com

[Zurück](#)  [Weiter](#) [Abbrechen](#)

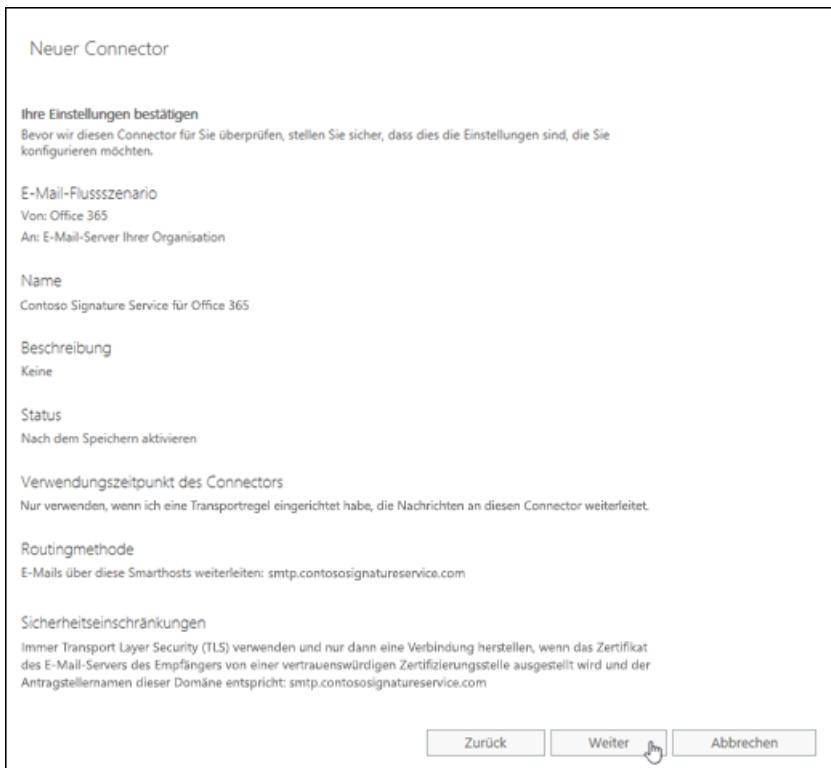
- Konfigurieren Sie auf der Seite **Wie sollte Office 365 eine Verbindung mit Ihrem E-Mail-Server herstellen?** die folgenden Einstellungen:

- Vergewissern Sie sich, dass **Immer TLS (Transport Layer Security) zum Sichern der Verbindung verwenden (empfohlen)** ausgewählt ist.
- Vergewissern Sie sich, dass **Von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt** ausgewählt ist.
- Wählen Sie **Und der Antragstellername oder der alternative Antragstellername (SAN) stimmt mit diesem Domänenamen überein** aus, und geben Sie den Smarthost ein, den Sie im vorherigen Schritt verwendet haben (beispielsweise smtp.contososignatureservice.com).



Klicken Sie nach Abschluss des Vorgangs auf **Weiter**.

7. Überprüfen Sie die Einstellungen auf der Seite **Ihre Einstellungen bestätigen**, und klicken Sie dann auf **Weiter**.



8. Klicken Sie auf **Hinzufügen**, auf der Seite **Überprüfen dieser Connector** [ ] Geben Sie im Dialogfeld **Add-e-Mail**, das angezeigt wird, eine e-Mail-Adresse, die nicht in Office 365 zum Testen der Verbindung (beispielsweise admin@fabrikam.com), klicken Sie auf **OK**, und klicken Sie auf **Überprüfen**.

Diesen Connector überprüfen

Wir überprüfen diesen Connector für Sie, um sicherzustellen, dass er wie erwartet funktioniert, aber Sie müssen zuerst mindestens eine E-Mail-Adresse angeben, damit wir eine Testnachricht senden können.

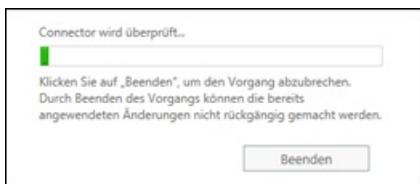
Geben Sie eine E-Mail-Adresse für ein aktives Postfach an, das sich auf Ihrem E-Mail-Server befindet. Wenn Ihre Organisation über mehrere Domänen verfügt, können Sie mehrere Adressen hinzufügen.

+ -

admin@fabrikm.com

Zurück Überprüfen Abbrechen

Ein Statusindikator wird angezeigt. Wenn die Überprüfung des Connectors abgeschlossen ist, klicken Sie auf **Schließen**.



## 9. Klicken Sie auf der Seite **Überprüfungsergebnis** auf **Speichern**.

### Verwenden von Exchange Online PowerShell den ausgehenden Connector an den e-Mail-Add-on-Dienst erstellen

Verwenden Sie folgende Syntax, um den ausgehenden Connector an den e-Mail-Add-on-Dienst in Exchange Online PowerShell zu erstellen:

```
New-OutboundConnector -Name "<Descriptive Name>" -ConnectorType OnPremises -IsTransportRuleScoped $true -UseMxRecord $false -SmartHosts <SmartHost> -TlsSettings DomainValidation -TlsDomain <SmartHost> [-CloudServicesMailEnabled $true]
```

In diesem Beispiel wird ein ausgehender Connector mit diesen Einstellungen erstellt:

- **Name:** Office 365 zu Contoso-Signatur-Dienst
- **Smarthost Ziel des e-Mail-Add-on-Dienst:** smtp.contososignatureservice.com
- **TLS-Domäne für die domänenüberprüfung:** smtp.contososignatureservice.com
- Interne Exchange-Nachrichtenköpfe, die Nachrichten als intern identifizieren, werden in den ausgehenden Nachrichten beibehalten.

```
New-OutboundConnector -Name "Office 365 to Contoso Signature Service" -ConnectorType OnPremises -IsTransportRuleScoped $true -UseMxRecord $false -SmartHosts smtp.contososignatureservice.com -TlsSettings DomainValidation -TlsDomain smtp.contososignatureservice.com -CloudServicesMailEnabled $true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-OutboundConnector](#).

### Woher wissen Sie, dass dieser Schritt erfolgreich war?

Verwenden Sie eines der folgenden Verfahren, um sich zu vergewissern, dass Sie erfolgreich einen ausgehenden Connector zum Weiterleiten von Nachrichten an den E-Mail-Add-On-Dienst erstellt haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Connectors**, wählen Sie den

Connector aus, klicken Sie auf **Bearbeiten** [ ] , und überprüfen Sie die Einstellungen.

- Ersetzen Sie in Exchange Online PowerShell \_ <Connectorname> \_ mit dem Namen der Connector und dieser Befehl so überprüfen Sie die Eigenschaftswerte ausführen:

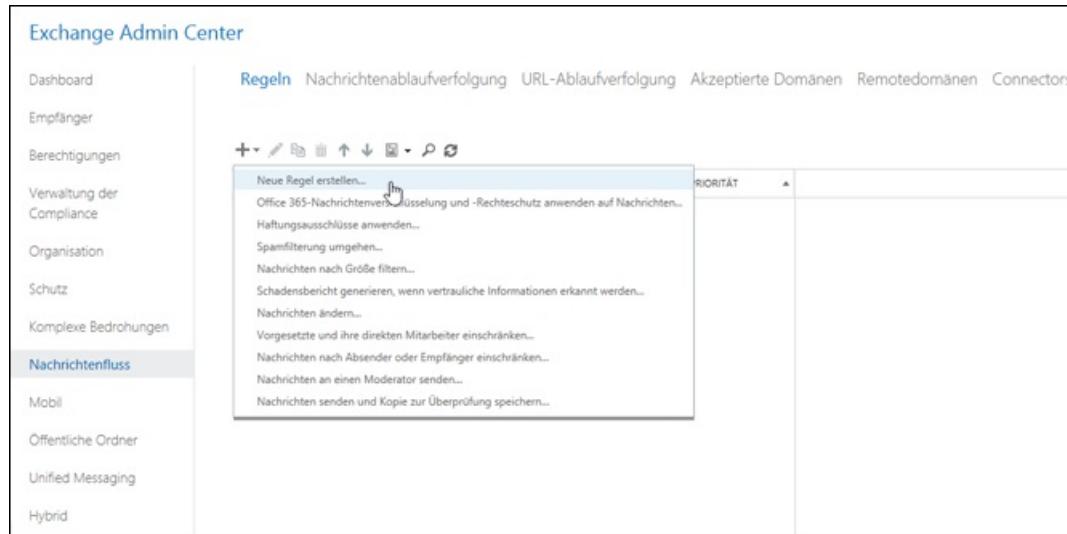
```
Get-OutboundConnector -Identity "<Connector Name>" | Format-List  
Name,ConnectorType,IsTransportRuleScoped,UseMxRecord,SmartHosts,TlsSettings,TlsDomain,CloudServicesMailEnabled
```

## Schritt 2: Erstellen einer E-Mail-Flussregel zum Weiterleiten nicht verarbeiteter Nachrichten an den E-Mail-Add-On-Dienst

Die Regel leitet Nachrichten von internen Absendern an den ausgehenden Connector weiter, den Sie in Schritt 1 erstellt haben, wenn die Nachrichten noch nicht vom E-Mail-Add-On-Dienst verarbeitet wurden (die Nachricht enthält nicht den benutzerdefinierten Kopf).

### Erstellen einer E-Mail-Flussregel zum Weiterleiten nicht verarbeiteter Nachrichten an den E-Mail-Add-On-Dienst mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Regeln**, und klicken Sie auf **neu** [ ], und wählen Sie dann auf **neue Regel erstellen**.



2. Klicken Sie auf der daraufhin geöffneten Seite **Neue Regel** auf **Weitere Optionen** unten auf der Seite.

3. Konfigurieren Sie auf der Seite **Neue Regel** diese Einstellungen:

- **Name:** Geben Sie einen beschreibenden Namen (beispielsweise Routen von e-Mails an Contoso Signatur Service).

- **Diese Regel anwenden, wenn:** Wählen Sie **die Absender > ist extern/interne** > wählen Sie **innerhalb der Organisation** aus, und klicken Sie dann auf **OK**.
- **Gehen Sie folgendermaßen vor:** Wählen Sie **Umleiten der Nachricht an > die folgenden Connectors** > wählen Sie den ausgehenden Connector, die Sie in Schritt 1 erstellt haben, und klicken Sie dann auf **OK**.
- **Außer wenn:** Klicken Sie auf **Ausnahme hinzufügen** > wählen Sie **ein Nachrichtenkopf > beinhaltet und diese Wörter**.
- Klicken Sie auf **Text eingeben**, geben Sie den Namen des benutzerdefinierten Kopffelds ein, das vom E-Mail-Add-On-Dienst angewendet wird (z. B. SignatureContoso), und klicken Sie dann auf **OK**.
- Klicken Sie auf **EINGABETASTE Wörter**, geben Sie den Wert der Header-dar, der angibt, eine Nachricht (z. B. true) vom e-Mail-Add-on-Dienst verarbeitet worden sind, klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **OK**.
- Wählen Sie im unteren Bereich der Seite **Keine weiteren Regeln anwenden**.

The screenshot shows the 'Neue Regel' (New Rule) dialog box. Key visible fields include:

- Name:** E-Mail an Contoso Signature Service weiterleiten
- \*Diese Regel anwenden, wenn...**: Der Absender befindet sich in... (Innerhalb der Organisation)
- \*Folgendermaßen vorgehen...**: Folgenden Connector verwenden... (Contoso Signature Service für Office 365)
- Außer wenn...**: Ein Nachrichtenkopf enthält... (SignatureCentoso) Kopfzeile enthält: true
- Eigenschaften dieser Regel:** Diese Regel mit folgendem Schweregrad überwachen: Nicht angegeben
- Modus für diese Regel auswählen:** Erzwingen (selected)
- Diese Regel an folgendem Datum aktivieren:** Di 10.10.2017 | 15:00
- Diese Regel an folgendem Datum deaktivieren:** Di 10.10.2017 | 15:00
- Keine weiteren Regeln anwenden** (checkbox checked)
- Nachricht zurückstellen, wenn die Regelverarbeitung nicht abgeschlossen wird** (checkbox)
- Absenderadresse in Nachricht vergleichen:** Kopfzeile
- Kommentare:** (empty text area)

At the bottom, a note reads: Die Rechteverwaltungsdienste (Rights Management Services, RMS) sind eine Premium-Funktion und erfordern eine Clientzugriffs Lizenz (CAL) der Enterprise Edition oder eine RMS-Online Lizenz für jedes Benutzerpostfach. [Weitere Informationen](#)

Buttons at the bottom right: Speichern (highlighted with a cursor icon) and Abbrechen.

Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

**Verwenden von Exchange Online PowerShell, erstellen Sie eine e-Mail-Flussregel nicht verarbeitete Nachrichten an die e-Mail-Add-on-Dienst weitergeleitet**

Um die Regel der e-Mail-Fluss in Exchange Online PowerShell erstellen, verwenden Sie folgende Syntax:

```
New-TransportRule -Name "<Descriptive Name>" -FromScope InOrganization -RouteMessageOutboundConnector "<Connector Name>" -ExceptIfHeaderContainsMessageHeader <HeaderName> -ExceptIfHeaderContainsWords <HeaderValue> -StopRuleProcessing $true
```

In diesem Beispiel wird die E-Mail-Flussregel mit diesen Einstellungen erstellt:

- **Name:** e-Mail an Contoso Signatur Service weiterleiten

- **Name des ausgehenden Connectors:** Office 365 zu Contoso-Signatur-Dienst
- **Kopffeld und Wert, der die Verarbeitung durch den E-Mail-Add-On-Dienst angibt** SignatureContoso mit dem Wert true.

```
New-TransportRule -Name "Route email to Contoso Signature Service" -FromScope InOrganization -
RouteMessageOutboundConnector "Office 365 to Contoso Signature Service" -ExceptIfHeaderContainsMessageHeader
SignatureContoso -ExceptIfHeaderContainsWords true -StopRuleProcessing $true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-TransportRule](#).

#### Woher wissen Sie, dass dieser Schritt erfolgreich war?

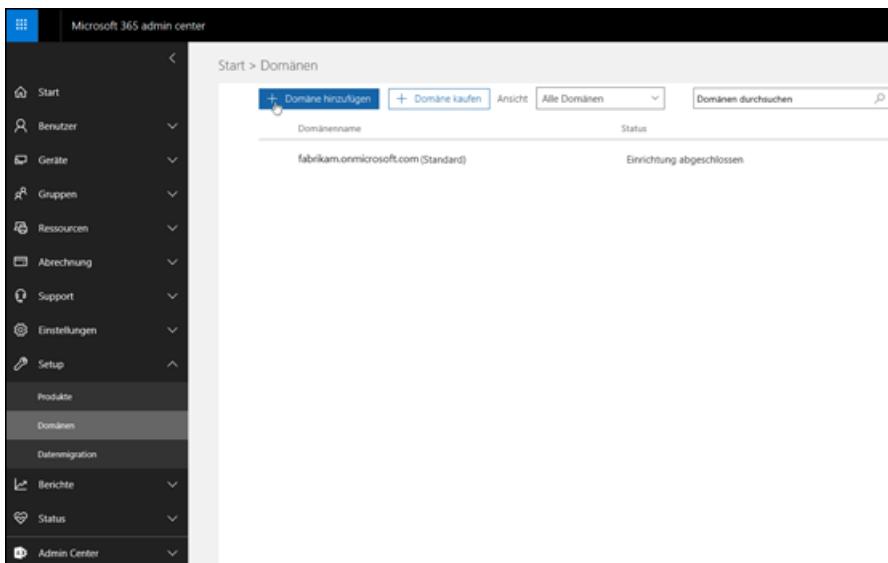
Verwenden Sie eines der folgenden Verfahren, um sich zu vergewissern, dass Sie erfolgreich eine E-Mail-Flussregel für die Weiterleitung nicht verarbeiteter Nachrichten an den E-Mail-Add-On-Dienst erstellt haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Regeln**, wählen Sie die Regel aus, klicken Sie auf **Bearbeiten**, und überprüfen Sie die Einstellungen der Regel.
- Ersetzen Sie in Exchange Online PowerShell `_ <Regelname> _` mit dem Namen der Regel und dieser Befehl so überprüfen Sie die Eigenschaftswerte ausführen:

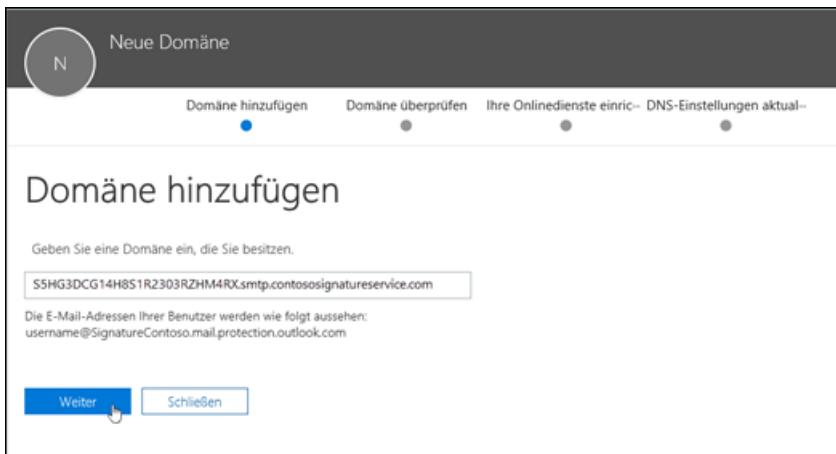
```
Get-TransportRule -Identity "<Rule Name>" | Format-List
Name,FromScope,RouteMessageOutboundConnector,ExceptIfHeaderContainsMessageHeader,ExceptIfHeaderContainsWords,StopRuleProcessing
```

## Schritt 3: Hinzufügen der benutzerdefinierten Zertifikatdomäne, die vom E-Mail-Add-On-Dienst bereitgestellt wird, als eine akzeptierte Domäne in Office 365

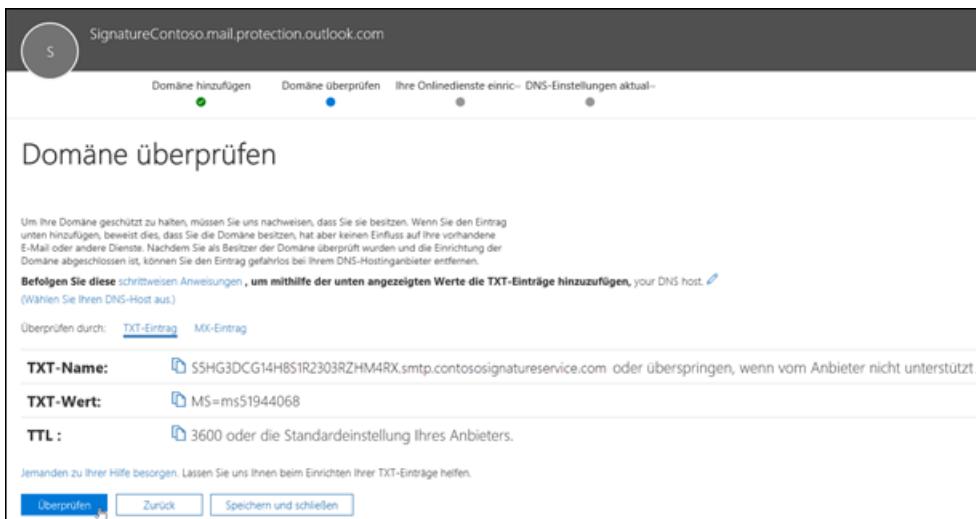
1. Wechseln Sie zum Office 365 Admin Center unter <https://portal.office.com/adminportal/home>, klicken Sie auf **Setup > Domänen**, und klicken Sie dann auf **Domäne hinzufügen**.



2. Geben Sie auf der daraufhin angezeigten Seite **Domäne hinzufügen** die benutzerdefinierte Zertifikatdomäne ein, die der E-Mail-Add-On-Dienst bereitgestellt hat, als Sie den Dienst registriert haben (z. B. S5HG3DCG14H8S1R2303RZHM4RX.smtp.contososignatureservice.com), und klicken Sie dann auf **Weiter**.



3. Verwenden Sie auf der Seite **Domäne überprüfen** die Details auf den Registerkarten **TXT-Eintrag** oder **MX-Eintrag**, um einen TXT- oder MX-Eintrag für den Nachweis des Domänenbesitzes für die benutzerdefinierte Zertifikatdomäne zu erstellen. Nachdem Sie den Eintrag für den Nachweis des Domänenbesitzes erstellt haben, klicken Sie auf **Überprüfen**. Nachdem die Domäne überprüft wurde, klicken Sie auf **Speichern und schließen**.



Weitere Informationen finden Sie unter [Hinzufügen Ihrer Domäne zu Office 365](#).

## Schritt 4: Erstellen eines eingehenden Connectors zum Empfangen von Nachrichten vom E-Mail-Add-On-Dienst

Die wichtigen Einstellungen für den Connector sind:

- Vom E-Mail-Add-On-Dienst zu Office 365.
- TLS-Verschlüsselung und Zertifikatüberprüfung basieren auf dem benutzerdefinierten Zertifikatdomänennamen, den Sie im vorherigen Schritt als eine akzeptierte Domäne konfiguriert haben.

### Erstellen eines eingehenden Connectors zum Empfangen von Nachrichten vom E-Mail-Add-On-Dienst mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Connectors**, und klicken Sie dann auf **New**

2. Der neue Connector-Assistent wird geöffnet. Konfigurieren Sie auf der Seite **Wählen Sie Ihr Nachrichtenübermittlungsszenario aus** die folgenden Einstellungen:

- **Von E-Mail-Server Ihrer Organisation**
- **An Office 365**

Klicken Sie nach Abschluss des Vorgangs auf **Weiter**.

3. Konfigurieren Sie auf der nächsten Seite die folgenden Einstellungen:

- **Name:** Geben Sie einen beschreibenden Namen (beispielsweise "Contoso" Signatur-Dienst zu Office 365).
- **Aufbewahren internen Exchange e-Mail-Headern (empfohlen):** Konfigurieren Sie einen der folgenden Werte:
- **Aktiviert:** behält interne Kopfzeilen in Nachrichten, die aus dem e-Mail-Add-on-Dienst zurückgegeben werden. Wenn Sie diesen Wert auf diese Einstellung für den ausgehenden Connector ausgewählt, die Sie in Schritt 1 erstellen haben, müssen Sie denselben Wert zu konfigurieren. Die internen Exchange-Header in die zurückgegebenen Nachrichten werden beibehalten, was bedeutet, dass die Rückgabe von Add-on-Dienst die e-Mail-Nachrichten als vertrauenswürdige interne Nachrichten behandelt werden.
- **Deaktiviert:** entfernt die internen Exchange-Kopfzeilen (falls vorhanden) von Nachrichten, die aus dem e-Mail-Add-on-Dienst zurückgegeben werden.

Neuer Connector

Mit diesem Connector kann Office 365 E-Mail-Nachrichten vom E-Mail-Server Ihrer Organisation (auch als lokaler Server bezeichnet) akzeptieren.

\*Name:  
Contoso Signature Service für Office 365

Beschreibung:

Was möchten Sie nach dem Speichern des Connectors tun?

Einschalten  
 Interne Exchange-E-Mail-Header beibehalten (empfohlen)

Weiter  Abbrechen

Klicken Sie nach Abschluss des Vorgangs auf **Weiter**.

4. Überprüfen Sie auf der Seite **Wie soll Office 365 E-Mail von Ihrem E-Mail-Server identifizieren?**, ob die erste Option ausgewählt ist (Überprüfung anhand des Zertifikats), und geben Sie die Zertifikatdomäne ein, die Sie vom E-Mail-Add-On-Dienst erhalten haben, als Sie sich beim Dienst registriert haben (z. B. S5HG3DCG14H8S1R2303RZHM4RX.smtp.contososignatureservice.com).

Neuer Connector

Wie soll Office 365 E-Mail von Ihrem E-Mail-Server identifizieren?

Durch Überprüfen, ob der Antragstellername des Zertifikats, mit dem der sendende Server die Authentifizierung bei Office 365 vornimmt, mit diesem Domänenamen übereinstimmt (empfohlen)  
S5HG3DCG14H8S1R2303RZHM4RX.smtp.contososignatureservice.com

Durch Überprüfen, ob die IP-Adresse des sendenden Servers mit einer dieser IP-Adressen übereinstimmt, die zu Ihrer Organisation gehören

+ / -

Office 365 akzeptiert Nachrichten über diesen Connector nur, wenn die Domäne des Absenders als akzeptierte Domäne für Ihre Office 365-Organisation konfiguriert ist. [Weitere Informationen](#)

Zurück Weiter  Abbrechen

Klicken Sie nach Abschluss des Vorgangs auf **Weiter**.

5. Überprüfen Sie die Einstellungen auf der Seite **Ihre Einstellungen bestätigen**, und klicken Sie dann auf **Speichern**.

Neuer Connector

Ihre Einstellungen bestätigen  
Stellen Sie vor dem Speichern sicher, dass dies die Einstellungen sind, die Sie konfigurieren möchten.

E-Mail-Flussszenario  
Von: E-Mail-Server Ihrer Organisation  
An: Office 365

Name  
Contoso Signature Service für Office 365

Beschreibung  
Keine

Status  
Nach dem Speichern aktivieren

Identifizieren von E-Mails, die von Ihrem E-Mail-Server gesendet wurden  
Identifizieren Sie eingehende Nachrichten von Ihrem E-Mail-Server, indem Sie überprüfen, dass der Antragstellername in dem die Verbindung herstellenden TLS-Zertifikat mit dieser Domäne übereinstimmt: S5HG3DCG14H8S1R2303RZHM4RX.smtp.contososignatureservice.com, und die E-Mail-Adresse des Absenders ist eine akzeptierte Domäne für Ihre Organisation.

## Verwenden von Exchange Online PowerShell erstellen einen eingehenden Connector Empfang von Nachrichten von der e-Mail-Add-on-Dienst

Verwenden Sie folgende Syntax, um den eingehenden Connector aus der e-Mail-Add-on-Dienst in Exchange Online PowerShell zu erstellen:

```
New-InboundConnector -Name "<Descriptive Name>" -SenderDomains * -ConnectorType OnPremises -RequireTls $true -RestrictDomainsToCertificate $true -TlsSenderCertificateName <CertificateDomainName> [-CloudServicesMailEnabled $true]
```

In diesem Beispiel wird ein ausgehender Connector mit diesen Einstellungen erstellt:

- **Name:** Contoso Signatur Service zu Office 365
- **Domänenname wird von der e-Mail-Add-on-Dienst-Zertifikat zur Authentifizierung mit Office 365-Organisation verwendet:** S5HG3DCG14H8S1R2303RZHM4RX.smtp.contososignatureservice.com
- Interne Exchange-Nachrichtenheader, die vom E-Mail-Add-On-Dienst zurückgegebene Nachrichten als interne Nachrichten identifizieren, werden beibehalten.

```
New-InboundConnector -Name "Contoso Signature Service to Office 365" -SenderDomains * -ConnectorType OnPremises -RequireTls $true -RestrictDomainsToCertificate $true -TlsSenderCertificateName S5HG3DCG14H8S1R2303RZHM4RX.smtp.contososignatureservice.com -CloudServicesMailEnabled $true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-InboundConnector](#).

### Woher wissen Sie, dass dieser Schritt erfolgreich war?

Verwenden Sie eines der folgenden Verfahren, um zu überprüfen, ob Sie erfolgreich einen eingehenden Connector zum Empfangen von Nachrichten vom E-Mail-Add-On-Dienst erstellt haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Connectors**, wählen Sie den Connector aus, klicken Sie auf **Bearbeiten**, und überprüfen Sie die Einstellungen.
- Ersetzen Sie in Exchange Online PowerShell `_ <Connectorname> _` mit dem Namen der Connector und dieser Befehl so überprüfen Sie die Eigenschaftswerte ausführen:

```
Get-InboundConnector -Identity "<Connector Name>" | Format-List  
Name,SenderDomains,ConnectorType,RequireTls,RestrictDomainsToCertificate,TlsSenderCertificateName,CloudS  
ervicesMailEnabled
```

# Verwenden Sie verzeichnisbasierte Edge-Blockierung zum Ablehnen von Nachrichten, die an ungültige Empfänger gesendet

18.12.2018 • 5 minutes to read

Verzeichnis basierend Edge-Blockierung (DBEB) in Exchange Online und Exchange Online Protection (EOP) können Sie die Nachrichten für ungültige Empfänger am dienstnetzwerkumkreis abzulehnen. DBEB kann Administratoren e-Mail-aktivierten Empfänger zu Office 365 hinzufügen und blockieren alle Nachrichten an e-Mail-Adressen, die nicht in Office 365 vorhanden sind.

Wenn eine Nachricht an eine gültige e-Mail-Adresse in Office 365 gesendet wird, wird die Nachricht über den Rest des Diensts Ebenen Filtern fortgesetzt: Modul, Antispam und Mail flow Regeln (auch als Transportregeln bezeichnet). Wenn die Adresse nicht ist, der Dienst blockiert die Nachricht vor dem Ausführen Filters sogar und non-Delivery Report (auch bekannt als ein Unzustellbarkeitsbericht oder eine *Unzustellbarkeitsnachricht*) wird an den Absender zurückgesendet. Der Unzustellbarkeitsbericht sieht folgendermaßen aus:

550 5.4.1 [<InvalidAlias>@\<Domain>]: Recipient address rejected: Access denied .

**Wenn alle Empfänger für Ihre Domäne in Exchange Online, werden DBEB ist bereits aktiviert, und Sie müssen nicht alles möglich.** Wenn Sie von einem anderen e-Mail-System zu Exchange Online migrieren, können Sie das Verfahren in diesem Thema verwenden, um DBEB für die Domäne vor der Migration zu aktivieren.

## NOTE

In hybridumgebungen, in der Reihenfolge für DBEB funktioniert, muss e-Mail für die Domäne zu Office 365 weitergeleitet werden zuerst (MX-Eintrag für die Domäne zu Office 365 zeigen muss).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 bis 10 Minuten
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter: [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren von DBEB

1. Stellen Sie sicher, dass Ihre akzeptierte Domäne in Exchange Online auf **Internes Relay**: a. In der Exchange-Verwaltungskonsole, rufen Sie die **E-Mail-Fluss > Akzeptierte Domänen**.
2. Wählen Sie die Domäne aus, und klicken Sie auf **Bearbeiten**

3. Stellen Sie sicher, dass der Domänenentyp auf **Internes Relay** festgelegt ist. Sollte er auf **Autorisiert** festgelegt sein, ändern Sie ihn in **Internes Relay**, und klicken Sie auf **Speichern**.
4. Hinzufügen von Benutzern zu Office 365. Zum Beispiel:
  - **Directory-Synchronisierung:** Office 365 synchronisieren aus der lokalen Active Directory-Umgebung von [Azure Active Directory](#) in der Cloud gültige Benutzer hinzuzufügen. Weitere Informationen zum Einrichten von verzeichnissynchronisierung finden Sie unter "Verwalten von Empfängern verzeichnissynchronisierung" in [Manage Mail Users in EOP](#).
  - **Hinzufügen von Benutzern über PowerShell oder der Exchange-Verwaltungskonsole:** Weitere Informationen hierzu finden Sie unter [Manage Mail Users in EOP](#) oder [Verwalten Postfachbenutzer in Exchange Online](#).
3. Legen Sie die akzeptierte Domäne in Exchange Online **authoritative**: a. In der Exchange-Verwaltungskonsole, rufen Sie die **E-Mail-Fluss > Akzeptierte Domänen**. b. Wählen Sie die Domäne aus, und klicken Sie auf **Bearbeiten**. c. festlegen Sie den Domänenentyp auf **autorisiert fest**.
4. Wählen Sie **Speichern** aus, um Ihre Änderungen zu speichern, und bestätigen Sie, dass Sie DBEB aktivieren möchten.

**Hinweise:**

- Bis alle Ihrer gültigen Empfängern zu Exchange Online hinzugefügt und durch das System repliziert wurden, lassen Sie die akzeptierte Domäne als **Internes Relay** konfiguriert. Nachdem Sie der Domänenentyp auf **autorisiert fest** geändert wurde, DBEB soll eine beliebige SMTP-Adresse zu ermöglichen, die mit dem Dienst (außer für e-Mail-aktivierte Öffentliche Ordner) hinzugefügt wurde. Es könnten seltene Instanzen, wo Empfängeradressen, die nicht in Office 365-Organisation vorhanden sind, über den Dienst weiterzuleiten zulässig sind.
- Weitere Informationen zu DBEB und e-Mail-aktivierte Öffentliche Ordner finden Sie unter [Unterstützung für Office 365 Directory Based Edge Blocking lokaler e-Mail-aktivierte Öffentliche Ordner](#).

# Verwalten akzeptierter Domänen in Exchange Online

18.12.2018 • 8 minutes to read

Wenn Sie Ihre Domäne zu Office 365 hinzufügen, hat dies eine akzeptierte Domäne bezeichnet. Dies bedeutet, dass Benutzer in dieser Domäne können e-Mails senden und empfangen. Weitere Informationen zum Hinzufügen Ihrer Domäne zu Office 365 mit Office 365 Administrationscenter finden Sie unter [Hinzufügen einer Domäne zu Office 365](#).

Nachdem Sie Ihre Domäne im Office 365 Admin Center hinzugefügt haben, können Sie Ihre akzeptierten Domänen im Exchange-Verwaltungskonsole (EAC) anzeigen und den Domänenentyp konfigurieren.

Es gibt zwei Arten von akzeptierten Domänen in Exchange Online:

- **Authoritative:** E-Mail wird übermittelt, um e-Mail-Adressen, die für Empfänger in Office 365 für diese Domäne aufgeführt sind. E-Mails für unbekannte Empfänger werden zurückgewiesen.
  - Wenn Sie Ihre Domäne gerade zu Office 365 hinzugefügt haben und diese Option auswählen, sollten Sie Ihre Empfänger zu Office 365 hinzufügen, bevor Sie die Weiterleitung von E-Mails über diesen Dienst einrichten.
  - In der Regel verwenden Sie diese Option, wenn alle e-Mail-Empfängern in Ihrer Domäne Office 365 verwenden. Sie können auch verwenden, wenn einige Empfänger auf Ihre eigenen e-Mail-Server vorhanden sind. Jedoch Wenn Empfänger auf Ihre eigenen e-Mail-Server vorhanden sind, müssen Sie Hinzufügen von Empfängern in Office 365-Domäne, um sicherzustellen, dass Nachrichten übermittelt werden, wie erwartet. Weitere Informationen zum Verwalten von Empfängern finden Sie unter folgenden Themen:
    - **Exchange Online:** [Verwalten von e-Mail-Benutzern](#)
    - **Exchange Online Protection:** [Verwalten von E-Mail-Benutzern in EOP](#)
  - Diese Option ermöglicht Directory basierend Edge-Blockierung (DBEB) festlegen, abgelehnt die Nachrichten für ungültige Empfänger am dienstnetzwerkumkreis. Weitere Informationen zum Konfigurieren von DBEB während einer Migrations finden Sie unter [Use Directory Based Edge Blocking ablehnen von Nachrichten an ungültige Empfänger gesendet](#).
- **Internes Relay (auch bekannt als nicht autorisiert):** Empfänger für diese Domäne können in Office 365 oder Ihre eigenen e-Mail-Server sein. E-Mail wird den bekannten Empfängern in Office 365 zugestellt oder an Ihrem eigenen e-Mail-Server weitergeleitet, wenn die Empfänger zu Office 365 bekannt sind nicht.
  - **Sie sollten diese Option nicht auswählen, wenn sich alle Empfänger für diese Domäne in Office 365 befinden.**
  - Wenn Sie diese Option auswählen, müssen Sie aus Office 365 einen Connector für den E-Mail-Fluss für den lokalen E-Mail-Server erstellen. Ansonsten können Empfänger in der Domäne, die nicht in Office 365 gehostet werden, keine E-Mails auf Ihren eigenen E-Mail-Servern empfangen. Weitere Informationen zum Einrichten von Connectors finden Sie unter [Einrichten von Connectors zur Weiterleitung von E-Mails zwischen Office 365 und Ihren eigenen E-Mail-Servern](#).
  - Diese Option ist erforderlich, wenn Sie in einer Domäne die Unterdomänen-Routingoption aktivieren, um E-Mails über den Dienst weiterzuleiten und an Unterdomänen Ihrer akzeptierten

Domänen zuzustellen. Weitere Informationen finden Sie unter [Aktivieren der Nachrichtenübermittlung für Unterdomänen in Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 10 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Domänen" im Thema [Mail flow permissions](#).
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Anzeigen von akzeptierten Domänen

### Anzeigen von akzeptierten Domänen mithilfe der Exchange-Verwaltungskonsole

1. Wechseln Sie im EAC zu **E-Mail-Fluss > Akzeptierte Domänen**.
2. Klicken Sie auf die Spaltenüberschriften **Name**, **Akzeptierte Domäne** oder **Domänentyp**, um sie in aufsteigender oder absteigender Reihenfolge alphabetisch zu sortieren. Standardmäßig sind die akzeptierten Domänen in aufsteigender Reihenfolge nach Namen alphabetisch sortiert.

### Anzeigen von akzeptierten Domänen mithilfe von Exchange Online PowerShell

Zum Anzeigen von zusammenfassende Informationen zu allen akzeptierten Domänen, führen Sie den folgenden Befehl:

```
Get-AcceptedDomain
```

Verwenden Sie die folgende Syntax, um Details zu einer bestimmten akzeptierten Domäne anzuzeigen.

```
Get-AcceptedDomain -Identity <Name> | Format-List
```

Dieses Beispiel zeigt Informationen über die akzeptierte Domäne mit dem Namen "contoso.com".

```
Get-AcceptedDomain -Identity contoso.com | Format-List
```

## Konfigurieren des Domänentyps

Nach dem Hinzufügen einer Domäne zu Ihrer Exchange Online-Organisation in der Office 365 Admin Center kann die Domäne konfiguriert werden.

### Ändern des Domänentyps mithilfe der Exchange-Verwaltungskonsole

1. Wechseln Sie im EAC zu **E-Mail-Fluss > Akzeptierte Domänen**.
2. Wählen Sie die Domäne aus, und klicken Sie auf **Bearbeiten** .
3. Wählen Sie im Fenster **Akzeptierte Domäne** im Bereich **Diese akzeptierte Domäne ist** den Domänentyp aus. Die möglichen Werte sind **Autoritativ** und **Internes Relay**.
  - Wenn Sie **Autoritativ** auswählen, müssen Sie bestätigen, dass Sie die verzeichnisbasierte Edge-Blockierung aktivieren möchten.
  - Wenn Sie **Internes Relay** ausgewählt haben, können Sie Unterdomänen Nachrichtenübermittlung an alle Unterdomänen zu aktivieren. Weitere Informationen finden Sie unter [Enable Nachrichtenübermittlung für Unterdomänen in Exchange Online](#).
4. Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

### Ändern des Domänentyps mithilfe von Exchange Online PowerShell

Verwenden Sie die folgende Syntax, um den Domänentyp zu konfigurieren:

```
Set-AcceptedDomain -Identity <Name> -DomainType <Authoritative | InternalRelay>
```

In diesem Beispiel wird die akzeptierte Domäne mit dem Namen "contoso.com" als interne Relaydomäne konfiguriert.

```
Set-AcceptedDomain -Identity contoso.com -DomainType InternalRelay
```

Informationen zur Syntax und Parametern finden Sie unter [Set-AcceptedDomain](#).

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie den Domänentyp erfolgreich konfiguriert haben, führen Sie einen der folgenden Schritte aus:

- In der Exchange-Verwaltungskonsole unter **E-Mail-Fluss > Akzeptierte Domänen**, klicken Sie auf **Aktualisieren** . In der Liste der akzeptierten Domänen stellen Sie sicher, dass der Wert der Type Domäne der akzeptierten Domäne ordnungsgemäß konfiguriert ist.
- Führen Sie in Exchange Online PowerShell den Befehl `Get-AcceptedDomain`. In der Liste der akzeptierten Domänen stellen Sie sicher, dass der Wert der Type Domäne der akzeptierten Domäne ordnungsgemäß konfiguriert ist.

# Aktivieren der Nachrichtenübermittlung für Unterdomänen in Exchange Online

18.12.2018 • 6 minutes to read

Wenn Sie eine hybridumgebung verfügen, mit Postfächern gehostet sowohl im Exchange Online und lokalem Exchange und Sie über Unterdomänen der akzeptierten Domänen, die nur in Ihrer lokalen Umgebung, können Sie e-Mail-Nachrichtenfluss zu und von diesen lokalen Unterdomänen. Beispielsweise wenn Sie eine akzeptierte Domäne haben "contoso.com", und aktivieren Sie Unterdomänen, Benutzer können e-Mail zu senden oder Empfangen von e-Mails von allen Unterdomänen "contoso.com", die in Ihrer lokalen Umgebung, wie beispielsweise "Marketing.contoso.com" vorhanden und nwregion.contoso.com: In Microsoft Forefront Online Protection for Exchange (FOPE) wurde dieses Feature \_Catch-All-Domänen\_ bezeichnet.

## IMPORTANT

Wenn Sie eine begrenzte Anzahl von Unterdomänen haben und die Namen aller Unterdomäne kennen, empfehlen wir einrichten jedes Unterdomäne als akzeptierte Domäne im Office 365 Administrationscenter verwenden, anstatt mithilfe der Verfahren in diesem Thema. Jede Unterdomäne separat einrichten, können Sie haben eine genauere Kontrolle über e-Mail-Fluss und eindeutige Transportregeln für jede Unterdomäne enthalten. Weitere Informationen zum Hinzufügen einer Domäne im Office 365 Administrationscenter finden Sie unter [Hinzufügen Ihrer Domäne zu Office 365](#). >>, Um abgeglichene Unterdomänen zu aktivieren, eine akzeptierte Domäne muss eingerichtet sein als interne Relaydomäne. Informationen zu den Domänenentyp auf internes Relay festlegen finden Sie unter [Manage akzeptierte Domänen im Exchange, Online](#). >> Nach dem Aktivieren von Unterdomänen, in der Reihenfolge für den Dienst Nachrichtenübermittlung für alle Unterdomänen zu Ihrer Organisation e-Mail-Server (außerhalb von Office 365), müssen Sie auch den ausgehenden Connector ändern. Anweisungen finden Sie unter [Verwenden der Exchange-Verwaltungskonsole auf die Domäne ausgehenden Connector hinzufügen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Domänen" im Thema [Featureberechtigungen in Exchange Online](#).
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Einrichten des Abgleichs von Unterdomänen mit der Exchange-Verwaltungskonsole

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenübermittlung > Akzeptierte Domänen**, und wählen Sie die Domäne aus.
2. Stellen Sie sicher, dass **Internes Relay** ausgewählt ist, klicken Sie im Detailbereich.
3. Aktivieren Sie **Unterdomänen für diese Domäne zum Senden und Empfangen von E-Mails abgleichen**.

Verwenden Sie die EAC, um die Domänen zu Ihrem ausgehenden Connector hinzuzufügen.

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Connectors**.
2. Klicken Sie unter **Ausgehende Connectors**, wählen Sie den Connector für Ihre Organisation e-Mail-Server und wählen Sie dann auf **Bearbeiten** .
3. Klicken Sie auf **Bereich**, und wählen Sie dann eine der folgenden Optionen aus:
  - Wählen Sie **Alle akzeptierten Domänen über diesen Connector weiterleiten**.
  - Wählen Sie im Abschnitt **Empfänger Domänen neu**  Geben Sie im Feld **Domäne hinzufügen** einen Platzhaltereintrag für die Domäne für die Domäne für die Unterdomänen aktiviert. Geben Sie beispielsweise, wenn Sie Unterdomänen für "contoso.com" aktiviert, \*. "contoso.com" als eine Domäne des Empfängers.

#### NOTE

Wenn Sie noch nicht über eines ausgehenden Connectors verfügen, finden Sie unter [Configure e-Mail-Fluss mithilfe von Connectors in Office 365](#).

## Verwenden von Exchange Online PowerShell Einrichten des Abgleichs von Unterdomänen

Um abgeglichene Unterdomänen einer Domäne hinzuzufügen, die als internes Relay festgelegt ist, verwenden Sie folgende Syntax:

```
Set-AcceptedDomain -Identity <Domain Name> -MatchSubdomains $true
```

In diesem Beispiel werden abgeglichene Unterdomänen für die Domäne ".contoso.com" eingerichtet.

```
Set-AcceptedDomain -Identity contoso.com -MatchSubdomains $true
```

Informationen zur Syntax und Parametern finden Sie unter [Set-AcceptedDomain](#).

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie erfolgreich abgeglichene Unterdomänen einer Domäne mit Exchange Online PowerShell hinzugefügt haben, führen Sie den folgenden Befehl zum Überprüfen des Eigenschaftswert *MatchSubdomains* aus:

```
Get-AcceptedDomain | Format-List Name,MatchSubdomains
```

# Remotedomänen in Exchange Online

18.12.2018 • 14 minutes to read

Es gibt viele Gründe, warum Sie möglicherweise steuern die Typen und das Format von Nachrichten, die die Benutzer über Exchange Online an Empfänger in externen Domänen senden (Domänen, *werden nicht* als akzeptierte Domänen in Exchange Online konfiguriert). Zum Beispiel:

- Sie möchten Ihre Benutzer Nachrichten an Empfänger in anderen Domänen weiterleiten können.
- Sie arbeiten mit einer Organisation, die Sie keine automatische Nachrichten aus (beispielsweise Unzustellbarkeitsberichte und Abwesenheits Antworten) erhalten möchten.
- Sie haben einen Geschäftspartner, der sich außerhalb Ihrer Organisation befindet, und Sie möchten, dass dieser Partner die gleichen Abwesenheits Antworten wie für die Personen innerhalb Ihrer Organisation empfangen.
- Ihre Benutzer senden häufig E-Mails an ein Unternehmen, das beschränkte E-Mail-Formate unterstützt, und Sie möchten sicherstellen, dass alle an diese Organisation gesendeten E-Mails in einem Format gesendet werden, das die Personen in diesem Unternehmen lesen können.

Um dies zu erreichen, verwenden Sie was eine \_Remotedomäne\_ aufgerufen hat. Die Remotedomäneinstellungen haben Vorrang vor Einstellungen, die möglicherweise Ihre Benutzer in Outlook oder Outlook im Web (vormals Outlook Web App) konfigurieren oder, die Sie in der Exchange-Verwaltungskonsole (EAC) oder Exchange Online PowerShell konfigurieren. Beispielsweise Benutzer möglicherweise eine Abwesenheits Antwort für Personen außerhalb der Organisation eingerichtet haben, aber wenn von einer Remotedomäne Absender sendet eine e-Mail an sie und die Remotedomäne Abwesenheits Antworten empfangen nicht festgelegt ist, wird keine Abwesenheits Antwort gesendet. Um die Einstellungen zu ändern, können Sie folgende Aktionen ausführen:

- Erstellen Sie eine Remotedomäne für eine bestimmte Domäne, und legen Sie eindeutige Eigenschaften für an diese Domäne gesendete E-Mails fest.
- Ändern Sie die Einstellungen für die Standardremotedomäne. Wenn Sie keine anderen Remotedomänen eingerichtet haben, werden Änderungen an der Standardremotedomäne für alle externen Domänen angewendet. Wenn Sie andere Remotedomänen eingerichtet haben, werden Änderungen an der Standardremotedomäne für alle externen Domänen angewendet.

Anweisungen zum Erstellen und Konfigurieren von Remotedomänen finden Sie unter [Verwalten von Remotedomänen in Exchange Online](#).

## Verringern oder Erhöhen des Informationsflusses an ein anderes Unternehmen

Wenn eine Nachricht von außerhalb Ihrer Organisation eingeht, können verschiedene automatische Antworten generiert werden. Einige Arten von Antworten werden von Benutzern in Outlook oder Outlook Web App eingerichtet, andere werden von Administratoren festgelegt. Da die Einstellungen für die Remotedomäne sowohl die von Benutzern konfigurierten Einstellungen als auch die von Administratoren konfigurierten E-Mail-Benutzer- und E-Mail-Kontakteinstellungen außer Kraft setzen, können Sie auswählen, welche Arten von automatischen Antworten an alle Personen in einer Remotedomäne gesendet werden.

Wenn in der Konfiguration einer Remotedomäne festgelegt ist, dass das Senden einer bestimmten Art von Antwort, z. B. eines Unzustellbarkeitsberichts, an Empfänger in dieser Domäne blockiert ist, wird die Antwort zwar

generiert, aber dann vor dem Senden gelöscht. Es wird keine Fehlermeldung gesendet. Wenn Sie beispielsweise das automatische Weiterleiten in der Standardremotedomäne deaktivieren und Benutzer versuchen, eine E-Mail automatisch an eine andere Domäne weiterzuleiten, können sie zwar ihre Einstellungen ändern oder eine Posteingangsregel erstellen, aber ihre Nachrichten werden nicht weitergeleitet.

In der folgenden Tabelle sind die Arten von Antworten, die Sie in einer Remotedomäne steuern können, und die Einstellungen aufgeführt, die von der jeweiligen Remotedomäneneinstellung außer Kraft gesetzt werden.

ART VON ANTWORT	BESCHREIBUNG	EINSTELLUNGEN AUF BENUTZERBASIS, DIE VON DIESER REMOTEDOMÄNENEINSTELLUNG AUSSER KRAFT GESETZT WERDEN
Abwesenheitsnachrichten	<p>Geben Sie an, ob eine Abwesenheitsnachricht an Personen in der Remotedomäne gesendet werden soll, und falls ja, welche Nachricht verwendet wird. Sie können entweder die Antwort, die der Benutzer in Ihrer Domäne für Personen außerhalb Ihrer Organisation eingerichtet hat, oder die Antwort für Personen innerhalb Ihrer Organisation auswählen.</p> <p>Standardmäßig wird die Abwesenheitsnachricht für Personen außerhalb Ihrer Organisation gesendet.</p>	<p>Mit dieser Einstellung werden die Einstellungen für Abwesenheitsnachrichten außer Kraft gesetzt, die von einzelnen Benutzern in <a href="#">Outlook</a> oder <a href="#">Outlook im Web</a> angegeben wurden.</p>
Automatische Antworten	<p>Geben Sie an, ob automatische Antworten an Absender in der Remotedomäne zugelassen sind oder verhindert werden. Standardmäßig werden automatische Antworten zulassen.</p>	<p>Mit dieser Einstellung werden die von Administratoren über das Cmdlet <a href="#">Set-MailboxAutoReplyConfiguration</a> eingerichteten automatischen Antworten außer Kraft gesetzt.</p>

ART VON ANTWORT	BESCHREIBUNG	EINSTELLUNGEN AUF BENUTZERBASIS, DIE VON DIESER REMOTEDOMÄNENEINSTELLUNG AUSSER KRAFT GESETZT WERDEN
Automatische Weiterleitungen	<p>Geben Sie an, ob das Senden von automatisch weitergeleiteten Nachrichten an Personen in der Remotedomäne zugelassen ist oder verhindert wird. Standardmäßig ist das automatische Weiterleiten zugelassen.</p>	<p>Wenn Benutzer die automatische Weiterleitung an Empfänger in einer Remotedomäne konfigurieren, überschreiben die Einstellungen der Remotedomäne die automatische Weiterleitungseinstellungen der Benutzer (Nachrichten werden blockiert, wenn automatische Weiterleitungen für die Remotedomäne deaktiviert sind).</p> <p>Benutzer können die automatische Weiterleitung mithilfe der folgenden Methoden konfigurieren:</p> <ul style="list-style-type: none"> <li>• Posteingang Regeln in Outlook oder Outlook im Web zum Weiterleiten von Nachrichten. Weitere Informationen zu Posteingangsregeln in <a href="#">Outlook</a> und <a href="#">Outlook im Web</a>.</li> <li>• Weiterleitungsoptionen in Outlook im Web. Weitere Informationen finden Sie unter <a href="#">Weiterleiten von e-Mails von Office 365 an ein anderes e-Mail-Konto</a>.</li> </ul> <p><b>Hinweis:</b> Wenn Administratoren andere Methoden verwenden, um die automatische Weiterleitung für Benutzer zu konfigurieren, sind die weitergeleiteten Nachrichten nicht von den Einstellungen der Remotedomäne betroffen (Nachrichten werden an Empfänger in der Remotedomäne weitergeleitet, selbst dann, wenn automatische Weiterleitungen für die Remotedomäne deaktiviert sind).</p> <p>Beispiel:</p> <ul style="list-style-type: none"> <li>• E-Mail-Weiterleitung für einen Benutzer. Weitere Informationen finden Sie unter <a href="#">Configure e-Mail-Weiterleitung für ein Postfach</a>.</li> <li>• E-Mail-Flussregeln (auch als Transportregeln bezeichnet) zum Weiterleiten von Nachrichten. Weitere Informationen finden Sie unter <a href="#">E-Mail-Fluss Regeln (Transportregeln) in Exchange Online</a>.</li> </ul>

ART VON ANTWORT	BESCHREIBUNG	EINSTELLUNGEN AUF BENUTZERBASIS, DIE VON DIESER REMOTEDOMÄNENEINSTELLUNG AUSSEN KRAFT GESETZT WERDEN
Übermittlungsberichte	Geben Sie an, ob das Senden einer Übermittlungsbestätigung an Personen in der Remotedomäne zugelassen ist oder verhindert wird. Standardmäßig ist das Senden von Übermittlungsberichten zugelassen.	Ein E-Mail-Absender in der Remotedomäne kann eine Übermittlungsbestätigung für eine Nachricht anfordern. Diese Einstellung für die Remotedomäne kann die Anforderung eines Übermittlungsberichts des Absenders außer Kraft setzen und verhindern, dass der Übermittlungsbericht gesendet wird. Weitere Informationen zum Anfordern einer Übermittlungsbestätigung finden Sie unter <a href="#">Hinzufügen von Nachverfolgung zu E-Mail-Nachrichten</a> .
Unzustellbarkeitsbericht	Geben Sie an, ob das Senden von Unzustellbarkeitsberichten an Personen in der Remotedomäne zugelassen ist oder verhindert wird. Standardmäßig ist das Senden von Unzustellbarkeitsberichten zugelassen.	Diese Remotedomäneneinstellung ist die einzige Methode, um das Senden von Unzustellbarkeitsberichten zu verhindern, wenn eine Nachricht nicht übermittelt werden kann.
Benachrichtigungen über Besprechungsweiterleitung	Geben Sie an, ob das Senden von Benachrichtigungen über Besprechungsweiterleitung an Personen in der Remotedomäne zugelassen ist oder verhindert wird. Standardmäßig wird das Senden von Besprechungsweiterleitungsberechtigungen verhindert.	Benachrichtigungen über Besprechungsweiterleitung werden automatisch erstellt und an den Besprechungsorganisator gesendet, wenn ein Besprechungsteilnehmer eine Besprechung weiterleitet. Normalerweise werden diese Benachrichtigungen nur an Besprechungsorganisatoren in Domänen gesendet, die Teil Ihrer Exchange Online-Organisation sind. Administratoren können das Senden dieser Benachrichtigungen an Besprechungsorganisatoren in der Remotedomäne aktivieren.

## Angeben des Nachrichtenformats

Sie können das Nachrichtenformat und den Zeichensatz für alle an die Remotedomäne gesendeten E-Mail-Nachrichten angeben, um sicherzustellen, dass E-Mails, die von Ihrer Exchange Online-Organisation gesendet werden, mit dem empfangenden Nachrichtensystem in dieser Remotedomäne kompatibel sind. Wenn Sie beispielsweise wissen, dass in der Remotedomäne Exchange nicht verwendet wird, können Sie angeben, niemals RTF (Rich-Text-Format) zu verwenden. In der folgenden Tabelle sind die Einstellungen für das Nachrichtenformat beschrieben.

EINSTELLUNG	BESCHREIBUNG	EINSTELLUNGEN, DIE DAMIT AUSSEN KRAFT GESETZT WERDEN
-------------	--------------	--

EINSTELLUNG	BESCHREIBUNG	EINSTELLUNGEN, DIE DAMIT AUSSER KRAFT GESETZT WERDEN
Rich-Text-Format (RTF)	<p>Wählen Sie aus, wie Nachrichten formatiert werden:</p> <ul style="list-style-type: none"> <li>• <b>Immer:</b> Verwenden Sie diesen Wert, wenn in die Remotedomäne Exchange verwendet wird.</li> <li>• <b>Nie:</b> Wenn Exchange in die Remotedomäne nicht verwendet wird, verwenden Sie diesen Wert.</li> <li>• <b>Führen Sie die Benutzereinstellungen:</b> vom Benutzer definierte Nachrichtenformate verwenden. Verwenden Sie diesen Wert, wenn Sie nicht wissen, welche e-Mail-System die Remotedomäne verwendet.</li> </ul> <p>Standardmäßig werden die Benutzereinstellungen verwendet.</p>	<p>Das Nachrichtenformat kann an mehreren Stellen definiert werden: Outlook oder Outlook im Web, zudem kann der Administrator die Einstellungen pro Empfänger auch über das Cmdlet <a href="#">Set-MailContact</a> oder das Cmdlet <a href="#">Set-MailUser</a> ändern.</p> <p>Die Einstellungen für die Remotedomäne setzen die von einem Benutzer oder dem Administrator angegebenen Einstellungen außer Kraft. Weitere Informationen zu Nachrichtenformaten und der Reihenfolge der Priorität von Nachrichtenformateinstellungen finden Sie unter <a href="#">Nachrichtenformat und -übertragung in Exchange Online</a>.</p>
MIME-Zeichensatz und Nicht-MIME-Zeichensatz	<ul style="list-style-type: none"> <li>• <b>Keine:</b> Verwenden Sie den in der Nachricht angegebenen Zeichensatz.</li> <li>• <b>Wählen Sie einen Zeichensatz aus der Liste aus:</b> Wenn die Nachricht einen Zeichensatz nicht vorhanden ist, wird der ausgewählte Zeichensatz verwendet.</li> </ul> <p>Standardmäßig werden keine Zeichensätze angegeben.</p>	<p>Diese Einstellungen dienen nur, wenn die Nachricht einen Zeichensatz enthalten nicht. Eine vollständige Liste der unterstützten Zeichensätzen finden Sie unter <a href="#">unterstützte Zeichensätze für Remotedomänen</a>.</p>

Wenn Sie für die Remotedomäne ein bestimmtes Nachrichtenformat festlegen, wird das Format der an die Domäne gesendeten Kopfzeilen und Nachrichteninhalte geändert.

## Weitere Einstellungen

Sie können andere Nachrichteneinstellungen für Remotedomänen über die Exchange Online PowerShell konfigurieren. Eine vollständige Liste der Einstellungen finden Sie unter [Set-RemoteDomain](#).

## Was muss ich sonst noch wissen?

- Sie können eine Remotedomäne nur für eine externe Domäne einrichten. Eine Domäne wird als extern definiert, wenn sie nicht auf der Seite **Office 365 Admin Center > Domänen** aufgelistet ist. Wenn beispielsweise fabrikam.com eine Ihrer Domänen ist, können Sie für fabrikam.com keine Remotedomäne konfigurieren.
- Die Standardremotedomäne kann nicht entfernt werden.
- Sie können alle Unterdomänen angeben, wenn Sie eine Remotedomäne erstellen.

## See also

[Verwalten von Remotedomänen in Exchange Online](#)

# Verwalten von Remotedomänen in Exchange Online

18.12.2018 • 12 minutes to read

Remotedomänen definieren Einstellungen basierend auf der Zieldomäne allen e-Mail-Nachrichten. Alle Organisationen verfügen über eine Standard-Remotedomäne namens "Default", die auf die Domäne angewendet wird "\*". Die Standardremotedomäne gilt die gleichen Einstellungen für alle e-Mail-Nachrichten unabhängig von der Zieldomäne. Jedoch können Sie bestimmte Einstellungen für eine bestimmte Zieldomäne konfigurieren.

Die folgende Tabelle zeigt die Standardwerte für allgemeine Einstellungen:

EINSTELLUNG	STANDARD
Abwesenheitsantworten	Externe Abwesenheitsantworten werden an Personen in der Remotedomäne gesendet.
Automatische Antworten	Automatische Antworten oder automatisch weitergeleitete Nachrichten können an Personen in der Remotedomäne gesendet werden.
Zustellungs- und Unzustellbarkeitsberichte	Zustellungs- und Unzustellbarkeitsberichte können an Personen in der Remotedomäne gesendet werden.
Besprechungsweiterleitungsbenachrichtigungen	Besprechungsweiterleitungsbenachrichtigungen können nicht an Personen in der Remotedomäne gesendet werden.
Rich-Text-Format (RTF)	Wenn eine Nachricht an Personen in der Remotedomäne gesendet wird, werden die von jedem Benutzer in Outlook oder Outlook Web App erstellten Einstellungen befolgt.
Unterstützter Zeichensatz	Keinen MIME- oder Nicht-MIME-Zeichensatz angegeben, wenn der Zeichensatz nicht in der Nachricht angegeben wurde, die an die Remotedomäne gesendet wird.

Weitere Informationen dazu, wann Remotedomänen konfiguriert werden, Beschreibungen der verfügbaren Einstellungen sowie Informationen dazu, wie benutzerbezogene Einstellungen durch Remotedomäneninstellungen überschrieben werden, finden Sie unter [Remotedomänen in Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Nachrichtenübermittlung" im Thema [Featureberechtigungen in Exchange Online](#).
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Erstellen und Konfigurieren von Remotedomänen

## Hinweise:

- Sie können eine Remotedomäne für eine Domäne, die aufgeführt wird für das **Office 365-Verwaltungskonsole** konfigurieren > Seite **Domänen**. Wenn fabrikam.com eines Ihre akzeptierten Domänen ist, können nicht Sie eine Remotedomäne für fabrikam.com erstellen.
- Wenn Sie eine Remotedomäne für eine bestimmte Zieldomäne und eine Einstellung für bestimmte Remotedomäne Konflikte mit der gleichen Einstellung in der Standardeinstellung Remotedomäne erstellen, überschreibt die Einstellung für die bestimmten Remotedomäne die Einstellung in der Standardremotedomäne.
- Wenn Sie eine Remotedomäne erstellt haben, nicht ändern oder Ersetzen Sie die Domäne in der Remotedomäne. In diesem Fall erstellen Sie und konfigurieren Sie eine neue Remotedomäne mit den neuen Domänennamen.

## Erstellen und Konfigurieren einer Remotedomäne mithilfe der Exchange-Verwaltungskonsole

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenübermittlung > Remotedomänen**.
2. So erstellen Sie eine neue Domäne
3. Wählen Sie **neue**
4. Geben Sie einen beschreibenden Namen für die Domäne in das Feld **Name** ein.
5. Geben Sie im Feld **Remotedomäne** den vollständigen Domänennamen ein. Verwenden Sie das Platzhalterzeichen (\*) für alle Unterdomänen einer angegebenen Domäne, z. B. ".contoso.com".
6. Wählen Sie **Standard** und dann **Bearbeiten** aus, um die Einstellungen für die Standarddomäne zu ändern.
7. Wählen Sie die gewünschten Optionen aus:
  - Geben Sie im Abschnitt **Out of Office Reply Typen** an, abwesend welche, die Antworten an Personen in dieser Domäne gesendet werden soll.
  - Geben Sie im Bereich **Automatische Antworten** an, ob Sie automatische Antworten, automatische Weiterleitungen oder beides zulassen möchten.
  - Klicken Sie im Abschnitt **Nachricht reporting** angeben:
    - Ob Sie Zustellungsberichte und Unzustellbarkeitsberichte zulassen möchten.
    - Wenn eine von einer Person in der Remotedomäne eingerichtete Besprechung an eine andere Person in Ihrer Organisation weitergeleitet wird, ob die Benachrichtigung an den Besprechungsorganisator in der Remotedomäne gesendet werden soll.
  - Geben Sie im Bereich **Rich-Text-Format verwenden** an, ob die Nachrichteneinstellungen der einzelnen Benutzer befolgt werden sollen oder ob die RTF-Formatierung immer bzw. niemals beibehalten werden soll. Das Auswählen von **Nie** bedeutet, dass RTF-Nachrichten als Nur-Text oder HTML gesendet werden.
  - Klicken Sie im Bereich **Unterstützten Zeichensatz** Geben Sie an, welcher Zeichensatz verwenden, wenn die Nachricht nicht Zeichensatz angegeben ist.

5. Klicken Sie auf **Speichern**. Wenn Sie eine neue Remotedomäne erstellt haben, wird diese der Liste hinzugefügt.

## Verwenden Sie zum Erstellen und Konfigurieren einer Remotedomäne Exchange Online PowerShell

Nachdem Sie die Remotedomäne erstellt haben, können Sie die Einstellungen (Sie können nicht die Remotedomäne erstellen und konfigurieren Sie die Einstellungen in einem Schritt) konfigurieren.

### Schritt 1: Erstellen der Remotedomäne

Wenn eine neue Remotedomäne erstellen möchten, verwenden Sie die folgende Syntax:

```
New-RemoteDomain -Name "<Unique Name>" -DomainName <single SMTP domain | domain with subdomains>
```

In diesem Beispiel wird eine Remotedomäne für Nachrichten erstellt, die an die Domäne "contoso.com" gesendet werden.

```
New-RemoteDomain -Name Contoso -DomainName contoso.com
```

In diesem Beispiel wird eine Remotedomäne für Nachrichten erstellt, die an die Domäne "contoso.com" und alle ihre Unterdomänen gesendet werden.

```
New-RemoteDomain -Name "Contoso and subdomains" -DomainName *.contoso.com
```

Ausführliche Parameterinformationen zu Syntax und finden Sie unter [New-RemoteDomain](#).

### Schritt 2: Konfigurieren der Remotedomäneinstellungen

Um die Einstellungen für eine Remotedomäne festlegen möchten, verwenden Sie die folgende Syntax:

```
Set-RemoteDomain -Identity <Name> [-AllowedOOFType <External | InternalLegacy | ExternalLegacy | None>] [-AutoForwardEnabled <$true | $false>] [-AutoReplyEnabled <$true | $false>] [-CharacterSet <SupportedCharacterSet>] [-DeliveryReportEnabled <$true | $false>] [-NonMimeCharacterSet <SupportedCharacterSet>] [-TNEFEnabled <$true | $false>]
```

In diesem Beispiel werden automatische Antworten, automatische Weiterleitungen und Abwesenheitsbenachrichtigungen an Empfänger in allen Remotedomänen deaktiviert, die nicht bei ihrer eigenen Remotedomäne angegeben sind.

```
Set-Set-RemoteDomain -Identity Default -AutoReplyEnabled $false -AutoForwardEnabled $false -AllowedOOFType None
```

In diesem Beispiel werden interne Abwesenheitsbenachrichtigungen an Benutzer in der Remotedomäne namens Contoso gesendet.

```
Set-Set-RemoteDomain -Identity Contoso -AllowedOOFType InternalLegacy
```

In diesem Beispiel werden Zustellungs- und Unzustellbarkeitsberichte an Benutzer in Contoso deaktiviert.

```
Set-Set-RemoteDomain -Identity Contoso -DeliveryReportEnabled $false -NDREnabled $false
```

In diesem Beispiel sendet alle Nachrichten an Contoso mit Codierung Transport Neutral Encapsulation Bildung (TNEF) statt mit MIME-Codierung. Dadurch wird die Rich-Text-Format in Nachrichten beibehalten.

```
Set-Set-RemoteDomain -Identity Contoso -TNEFEnabled $true
```

In diesem Beispiel werden alle Nachrichten an Contoso über die MIME-Codierung gesendet; dies bedeutet, dass alle RTF-Nachrichten stets zu HTML oder Nur-Text konvertiert werden.

```
Set-Set-RemoteDomain -Identity Contoso -TNEFEnabled $false
```

In diesem Beispiel werden die vom Benutzer in Outlook oder Outlook Web App zur Codierung von Nachrichten definierten Einstellungen für das Nachrichtenformat verwendet.

```
Set-Set-RemoteDomain -Identity Contoso -TNEFEnabled $null
```

In diesem Beispiel wird der koreanische Zeichensatz (ISO) für MIME-Nachrichten verwendet, die an Contoso gesendet werden.

```
Set-Set-RemoteDomain -Identity Contoso -CharacterSet iso-2022-kr
```

In diesem Beispiel wird die Verwendung des Unicode-Zeichensatzes für Nicht-MIME-Nachrichten dargestellt, die an Contoso gesendet werden.

```
Set-Set-RemoteDomain -Identity Contoso -NonMimeCharacterSet utf-8
```

Informationen zur Syntax und Parametern finden Sie unter [Set-RemoteDomain](#).

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie erfolgreich erstellt und eine Remotedomäne konfiguriert haben, verwenden Sie entweder die folgenden Schritte:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Remotedomänen**, wählen Sie die Remotedomäne aus, und klicken Sie dann auf **Bearbeiten**  um die Einstellungen zu überprüfen.
- Ersetzen Sie in Exchange Online PowerShell <Remote Domänenamen> mit dem Namen der Remotedomäne und führen den folgenden Befehl, um die Einstellungen zu überprüfen:

```
Get-RemoteDomain -Identity "<Remote Domain Name>" | Format-List
```

## Entfernen von Remotedomänen

### Hinweise:

- Die Standardremotedomäne kann nicht entfernt werden.
- Wenn Sie eine Remotedomäne entfernen, werden die Standardeinstellungen für die Remotedomäne klicken Sie dann auf an diese Domäne gesendete Nachrichten angewendet.
- Durch das Entfernen einer Remotedomäne wird der E-Mail-Fluss zur Remotedomäne nicht deaktiviert.

### Entfernen einer Remotedomäne mithilfe der Exchange-Verwaltungskonsole

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenübermittlung > Remotedomänen**.
2. Wählen Sie eine Remotedomäne aus, und wählen Sie dann **Löschen** .

3. Klicken Sie im Dialogfeld der Warnmeldung auf **Ja**.

### **Entfernen einer Remotedomäne mithilfe von Exchange Online PowerShell**

Wenn Sie eine Remotedomäne entfernen möchten, verwenden Sie die folgende Syntax:

```
Remove-RemoteDomain -Identity <Remote Domain Name>
```

In diesem Beispiel wird die Remotedomäne "Contoso" entfernt.

```
Remove-RemoteDomain -Identity Contoso
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Remove-RemoteDomain](#).

### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Zum bestätigen, dass Sie eine Remotedomäne erfolgreich entfernt haben, führen Sie einen der folgenden Schritte aus:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > Remotedomänen** und überprüfen Sie, ob die Remotedomäne wird nicht aufgeführt.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, und stellen Sie sicher, dass die Remotedomäne aufgeführt ist:

```
Get-RemoteDomain
```

# Unterstützte Zeichensätze für Remotedomänen in Exchange Online

18.12.2018 • 2 minutes to read

Remotedomänen definieren Einstellungen basierend auf der Zieldomäne allen e-Mail-Nachrichten. Alle Organisationen verfügen über eine Standard-Remotedomäne namens "Default", die auf die Domäne angewendet wird "\*". Die Standardremotedomäne gilt die gleichen Einstellungen für alle e-Mail-Nachrichten unabhängig von der Zieldomäne. Jedoch können Sie bestimmte Einstellungen für eine bestimmte Zieldomäne konfigurieren.

Weitere Informationen zu Remotedomänen finden Sie unter [Remotedomänen in Exchange Online](#).

Remotedomäne Anweisungen finden Sie unter [Verwalten von Remotedomänen in Exchange Online](#).

Die folgende Tabelle beschreibt die Zeichensätze, die Sie in Remotedomänen konfigurieren können.

- Navigieren Sie im Exchange Administrationscenter (EAC) zu **Nachrichtenfluss > Remotedomänen**. Klicken Sie auf **neu**  eine neue Remotedomäne erstellen, oder wählen Sie die vorhandene Remotedomäne, und klicken Sie auf **Bearbeiten** . Klicken Sie im Einstellungsfenster, das geöffnet wird mithilfe der Dropdownlisten **MIME-Zeichensatz** und **nicht-MIME-Zeichensatz** den Zeichensatz aus.
- Verwenden Sie in Exchange Online PowerShell den Wert in der Spalte Name in der folgenden Tabelle für den *UTF*-Parameter oder 'NonMimeCharacterSet' Parameter im Cmdlet [Set-RemoteDomain](#) .

NAME	BESCHREIBUNG
Big5	Chinesisch Traditionell (Big5)
DIN_66003	Deutsch (IA5)
euc-jp	Japanisch (EUC)
euc-kr	Koreanisch (EUC)
GB18030	Chinesisch Vereinfacht (GB18030)
GB2312	Chinesisch Vereinfacht (GB2312)
hz-gb-2312	Chinesisch Vereinfacht (HZ)
ISO-2022-JP	Japanisch (JIS)
ISO-2022-KR	Koreanisch (ISO)
ISO-8859-1	Westeuropäisch (ISO)
ISO-8859-2	Mitteleuropäisch (ISO)
ISO-8859-3	Lateinisch 3 (ISO)

NAME	BESCHREIBUNG
ISO-8859-4	Baltisch (ISO)
ISO-8859-5	Kyrillisch (ISO)
ISO-8859-6	Arabisch (ISO)
ISO-8859-7	Griechisch (ISO)
ISO-8859-8	Hebräisch (ISO)
ISO-8859-9	Türkisch (ISO)
ISO-8859-13	Estnisch (ISO)
ISO-8859-15	Lateinisch 9 (ISO)
KOI8-R	Kyrillisch (KOI8-R)
KOI8-U	Kyrillisch (KOI8-U)
KS_C_5601-1987	Koreanisch (Windows)
NS_4551-1	Norwegisch (IA5)
SEN_850200_B	Schwedisch (IA5)
Shift_jis	Japanisch (Shift-JIS)
UTF-8	Unicode (UTF-8)
Windows-1250	Mitteleuropäisch (Windows)
Windows-1251	Kyrillisch (Windows)
Windows-1252	Westeuropäisch (Windows)
Windows-1253	Griechisch (Windows)
Windows-1254	Türkisch (Windows)
Windows-1255	Hebräisch (Windows)
Windows-1256	Arabisch (Windows)
Windows-1257	Baltisch (Windows)
Windows-1258	Vietnamesisch (Windows)
Windows-874	Thailändisch (Windows)

# Nachrichtenformat und -übertragung in Exchange Online

18.12.2018 • 10 minutes to read

Es gibt Einstellungen in Outlook, Outlook im Web und Exchange Online das Steuerelement das Format der e-Mail-Nachrichten und wie sie an Personen in anderen Domänen gesendet werden. Die Standardeinstellungen für die Arbeit in den meisten Fällen. Wenn Sie bestimmte Empfänger Probleme beim Lesen von Nachrichten, die von Ihrer Organisation gesendet haben, können Sie die Einstellungen für einzelne Benutzer oder für alle Benutzer auf eine bestimmte Domäne anpassen. Beispielsweise können Sie verhindern, dass Empfänger winmail.dat-Anlagen empfangen.

Es gibt zwei Arten von Einstellungen, die Sie verwenden können:

- **Nachrichtenformat:** Beim Erstellen von Nachrichten können Benutzer das Nachrichtenformat auswählen, in dem die Nachricht verfasst wird. In Outlook haben sie die Wahl zwischen "Nur-Text", "HTML" und "RTF (Rich Text Format)". In Outlook Web App können sie zwischen "Nur Text" und "HTML" wählen.
- **Nachrichtenübertragung:** Hiermit wird angegeben, wie die Nachricht tatsächlich an das andere E-Mail-System gesendet wird. Exchange kann Nachrichten an andere Domänen mithilfe von MIME (Multipurpose Internet Mail Extensions) oder TNEF (Transport Neutral Encapsulation Format) senden. Alle drei Nachrichtenformate können mit TNEF gesendet werden. Nur die Formate "HTML" und "Nur Text" können mit MIME gesendet werden. Das Nachrichtenübertragungsformat kann von einem Administrator pro Domäne oder pro Empfänger festgelegt werden. Benutzer können das Nachrichtenübertragungsformat ebenfalls festlegen.

## Nachrichtenformate

In der folgenden Liste werden die drei Nachrichtenformate beschrieben, die in Exchange Online verfügbar sind. Sie zeigt, welche Formate in Outlook und Outlook Web App zur Verfügung stehen:

FORMAT	BESCHREIBUNG	VERFÜGBAR IN OUTLOOK	VERFÜGBAR IN OUTLOOK IM WEB
<b>Nur-Text</b>	Eine Nur-Text-Nachricht verwendet ausschließlich US-ASCII-Text gemäß RFC 2822. Die Nachricht kann keine unterschiedlichen Schriftarten oder andere Textformatierungen enthalten.	Ja	Ja
<b>HTML</b>	Eine HTML-Nachricht unterstützt Textformatierung, Hintergrundbilder, Tabellen, Aufzählungszeichen und andere grafische Elemente.	Ja	Ja

FORMAT	BESCHREIBUNG	VERFÜGBAR IN OUTLOOK	VERFÜGBAR IN OUTLOOK IM WEB
<b>Rich-Text-Format (RTF)</b>	RTF unterstützt die Textformatierung und andere grafische Elemente. Nur Outlook, Outlook Web App und einige wenige andere MAPI-E-Mail-Clients können RTF-Nachrichten auswerten.	Ja	Kann als RTF formatierte Nachrichten lesen, aber keine Nachrichten in diesem Format erstellen oder senden

[Return to top](#)

## Nachrichtenübertragungsformate für an externe Empfänger gesendete E-Mails

In der folgenden Tabelle werden die Nachrichtenübertragungsformate beschrieben, die Exchange Online zum Senden von E-Mails an externe Empfänger verwendet.

ÜBERTRAGUNGSFORMAT	BESCHREIBUNG
<b>TNEF (Transport Neutral Encapsulation Format)</b>	<p>TNEF ist ein Microsoft-spezifisches Format über die Übermittlung formatierter E-Mails. Eine TNEF-Nachricht enthält eine Nur-Text-Version der Nachricht sowie eine Anlage, die eine gepackte Version der formatierten Originalversion der Nachricht enthält. Diese Anlage hat in der Regel den Namen "Winmail.dat". Die Winmail.dat-Anlage enthält die Formatierung, Anlagen sowie Outlook-spezifische Features wie Besprechungsanfragen.</p> <p>Ein E-Mail-Client, der TNEF vollständig interpretieren kann, wie z. B. Outlook, verarbeitet die Anlage "Winmail.dat" und zeigt den ursprünglichen Nachrichteninhalt an, ohne je die Anlage "Winmail.dat" anzuzeigen. Ein E-Mail-Client, der TNEF nicht interpretieren kann, stellt eine TNEF-Nachricht möglicherweise auf eine der folgenden Arten dar:</p> <ul style="list-style-type: none"> <li>Die Textversion der Nachricht wird angezeigt, und die Nachricht enthält eine Anlage, die mit dem Namen "Winmail.dat", Win.dat oder einen anderen generischen Namen wie Att_nnnnn_dat oder Att_nnnnn_eml, wobei der Platzhalter Nnnnn eine Zufallszahl darstellt.</li> <li>Die Nur-Text-Version der Nachricht wird angezeigt. Die TNEF-Anlage wird ignoriert oder entfernt. Das Ergebnis ist eine Nur-Text-Nachricht.</li> <li>Es gibt Dienstprogramme von Drittanbietern, die bei der Konvertierung von Winmail.dat-Anlagen helfen können.</li> </ul>
MIME (Multipurpose Internet Mail Extensions)	MIME ist ein Internetstandard, der Text in anderen Zeichensätzen als ASCII, Anlagen, die kein Text sind, Nachrichtentext mit mehreren Teilen und Headerinformationen in Nicht-ASCII-Zeichensätzen unterstützt.

## Nachrichtenformat und Übertragungseinstellungen

Administratoren und Benutzer können die Nachrichtenformatierung und -übermittlung steuern. Administratoreinstellungen setzen Benutzereinstellungen außer Kraft.

Administratoren können die folgenden Einstellungen steuern:

- **Remotedomäneneinstellungen:** Remotedomäneneinstellungen steuern das Format von Nachrichten an Personen in der Remotedomäne gesendet. Sie können das Format für eine bestimmte externe Domäne oder für alle externen Domänen steuern. Weitere Informationen zu Remotedomänen finden Sie unter [Remotedomänen in Exchange Online](#). Die Remotedomäneneinstellungen haben Vorrang vor der benutzerspezifische Einstellungen, die von Administratoren oder Benutzern festgelegt.
- **E-Mail-Benutzer und e-Mail-kontakteinstellungen:** die Einstellungen für einzelne Empfänger durch Ändern der Einstellungen für bestimmte e-Mail-Benutzer oder e-Mail-Kontakte ändern. E-Mail-Benutzer und e-Mail-Kontakte sind ähnlich, da beide über externe e-Mail-Adressen verfügen und Informationen zu Personen außerhalb der Exchange Online-Organisation enthalten. Der Hauptunterschied ist, dass e-Mail-Benutzer-Benutzer-IDs verfügen, die zur Anmeldung bei der Exchange Online-Organisation verwendet werden können. Ein Administrator eine Einstellung für die pro Empfänger geändert wird, überschrieben Einstellungen, die ein Benutzer für diesen Empfänger festlegt. Weitere Informationen über die administratoreinstellung finden Sie unter [Manage Mail Users](#) und [Verwalten von e-Mail-Kontakte](#).

Benutzer können die folgenden Einstellungen steuern:

- **Outlook-Einstellungen:** In Outlook können Sie die Nachricht nachrichtenformatierungs- und Codierungsoptionen in der folgenden Liste beschriebenen festlegen:
  - **Nachrichtenformat:** Sie können das Standard-Nachrichtenformat für alle Nachrichten festlegen. Sie können das standardmäßige Nachrichtenformat außer Kraft setzen, wie Sie eine bestimmte Nachricht erstellen.
  - **Internet-Nachrichtenformat:** Sie können steuern, ob TNEF-Nachrichten zu remote Empfänger gesendet werden, oder gibt an, ob sie zuerst in ein kompatibler Format konvertiert werden. Sie können auch verschiedene nachrichtencodierungsoptionen für Nachrichten an Empfänger remote angeben. Diese Einstellungen gelten nicht für Nachrichten, die an Empfänger in der Exchange Online-Organisation gesendet.
  - **Nachrichtenformat für Internetempfänger:** Sie können steuern, ob die TNEF-Nachrichten an bestimmte Empfänger gesendet werden, oder gibt an, ob sie zuerst in ein kompatibler Format konvertiert werden. Sie können die Optionen für bestimmte Kontakte im Ordner Kontakte festlegen und Sie können diese Optionen für einen bestimmten Empfänger im Feld an, Cc, außer Kraft setzen oder Bcc Felder wie einer Nachricht verfassen. Diese Optionen sind nicht verfügbar für Empfänger in der Exchange Online-Organisation.
  - **Nachrichtenformat für Internetempfänger Internet Codierungsoptionen:** können Sie steuern, die MIME- oder nur-Text-Codierung Optionen für bestimmte Kontakte im Ordner Kontakte, und Sie können diese Optionen für einen bestimmten Empfänger im Feld an, Cc, außer Kraft setzen oder Bcc Felder wie beim Verfassen einer Nachricht. Diese Optionen sind nicht verfügbar für Empfänger in der Exchange Online-Organisation.
  - **Internationale Optionen:** Sie können in Nachrichten verwendeten Zeichensätze steuern.

Weitere Informationen zu den Outlook-Einstellungen finden Sie unter [Ändern des Nachrichtenformats in "Nur-Text", "HTML" oder "Rich-Text-Format"](#).

- **Outlook Web App/Outlook auf der webeinstellungen:** Sie können die Nachricht in der folgenden Liste beschriebenen Formatierungsoptionen festlegen:
  - **Nachrichtenformat:** Sie können das Standard-Nachrichtenformat für alle Nachrichten festlegen. Sie können das standardmäßige Nachrichtenformat außer Kraft setzen, wie Sie eine bestimmte Nachricht erstellen.

Weitere Informationen zu den Outlook Web App-Einstellungen finden Sie unter [Erstellen und Beantworten von Nachrichten](#).

[Return to top](#)

# Konfigurieren der externen Postmasteradresse in Exchange Online

18.12.2018 • 3 minutes to read

Führen Sie dieses Verfahren aus, um die externe Postmasteradresse Ihres Unternehmens zu ändern. Die externe Postmasteradresse wird als Absender für vom System generierte Nachrichten und Benachrichtigungen verwendet, die an Nachrichtenabsender außerhalb Ihrer Microsoft Exchange Online-Organisation gesendet werden. Ein externer Absender ist jeder Absender mit einer E-Mail-Adresse in einer Domäne, die nicht als akzeptierte Domäne in Ihrer Organisation konfiguriert ist.

Standardmäßig ist der Wert der Einstellung der externen Postmaster-Adresse leer. Dieser Standardwert wird die externe Postmaster-Adresse auf den Wert Postmaster @<Standard akzeptierte Domäne > für Ihre Organisation.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 15 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Transportkonfiguration" im Thema [Mail flow permissions](#).
- Sie können nur Exchange Online PowerShell verwenden, um dieses Verfahren auszuführen. So verwenden Sie Windows PowerShell für die Verbindung zu Exchange Online finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## Verwenden von Exchange Online PowerShell so konfigurieren Sie die externen Postmaster-Adresse

Verwenden Sie folgende Syntax, um die externe Postmasteradresse zu konfigurieren.

```
Set-TransportConfig -ExternalPostmasterAddress <postmaster address>
```

Beispiel für die externe Postmaster-Adresse auf den Wert festlegen `postmaster@contoso.com`, führen Sie den folgenden Befehl

```
Set-TransportConfig -ExternalPostmasterAddress postmaster@contoso.com
```

Um die externe Postmasteradresse auf den Standardwert festzulegen, führen Sie den folgenden Befehl aus:

```
Set-TransportConfig -ExternalPostmasterAddress $null
```

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie folgendermaßen vor, um sicherzustellen, dass Sie die externe Postmasteradresse erfolgreich konfiguriert haben:

1. Führen Sie den folgenden Befehl aus, um den Wert für die externe Postmasteradresse zu überprüfen:

```
Get-TransportConfig | Format-List ExternalPostmasterAddress
```

2. Senden Sie von einem externen E-Mail-Konto eine Nachricht an Ihre Exchange-Organisation, die eine Benachrichtigung über den Zustellungsstatus generieren wird. Um sicherzustellen, dass eine Benachrichtigung über den Zustellungsstatus von Ihrer externen Postmasteradresse gesendet wird, können Sie eine Transportregel zum Senden eines Unzustellbarkeitsberichts (eine Art Benachrichtigung über den Zustellungsstatus) für eine Nachricht von diesem Absender konfigurieren, die spezielle Schlüsselwörter enthält. Stellen Sie sicher, dass die E-Mail-Adresse des Absenders in der Benachrichtigung über den Zustellungsstatus mit der von Ihnen angegebenen externe Postmasteradresse übereinstimmt.

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Verwalten aller Postfächer und des Nachrichtenflusses mithilfe von Office 365

18.12.2018 • 4 minutes to read

**Zusammenfassung:** Informationen zur Verwendung des gehosteten E-Mail-Flusses mit Office 365.

Für die meisten Organisationen wird die Verwendung eines gehosteten Nachrichtenflusses empfohlen, da dies bedeutet, dass Office 365 alle Postfächer verwaltet und filtert. Diese einfache Konfiguration vereinfacht das Einrichten und Verwalten des E-Mail-Flusses.

## Verwalten aller Postfächer und des Nachrichtenflusses mithilfe von Office 365 (empfohlen)

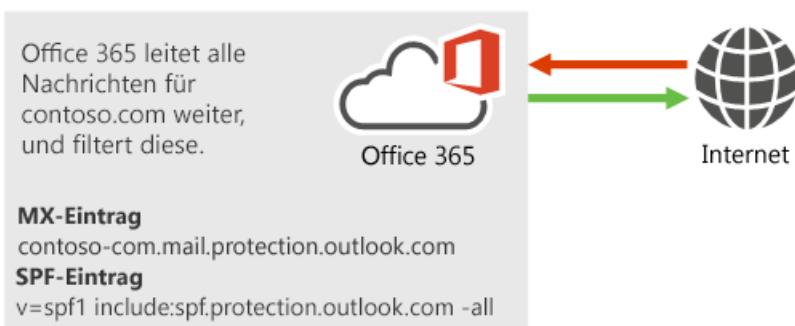
### Gehostete Nachrichtenübermittlungszenarien

- Ich bin ein neuer Office 365-Kunde, und alle meine Benutzerpostfächer befinden sich in Office 365. Ich möchte alle von Office 365 bereitgestellten Filterlösungen verwenden.
- Ich bin ein neuer Office 365-Kunde. Ich verfüge über einen E-Mail-Dienst, möchte jedoch unmittelbar die vorhandenen Benutzerpostfächer in die Cloud verschieben. Ich möchte alle von Office 365 bereitgestellten Filterlösungen verwenden.

In diesem Szenario sieht der Nachrichtenfluss in Ihrer Organisation aus wie im folgenden Diagramm dargestellt:

### Gehosteter Nachrichtenfluss

MX-Eintrag verweist auf Office 365



### Bewährte Methoden für gehostete Nachrichtenflussszenarien

Zum Einrichten des gehosteten Nachrichtenflusses wird empfohlen, den Office 365-Installations-Assistenten zu verwenden. Wechseln Sie zum Aufrufen des Office 365-Installations-Assistenten zu **Setup** im Office 365 Admin Center.

The screenshot shows the 'Office 365 Admin Center' interface. On the left, there's a sidebar with various navigation links like 'DASHBOARD', 'SETUP', 'BENUTZER', etc. The 'SETUP' link is highlighted with a pink box. The main content area has a title 'Setup' with a pink box around it. Below it is a 'Dienstübersicht' (Service Overview) section with tabs for 'Dienststatus' (Service status) and 'Nachrichtencenter' (Message center). Under 'Dienststatus', there are sections for 'Serviceanfragen' (Service requests) and 'E-Mail-Schutz' (Email protection), both showing some problems. To the right, there's a 'Aktueller Status' (Current status) table with several service entries. At the bottom, there's a 'Geplante Wartung' (Planned maintenance) section.

Der Office 365-Installations-Assistent führt Sie durch die folgenden Schritte.

1. Hinzufügen von benutzerdefinierten Domänen in Office 365, und Nachweisen, dass Sie der Eigentümer der Domänen sind, indem Sie die Anweisungen unter [Hinzufügen von Benutzern und Domänen](#) befolgen.
2. [Erstellen von Benutzerpostfächern in Exchange Online](#), oder [Verschieben Sie alle Benutzerpostfächer zu Office 365](#).
3. Aktualisieren der DNS-Einträge für die Domänen, die Sie in Schritt 1 hinzugefügt haben. (Sie sind nicht sicher, wie Sie dies tun? Befolgen Sie die Anweisungen auf [dieser Seite](#).)

Die folgenden DNS-Einträge steuern den Nachrichtenfluss:

- **MX-Eintrag** - Der MX-Eintrag muss im folgenden Format auf Office 365 verweisen: <domainKey>-com.mail.protection.outlook.com.
- Beispiel: Die Domäne contoso.com muss über den folgenden MX-Eintrag verfügen: contoso-com.mail.protection.outlook.com.
- **SPF-Eintrag**: Dies ist ein spezieller TXT-Eintrag im DNS, der zum Identifizieren eines Diensts als gültiger Absender für eine bestimmte Domäne verwendet wird. Da alle Ihre Nachrichten von Office 365 gesendet werden, führen Sie nur Office 365 als gültigen Absender für Ihre Domäne auf. Fügen Sie dazu einen SPF-Eintrag für Ihre Domäne im folgenden Format hinzu:

```
v=spf1 include:spf.protection.outlook.com -all
```

Vollständige Setupanweisungen finden Sie unter [Einrichten von Office 365 Business](#) oder [Bereitstellen von Office 365 Enterprise für Ihre Organisation](#).

## See also

[Bewährte Methoden für die Nachrichtenübermittlung für Exchange Online und Office 365 \(Übersicht\)](#)

[Verwalten des E-Mail-Flusses mithilfe eines Drittanbieter-Clouddiensts mit Office 365](#)

[Verwalten des E-Mail-Flusses mit Postfächern an mehreren Speicherorten \(Office 365 und lokal\)](#)

[Verwalten des Mailflusses mithilfe eines Drittanbieter-Clouddiensts mit Postfächern in Office 365 und lokalen](#)

[Postfächern](#)

[Beheben von Problemen beim Office 365-Nachrichtenfluss](#)

[Testen der Nachrichtenübermittlung durch Überprüfen der Office 365-Connectors](#)

# Verwalten von e-Mail-Fluss von einem Drittanbieter-Clouddienst mit Exchange Online

18.12.2018 • 5 minutes to read

In diesem Thema werden die folgenden komplexen Nachrichtenübermittlungsszenarien mit Exchange Online behandelt:

Szenario 1: MX-Eintrag verweist auf den Spamfilterdienst eines Drittanbieters

Szenario 2: MX-Eintrag verweist auf die Drittanbieterlösung ohne Spamfilterung

## NOTE

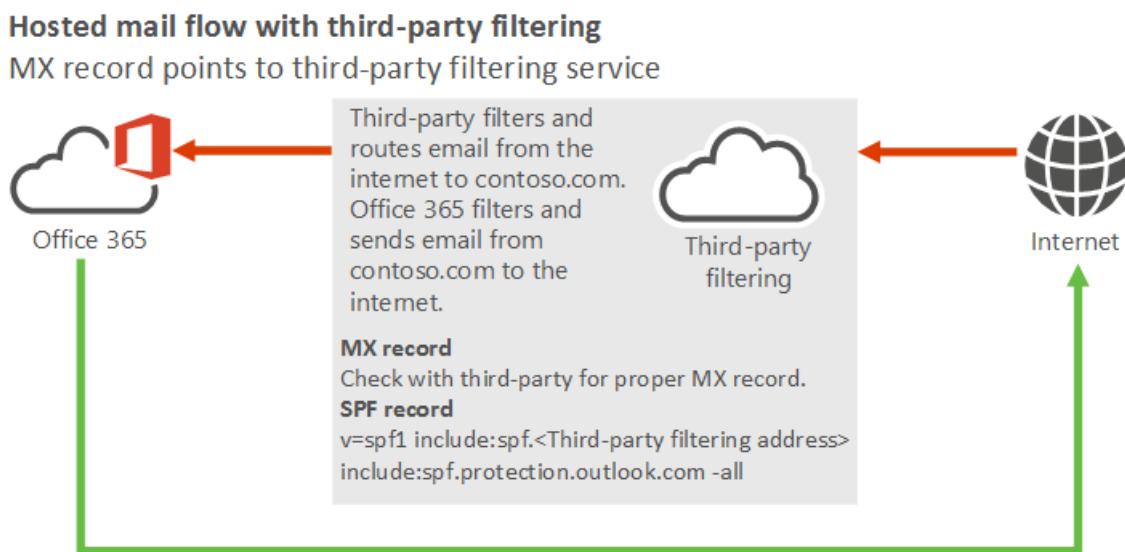
In den in diesem Thema verwendeten Beispielen wird die fiktive Organisation Contoso verwendet, die Eigentümer der folgenden Domäne ist: contoso.com. Die IP-Adresse des Contoso-E-Mail-Servers lautet 131.107.21.231, und der Drittanbieter verwendet 10.10.10.1 als IP-Adresse. Dies sind nur Beispiele. Sie können die Domänennamen und die öffentlichen IP-Adressen in diesen Beispielen entsprechend Ihrer Organisation anpassen.

## Verwenden eines Drittanbieter-Clouddiensts mit Office 365

**Szenario 1: MX-Eintrag verweist auf den Spamfilterdienst eines Drittanbieters**

- Ich werde Exchange Online verwenden zum Hosten von Meine Organisation Postfächer. Meine Organisation verwendet einen Drittanbieter-Clouddienst zum Filtern von Spam und Malware. Alle e-Mails, die im Internet sendet muss nach dieser Drittanbieter-Clouddienst gefiltert werden.

In diesem Szenario sieht der Nachrichtenfluss in Ihrer Organisation aus wie im folgenden Diagramm dargestellt.



## Bewährte Methoden zum Verwenden eines Drittanbieter-Clouddiensts mit Office 365

- Hinzufügen von benutzerdefinierten Domänen in Office 365, und Nachweisen, dass Sie der Eigentümer der Domänen sind, indem Sie die Anweisungen unter [Hinzufügen von Benutzern und Domänen](#) befolgen.
- [Erstellen von Benutzerpostfächern in Exchange Online](#), oder [Verschieben Sie alle Benutzerpostfächer zu Office 365](#).
- Aktualisieren der DNS-Einträge für die Domänen, die Sie in Schritt 1 hinzugefügt haben. (Sie sind nicht

sicher, wie Sie dies tun? Befolgen Sie die Anweisungen auf [dieser Seite](#).) Die folgenden DNS-Einträge steuern den Nachrichtenfluss:

- **MX-Eintrag:** MX-Eintrag für Ihre Domäne muss für Ihren Dienstanbieter Drittanbieter zeigen. Befolgen Sie die Richtlinien zum Konfigurieren des MX-Eintrags für das.
- **SPF-Datensatz:** da Ihre Domäne MX-Eintrag mit dem Drittanbieter-Dienst verweisen muss (mit anderen Worten, Sie erfordern komplexer routing), SPF-Eintrag sollte diese ebenfalls enthalten. Führen Sie die Richtlinien aus dem Drittanbieter-Cloud-Dienst. Sie sollten jedoch auch Office 365 als gültigen Absender hinzufügen.

Beispiel: Wenn contoso.com Ihre Domäne ist, und die IP-Adresse für den Drittanbieter-Clouddienst 10.10.10.1 lautet, sollte der SPF-Eintrag für contoso.com wie folgt aussehen:

```
v=spf1 ip4:10.10.10.1 include:spf.protection.outlook.com -all
```

Alternativ müssen Sie je nach den Anforderungen des Drittanbieters ggf. die Domäne des Drittanbieters hinzufügen, wie im folgenden Beispiel dargestellt:

```
v=spf1 include:spf.protection.outlook.com include:third_party_cloud_service.com -all
```

#### Szenario 2 (nicht unterstützt): MX-Eintrag verweist auf Drittanbieterlösung ohne Filter

- Ich werde Exchange Online verwenden zum Hosten von Meine Organisation Postfächer. Meine Organisation muss alle e-Mails an einen Drittanbieter-Dienst wie Archivierung oder Überwachung senden. Jedoch bereitstellen nicht der Drittanbieter-Dienst eine Spamfilterung Lösung.

Dieses Szenario wird nicht empfohlen und nicht unterstützt, da hier die Office 365-Spamfilterung nicht ordnungsgemäß funktioniert. Wenn Sie sich für dieses Szenario entscheiden, sieht der Nachrichtenfluss in Ihrer Organisation aus wie im folgenden Diagramm dargestellt.



#### Bewährte Methoden zum Verwenden eines Drittanbieter-Clouddiensts mit Office 365

- Verwenden Sie dieses Szenario nicht, da es derzeit nicht unterstützt wird. Es wird empfohlen, Archivierungs- und Überwachungslösungen zu verwenden, die Office 365 bereitstellt.

## Siehe auch

[Bewährte Methoden für die Nachrichtenübermittlung für Exchange Online und Office 365 \(Übersicht\)](#)

[Verwalten aller Postfächer und des Nachrichtenflusses mithilfe von Office 365](#)

Verwalten des E-Mail-Flusses mit Postfächern an mehreren Speicherorten (Office 365 und lokal)

Verwalten von e-Mail-Fluss von einem Drittanbieter-Clouddienst mit Exchange Online und lokalen Postfächern

Beheben von Problemen beim Office 365-Nachrichtenfluss

Testen der Nachrichtenübermittlung durch Überprüfen der Office 365-Connectors

# Verwalten von e-Mail-Fluss mit Postfächern an mehreren Standorten (Exchange Online und lokalen)

18.12.2018 • 22 minutes to read

**Zusammenfassung:** Informationen zum Verwalten des E-Mail-Flusses in einer Exchange-Hybridumgebung mit lokalen Postfächern und Postfächern in Office 365.

Dieses Thema behandelt die folgenden komplexen E-Mail-Flussszenarien mit Office 365:

- [Szenario 1: MX-Eintrag verweist auf Office 365, und Office 365 filtert alle Nachrichten](#)
- [Szenario 2: Der MX-Eintrag verweist auf Office 365, und E-Mails werden lokal gefiltert](#)
- [Szenario 3: MX-Eintrag verweist auf lokale Server](#)
- [Szenario 4: MX-Eintrag verweist auf den lokalen Server, der Ihre Nachrichten filtert und Compliancelösungen bereitstellt. Der lokale Server muss die Nachrichten über Office 365 ins Internet weiterleiten.](#)

## NOTE

Beispiele in diesem Thema verwenden die fiktive Organisation Contoso, das die im Besitz der Domäne "contoso.com" ist. Die IP-Adresse des e-Mail-Servers Contoso ist 131.107.21.231 und seine Drittanbieter 10.10.10.1 für ihre IP-Adresse verwendet. Dies sind nur Beispiele. Sie können in diesen Beispielen gestreckt Domänennamen und öffentliche IP-Adresse Ihres Unternehmens gegebenenfalls anpassen.

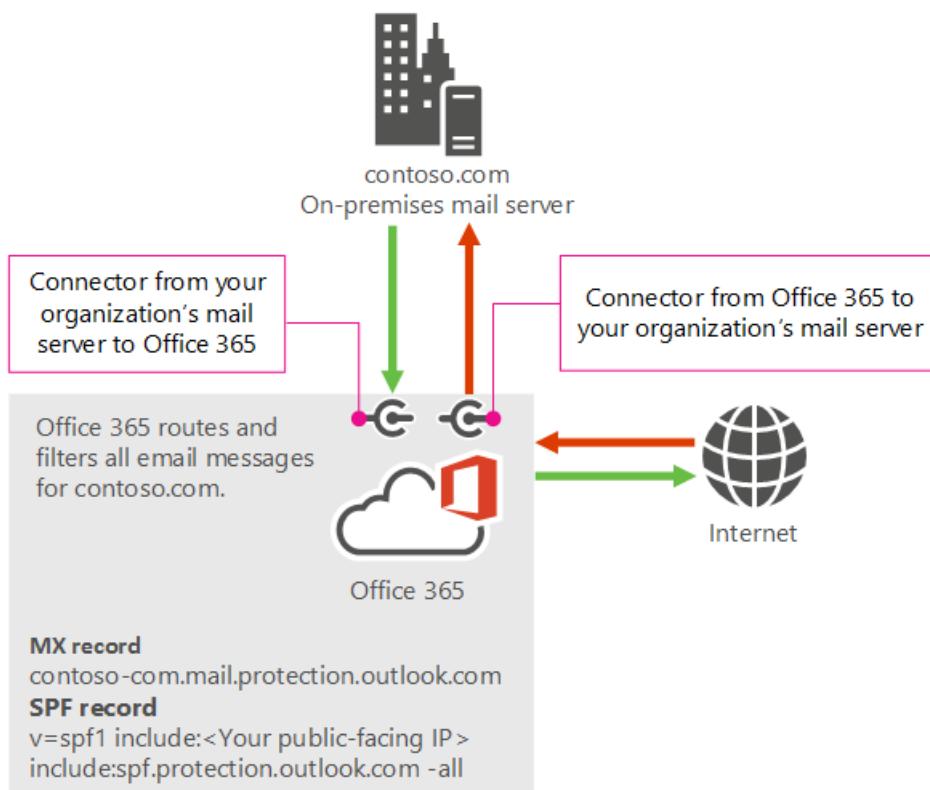
## Verwalten von e-Mail-Fluss, in denen einige Postfächer befinden sich in Office 365 und einige Postfächer befinden sich auf Ihrer Organisation e-Mail-Servern

### Szenario 1: MX-Eintrag verweist auf Office 365, und Office 365 filtert alle Nachrichten

- Ich habe mein Postfächer zu Exchange Online migrieren, und ich Postfächer auf Meine Organisation e-Mail-Server (lokale) gespeichert werden sollen. Ich möchte Verwenden von Office 365 als meine Spamfilterung Lösung und mithilfe von Office 365 Meine Nachrichten vom lokalen Server an das Internet senden möchten. Office 365 sendet und empfängt alle Nachrichten.

Die meisten Kunden, die einen hybriden Nachrichtenfluss einrichten müssen, sollten das Filtern und Routing für Office 365 zulassen. Es wird empfohlen, dass der MX-Eintrag auf Office 365 verweist, da dies die genaueste Spamfilterung bietet. In diesem Szenario sieht der Nachrichtenfluss in Ihrer Organisation aus wie im folgenden Diagramm dargestellt.

## Hybrid mail flow – MX record points to Office 365 and Office 365 filters all messages Filtering happens in Office 365 (Recommended for most hybrid organizations)



### Bewährte Methoden

1. Hinzufügen von benutzerdefinierten Domänen in Office 365, und Nachweisen, dass Sie der Eigentümer der Domänen sind, indem Sie die Anweisungen unter [Hinzufügen von Benutzern und Domänen](#) befolgen.
2. Erstellen von Benutzerpostfächern in Exchange Online , oder [Verschieben Sie alle Benutzerpostfächer zu Office 365](#).
3. Aktualisieren der DNS-Einträge für die Domänen, die Sie in Schritt 1 hinzugefügt haben. (Sie sind nicht sicher, wie Sie dies tun? Befolgen Sie die Anweisungen auf [dieser Seite](#).) Die folgenden DNS-Einträge steuern den Nachrichtenfluss:
  - **MX-Eintrag:** Der MX-Eintrag muss im folgenden Format auf Office 365 verweisen: <domainKey>-com.mail.protection.outlook.com  
Wenn Ihre Domäne z. B. contoso.com ist, muss der MX-Eintrag wie folgt aussehen: contoso-com.mail.protection.outlook.com.
  - **SPF-Datensatz:** Dies sollte Office 365 als gültigen Absender plus alle IP-Adressen von Ihren lokalen Servern, die mit EOP verbunden, und alle dritte Parteien e-Mail senden im Auftrag Ihrer Organisation. Beispielsweise sollte Ihrer Organisation e-Mail-Server Internet-seitige IP 131.107.21.231 Adresse, der SPF-Eintrag für contoso.com sein:

```
v=spf1 ip4:131.107.21.231 include:spf.protection.outlook.com -all
```

Alternativ müssen Sie je nach den Anforderungen des Drittanbieters ggf. die Domäne des Drittanbieters hinzufügen, wie im folgenden Beispiel dargestellt:

```
...
v=spf1 include:spf.protection.outlook.com include:third_party_cloud_service.com -all
...
```

4. Verwenden Sie für die folgenden Szenarien den Connector-Assistenten im Exchange-Verwaltungskonsole zum [Configure mail flow using connectors in Office 365](#):

- Senden von Nachrichten in Office 365 zu Ihrer Organisation e-Mail-Servern
- Senden von E-Mails von Ihren lokalen Servern an Office 365

Wenn eines der folgenden Szenarien auf Ihre Organisation zutrifft, müssen Sie einen Connector erstellen, um das Senden von E-Mails von Ihren lokalen Servern an Office 365 zu unterstützen.

- Ihre Organisation ist im Auftrag Ihres Kunden zum Senden von E-Mails autorisiert, Ihr Organisation gehört die Domäne jedoch nicht. So ist beispielsweise contoso.com autorisiert, E-Mails über fabrikam.com zu senden, die nicht zu contoso.com gehört.
- Ihre Organisation leitet keine Unzustellbarkeitsberichte (auch bekannt als Unzustellbarkeitsberichte oder Springeffekt Nachrichten) mit dem Internet über Office 365.

Wählen Sie die erste Option im Erstellungs-Assistenten für den Connector auf dem Bildschirm **Wie Office 365 E-Mails für Ihren E-Mail-Server identifizieren sollte**, um den Connector zu erstellen.

#### New connector

How should Office 365 identify email from your email server?

- By verifying that the subject name on the certificate that the sending server uses to authenticate with Office 365 matches this domain name (recommended)

Example: contoso.com or \*.contoso.com

- By verifying that the IP address of the sending server matches one of these IP addresses that belong to your organization



This option requires all email messages from your email server to be sent over Transport Layer Security (TLS), a secure channel. Your email server secures this channel by authenticating with Office 365 using a digital certificate. Office 365 then verifies that the subject name in the digital certificate matches the domain name specified here. The domain name can contain wildcard characters. For example contoso.com and \*.contoso.com are both valid. [Learn more](#)

- Office 365 will only accept messages through this connector if the sender domain is configured as an accepted domain for your Office 365 organization. [Learn more](#)

Auf diese Weise kann Office 365 Ihren E-Mail-Server mithilfe des Zertifikats identifizieren. In diesem Szenario enthält der allgemeine Name des Zertifikats oder der alternative Antragstellername die Domäne, die zu Ihrer Organisation gehört. Weitere Informationen finden Sie unter [Identifying email from your email server](#). Details zur Connector-Konfiguration finden Sie unter [Teil 2: Konfigurieren von E-Mails für den Fluss von Ihrem E-Mail-Server zu Office 365](#).

5. In den folgenden Szenarien sind keine Connectors notwendig, solange keine besonderen Anforderungen bei einem Ihrer Partner vorhanden sind, z. B. Erzwingen von TLS mit einer Bank.

- Senden von E-Mails von Office 365 an eine Partnerorganisation
- Senden von E-Mails von einer Partnerorganisation an Office 365

#### NOTE

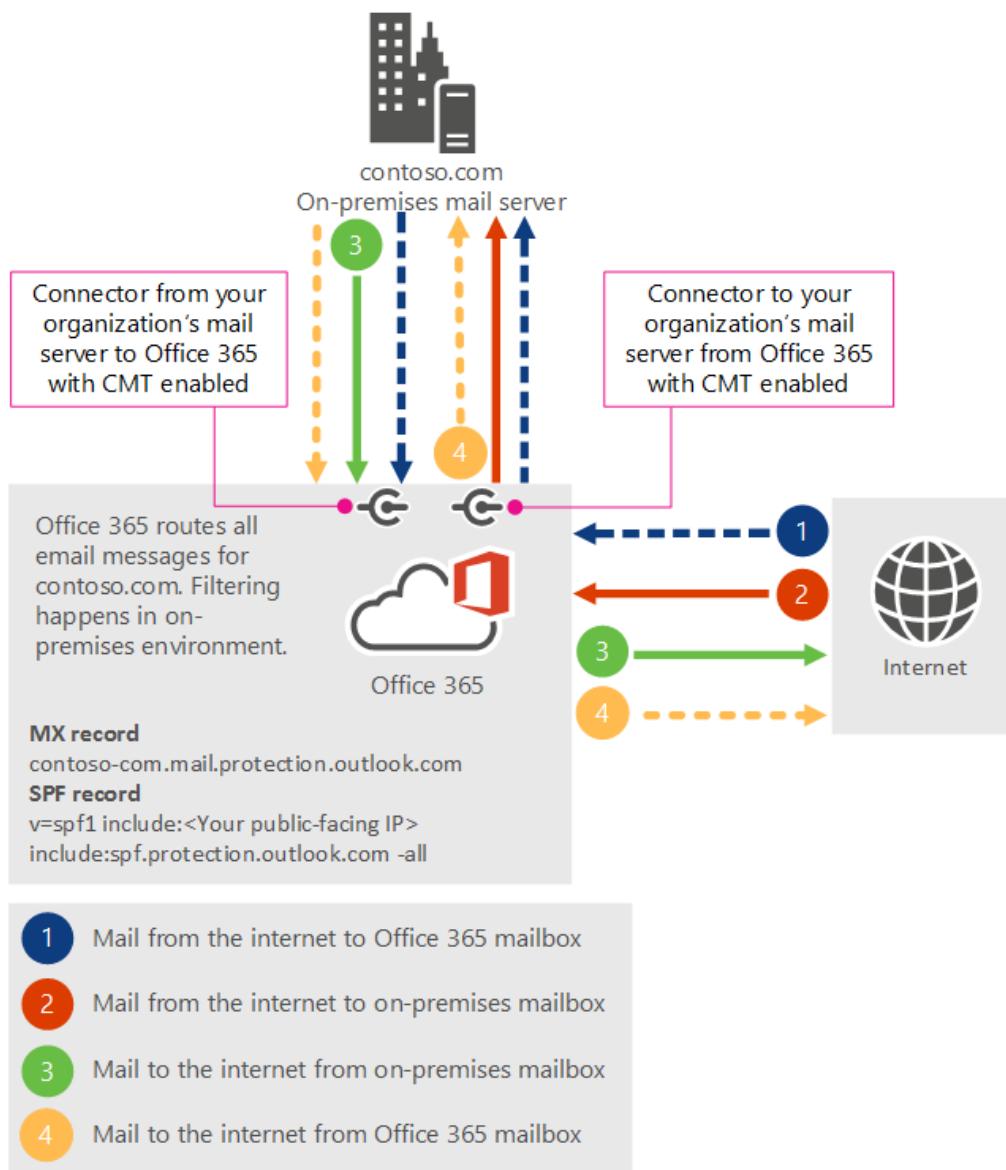
Wenn Ihre Organisation Exchange 2010 verwendet oder höher, wir empfehlen, verwenden Sie den [Hybrid Configuration Wizard](#) Connectors in Office 365 ebenso wie auf den lokalen Exchange-Servern zu konfigurieren. Für dieses Szenario kann nicht MX-Eintrag für Ihre Domäne zu Ihrer Organisation e-Mail-Server zeigen.

#### Szenario 2: Der MX-Eintrag verweist auf Office 365, und E-Mails werden lokal gefiltert

- Ich bin Postfächern zu Exchange Online migrieren, und ich Postfächer auf Meine Organisation e-Mail-Server (lokale) gespeichert werden sollen. Ich möchte die Filterung und Compliance-Lösungen verwenden, die bereits in meiner lokalen Umgebung sind. Alle Nachrichten, die aus dem Internet auf meinen Cloud-Postfächer stammen oder an das Internet gesendete Nachrichten von meinen Cloud-Postfächer müssen über meine lokalen Server weiterleiten.

Wenn Sie aufgrund von geschäftlichen oder rechtlichen Anforderungen E-Mails in Ihrer lokalen Umgebung filtern müssen, wird empfohlen, dass der MX-Eintrag der Domäne auf Office 365 verweist und der zentrale E-Mail-Transport aktiviert ist. Dieses Setup bietet optimale Spamfilterung und schützt die IP-Adressen Ihrer Organisation. In diesem Szenario sieht der Nachrichtenfluss in Ihrer Organisation aus wie im folgenden Diagramm dargestellt.

**Hybrid mail flow – MX record points to Office 365, Centralized Mail Transport is enabled**  
Recommended setup when filtering must happen on-premises for all messages.



1. Hinzufügen von benutzerdefinierten Domänen in Office 365, und Nachweisen, dass Sie der Eigentümer der Domänen sind, indem Sie die Anweisungen unter [Hinzufügen von Benutzern und Domänen](#) befolgen.
  2. [Erstellen von Benutzerpostfächern in Exchange Online](#), oder [Verschieben Sie alle Benutzerpostfächer zu Office 365](#).
  3. Aktualisieren der DNS-Einträge für die Domänen, die Sie in Schritt 1 hinzugefügt haben. (Sie sind nicht sicher, wie Sie dies tun? Befolgen Sie die Anweisungen auf [dieser Seite](#).) Die folgenden DNS-Einträge steuern den Nachrichtenfluss:
- **MX-Eintrag:** Der MX-Eintrag muss im folgenden Format auf Office 365 verweisen: <domainKey>-com.mail.protection.outlook.com

Wenn Ihre Domäne z. B. contoso.comist, muss der MX-Eintrag wie folgt aussehen: contoso-com.mail.protection.outlook.com.

- **SPF-Datensatz:** Dies sollte Office 365 als gültigen Absender plus alle IP-Adressen von Ihren lokalen Servern, die mit EOP verbunden, und alle dritte Parteien e-Mail senden im Auftrag Ihrer Organisation. Beispielsweise sollte Ihrer Organisation e-Mail-Server Internet-seitige IP is131.107.21.231 Adresse, der SPF-Eintrag für contoso.com sein:

```
v=spf1 ip4:131.107.21.231 include:spf.protection.outlook.com -all
```

4. Verwenden Sie den zentralen E-Mail-Transport für lokale Compliancelösungen.
- E-Mail-Nachrichten, die aus dem Internet an ein Postfach im Exchange Online stammt ruft zunächst mit dem lokalen Server gesendet und kommt dann zurück zu Exchange Online an das Postfach übermittelt werden. Zeile 1 steht für diesen Pfad in das Diagramm Szenario 2.
  - Nachrichten kommt von Exchange Online und an das Internet gesendet wird zuerst werden gesendet, um Ihre lokalen Servern, und klicken Sie dann zurückkehrt zu Exchange Online und wird dann an das Internet gesendet. Zeile 4 stellt diesen Pfad in Szenario 2-Diagramm dar.
  - Um diese Konfiguration zu erreichen, Connectors über den [Hybrid Configuration Wizard](#) oder Cmdlets erstellen, und CMT aktivieren. Ausführliche Informationen zu CMT finden Sie unter [Transport Options in Exchange Hybrid Deployments](#).

In den folgenden Szenarien sind keine Connectors notwendig, solange keine besonderen Anforderungen bei einem Ihrer Partner vorhanden sind, z. B. Erzwingen von TLS mit einer Bank.

- Senden von E-Mails von Office 365 an eine Partnerorganisation
- Senden von E-Mails von einer Partnerorganisation an Office 365

### Szenario 3: MX-Eintrag verweist auf lokale Server

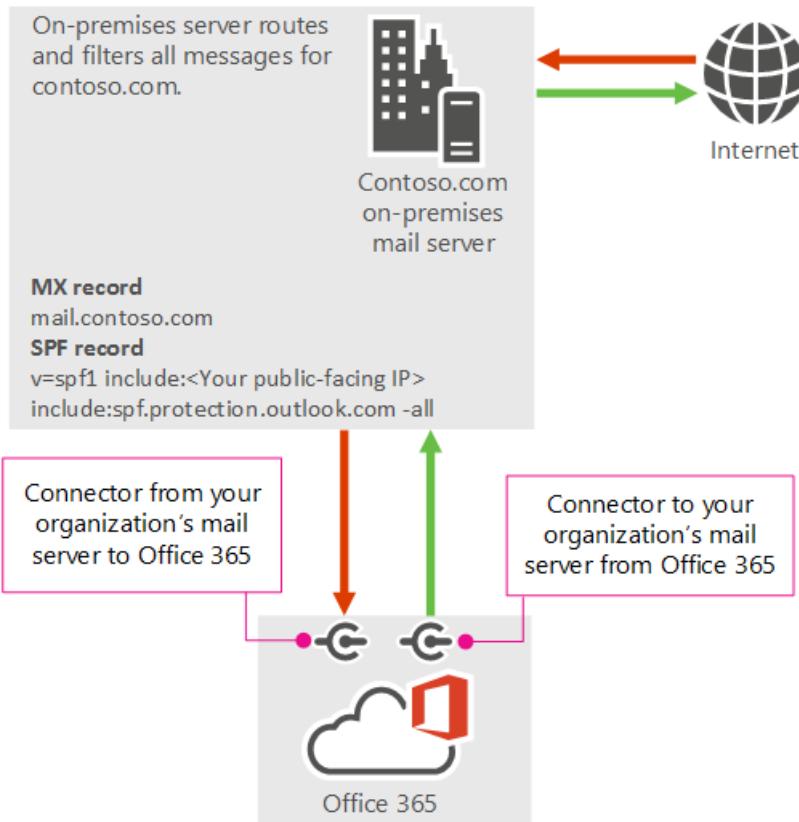
- Ich habe mein Postfächer zu Exchange Online migrieren, und ich Postfächer auf Meine Organisation e-Mail-Server (lokale) gespeichert werden sollen. Ich möchte die Filterung und Compliance-Lösungen verwenden, die bereits in meiner lokalen e-Mail-Umgebung sind. Alle Nachrichten, die aus dem Internet auf meinen Cloud-Postfächer stammen oder an das Internet gesendete Nachrichten von Cloud-Postfächer müssen über meine lokalen Server weiterleiten. Muss ich meine Domäne MX-Eintrag mit dem lokalen Server zu verweisen.

Als Alternative zu Szenario 2 können Sie den MX-Eintrag für Ihre Domäne zu Ihrer Organisation e-Mail-Server und nicht nach Office 365 zeigen. Einige Organisationen ein Unternehmen oder behördliche Notwendigkeit Setup, doch Filtern in der Regel besser funktioniert, wenn Sie Szenario 2 verwenden.

In diesem Szenario sieht der Nachrichtenfluss in Ihrer Organisation aus wie im folgenden Diagramm dargestellt.

## Hybrid mail flow – MX record points to on-premises server

Filtering happens on-premises



### Bewährte Methoden

Verwenden Sie die folgenden bewährten Methoden, wenn der MX-Eintrag für Ihre Domäne auf Ihre lokalen IP-Adresse verweisen muss:

1. Hinzufügen von benutzerdefinierten Domänen in Office 365, und Nachweisen, dass Sie der Eigentümer der Domänen sind, indem Sie die Anweisungen unter [Hinzufügen von Benutzern und Domänen](#) befolgen.
2. [Erstellen von Benutzerpostfächern in Exchange Online](#), oder [Verschieben Sie alle Benutzerpostfächer zu Office 365](#).
3. Aktualisieren der DNS-Einträge für die Domänen, die Sie in Schritt 1 hinzugefügt haben. (Sie sind nicht sicher, wie Sie dies tun? Befolgen Sie die Anweisungen auf [dieser Seite](#).) Die folgenden DNS-Einträge steuern den Nachrichtenfluss:
  - **SPF-Datensatz:** sollten diese Office 365 als gültigen Absender aufgeführt. Darüber sollte hinaus enthalten alle IP-Adressen von Ihren lokalen Servern, die mit EOP verbunden und dritten, die Senden von e-Mails im Namen Ihrer Organisation. Beispielsweise sollte Ihrer Organisation e-Mail-Server Internet-seitige IP `is131.107.21.231` Adresse, der SPF-Eintrag für contoso.com sein:

```
v=spf1 ip4:131.107.21.231 include:spf.protection.outlook.com -all
```

4. Da Sie keine Nachrichten von Ihren lokalen Servern an das Internet über Office 365 übertragen, müssen Sie aus technischer Sicht keine Connectors für die folgenden Szenarien erstellen. Wenn Sie aber zu irgendeinem Zeitpunkt Ihren MX-Eintrag so ändern, dass er auf Office 365 verweist, müssen Sie Connectors erstellen, es bietet sich daher an, dies gleich vorab zu tun. Verwenden Sie für die folgenden Szenarien den Connector-Assistenten im Exchange-Verwaltungskonsole zum [Teil 2: Konfigurieren von E-Mails für den Fluss von Ihrem E-Mail-Server zu Office 365](#), oder verwenden Sie den [Hybrid Configuration Wizard](#), um Connectors zu erstellen.

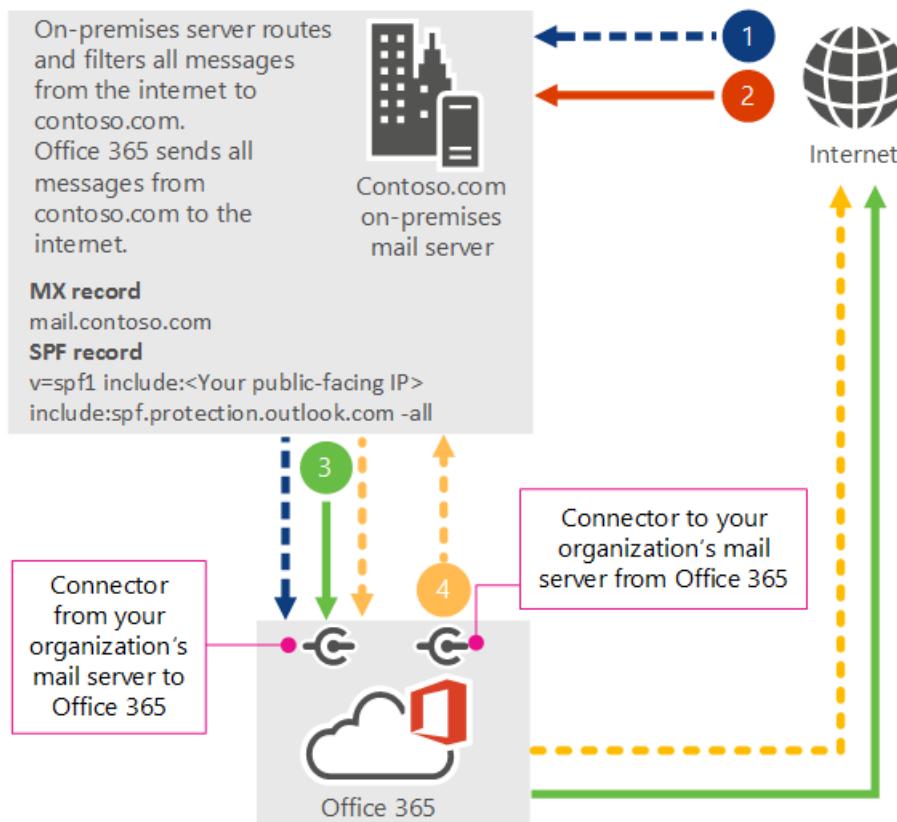
- Senden von e-Mail in Office 365 zu Ihrer Organisation e-Mail-Servern
  - Senden von E-Mails von Ihren lokalen Servern an Office 365
5. Um sicherzustellen, dass Nachrichten an die lokalen Server der Organisation über MX gesendet werden, gehen Sie zu [Auf von einer Partnerorganisation gesendete E-Mails anwendbare Beispielsicherheitseinschränkungen](#), und befolgen Sie „Beispiel 3: Sämtliche von der Domäne „ContosoBank.com“ Ihrer Partnerorganisation stammenden E-Mails sollen über einen bestimmten IP-Adressbereich gesendet werden.“

**Szenario 4: MX-Eintrag verweist auf den lokalen Server, der Ihre Nachrichten filtert und Compliance-Lösungen bereitstellt. Der lokale Server muss die Nachrichten über Office 365 ins Internet weiterleiten.**

- Ich habe mein Postfächer zu Exchange Online migriert, und ich Postfächer auf Meine Organisation e-Mail-Server (lokale) gespeichert werden sollen. Ich möchte die Filterung und Compliance-Lösungen verwenden, die bereits in meiner lokalen e-Mail-Umgebung sind. Alle Nachrichten von Meine lokalen Server müssen über Office 365 mit dem Internet erlaubt. Muss ich meine Domäne MX-Eintrag mit dem lokalen Server zu verweisen.

In diesem Szenario sieht der Nachrichtenfluss in Ihrer Organisation aus wie im folgenden Diagramm dargestellt.

**Hybrid mail flow – MX record points to on-premises server**  
Filtering happens on-premises, Office 365 sends messages to the internet



- 1 Mail from the internet to Office 365 mailbox
- 2 Mail from the internet to on-premises mailbox
- 3 Mail to the internet from on-premises mailbox
- 4 Mail to your organization's mail server and to the internet from Office 365 mailbox

**Bewährte Methoden**

Verwenden Sie die folgenden bewährten Methoden, wenn der MX-Eintrag für Ihre Domäne auf Ihre lokalen IP-Adresse verweisen muss:

1. Hinzufügen von benutzerdefinierten Domänen in Office 365, und Nachweisen, dass Sie der Eigentümer der Domänen sind, indem Sie die Anweisungen unter [Hinzufügen von Benutzern und Domänen](#) befolgen.
2. [Erstellen von Benutzerpostfächern in Exchange Online](#), oder [Verschieben Sie alle Benutzerpostfächer zu Office 365](#).
3. Aktualisieren der DNS-Einträge für die Domänen, die Sie in Schritt 1 hinzugefügt haben. (Sie sind nicht sicher, wie Sie dies tun? Befolgen Sie die Anweisungen auf [dieser Seite](#).) Die folgenden DNS-Einträge steuern den Nachrichtenfluss:

- **MX-Eintrag:** Der MX-Eintrag muss im folgenden Format auf Ihren lokalen Server verweisen: mail.<domainKey>.com

Wenn Ihre Domäne z. B. contoso.comist, muss der MX-Eintrag wie folgt aussehen: .mail.contoso.com.

- **SPF-Datensatz:** sollten diese Office 365 als gültigen Absender aufgeführt. Darüber sollte hinaus enthalten alle IP-Adressen von Ihren lokalen Servern, die mit EOP verbunden und dritten, die Senden von e-Mails im Namen Ihrer Organisation. Beispielsweise sollte Ihrer Organisation e-Mail-Server mit Internetzugriff IP-Adresse 131.107.21.231 ist, der SPF-Eintrag für contoso.com sein:

```
v=spf1 ip4:131.107.21.231 include:spf.protection.outlook.com -all
```

4. Verwenden Sie für die folgenden Szenarien den Connector-Assistenten im Exchange-Verwaltungskonsole zum [Configure mail flow using connectors in Office 365](#):

- Senden von e-Mail in Office 365 zu Ihrer Organisation e-Mail-Servern
- Senden von E-Mails von Ihren lokalen Servern an Office 365

Sie müssen einen Connector erstellen, um das Senden von E-Mails von Ihren lokalen Servern an Office 365 zu unterstützen, wenn eines der folgenden Szenarien auf Ihre Organisation zutrifft:

- Ihre Organisation ist im Auftrag Ihres Kunden zum Senden von E-Mails autorisiert, Ihrer Organisation gehört die Domäne jedoch nicht. So ist beispielsweise contoso.com autorisiert, E-Mails über fabrikam.com zu senden, die nicht zu contoso.com gehört.
- Ihre Organisation leitet Unzustellbarkeitsberichte (NDR) mit dem Internet über Office 365.
- Der MX-Datensatz Ihrer Domäne (contoso.com) zeigt auf Ihren lokalen Server. Benutzer in Ihrer Organisation leiten Nachrichten automatisch an E-Mail-Adressen weiter, die sich außerhalb Ihrer Organisation befinden. So hat beispielsweise kate@contoso.com die Weiterleitung aktiviert, und alle Nachrichten werden an kate@tailspintoys.com weitergeleitet. Wenn john@fabrikam.com eine Nachricht an kate@contoso.com sendet, lauten zum Zeitpunkt, wenn die Nachricht bei Office 365 ankommt, die Absenderdomäne fabrikam.com und die Empfängerdomäne tailspin.com. Weder die Absender- noch die Empfängerdomäne gehört zu Ihrer Organisation.

Wählen Sie die erste Option im Erstellungs-Assistenten für den Connector auf dem Bildschirm **Wie Office 365 E-Mails für Ihren E-Mail-Server identifizieren sollte**, um den Connector zu erstellen.

## New connector

How should Office 365 identify email from your email server?

- By verifying that the subject name on the certificate that the sending server uses to authenticate with Office 365 matches this domain name (recommended)

Example: contoso.com or \*.contoso.com

- By verifying that the IP address of the sending server matches one of these IP addresses that belong to your organization



This option requires all email messages from your email server to be sent over Transport Layer Security (TLS), a secure channel. Your email server secures this channel by authenticating with Office 365 using a digital certificate. Office 365 then verifies that the subject name in the digital certificate matches the domain name specified here. The domain name can contain wildcard characters. For example contoso.com and \*.contoso.com are both valid. [Learn more](#)

Office 365 will only accept messages through this connector if the sender domain is configured as an accepted domain for your Office 365 organization. [Learn more](#)

Auf diese Weise kann Office 365 Ihren E-Mail-Server mithilfe des Zertifikats identifizieren. In diesem Szenario enthält der allgemeine Name des Zertifikats oder der alternative Antragstellername die Domäne, die zu Ihrer Organisation gehört. Weitere Informationen finden Sie unter [Identifying email from your email server](#). Details zur Connector-Konfiguration finden Sie unter [Teil 2: Konfigurieren von E-Mails für den Fluss von Ihrem E-Mail-Server zu Office 365](#).

5. [Einrichten von Connectors für den sicheren Nachrichtenfluss mit einer Partnerorganisation](#), um sicherzustellen, dass Nachrichten an die lokalen Server Ihrer Organisation über MX gesendet werden.

## See also

[Bewährte Methoden für die Nachrichtenübermittlung für Exchange Online und Office 365 \(Übersicht\)](#)

[Verwalten aller Postfächer und des Nachrichtenflusses mithilfe von Office 365](#)

[Verwalten des E-Mail-Flusses mithilfe eines Drittanbieter-Clouddiensts mit Office 365](#)

[Verwalten des Mailflusses mithilfe eines Drittanbieter-Clouddiensts mit Postfächern in Office 365 und lokalen Postfächern](#)

[Beheben von Problemen beim Office 365-Nachrichtenfluss](#)

[Testen der Nachrichtenübermittlung durch Überprüfen der Office 365-Connectors](#)

# Verwalten von e-Mail-Fluss von einem Drittanbieter-Clouddienst mit Exchange Online und lokalen Postfächern

18.12.2018 • 3 minutes to read

Dieses Thema behandelt die komplexesten E-Mail-Flussszenarien mit Office 365.

## NOTE

Beispielecontoso.com. Die IP-Adresse des Contoso-E-Mail-Servers lautet 131.107.21.231, und der Drittanbieter verwendet 10.10.10.1 als IP-Adresse. Dies sind nur Beispiele. Sie können die Domänennamen und die öffentlichen IP-Adressen in diesen Beispielen entsprechend Ihrer Organisation anpassen.

## Verwenden eines Drittanbieter-Cloud-Diensts mit Postfächern in Exchange Online und auf Meine Organisation e-Mail-Servern

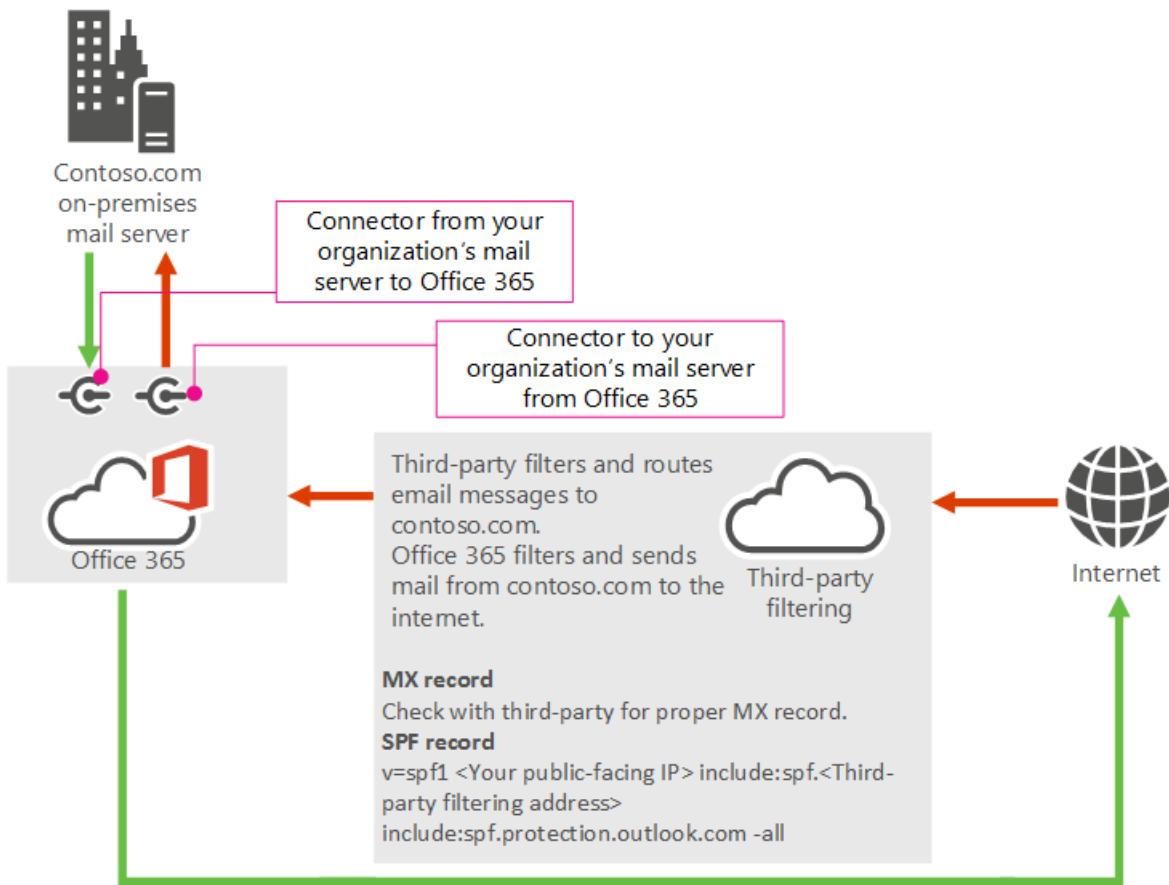
### Szenario

- Ich habe mein Postfächer zu Exchange Online migrieren, und ich einige Postfächer in der Organisation lokalen e-Mail-Server gespeichert werden sollen. Ich möchte einen Drittanbieter-Cloud-Dienst verwenden, um Spam über das Internet zu filtern. Meine Nachrichten an das Internet müssen über Office 365, um zu verhindern, dass meine lokalen-Server-IP-Adressen zu externen Sperrlisten hinzugefügten weiterleiten.

In diesem Szenario sieht der Nachrichtenfluss in Ihrer Organisation aus wie im folgenden Diagramm dargestellt.

## Hybrid mail flow with third-party filtering

MX record points to third-party filtering service



### Bewährte Methoden

1. Hinzufügen von benutzerdefinierten Domänen in Office 365, und Nachweisen, dass Sie der Eigentümer der Domänen sind, indem Sie die Anweisungen unter [Hinzufügen von Benutzern und Domänen](#) befolgen.
2. [Erstellen von Benutzerpostfächern in Exchange Online](#), oder [Verschieben Sie alle Benutzerpostfächer zu Office 365](#).
3. Aktualisieren der DNS-Einträge für die Domänen, die Sie in Schritt 1 hinzugefügt haben. (Sie sind nicht sicher, wie Sie dies tun? Befolgen Sie die Anweisungen auf [dieser Seite](#).) Die folgenden DNS-Einträge steuern den Nachrichtenfluss:
  - **MX-Eintrag:** Zeigen Sie Ihren MX-Eintrag mit dem Drittanbieter-Dienst. Befolgen Sie die Richtlinien für das Konfigurieren des MX-Eintrags.
  - **SPF-Datensatz:** da Ihre Domäne MX-Eintrag mit einem Drittanbieter-Dienst verweisen muss (mit anderen Worten, Sie erfordern komplexer routing), schließen Sie den Drittanbieter-Dienst in Ihres SPF-Eintrags. Befolgen Sie die Drittanbieter-Richtlinien für Ihre SPF-Eintrag hinzugefügt. Office 365 und die IP-Adressen der lokale Server werden auch als gültigen Absender hinzufügen. Angenommen, wenn "contoso.com" der Domänenname ist, die Drittanbieter-Cloud-Dienst-IP-Adresse 10.10.10.1 ist und Ihre lokalen Server IP-Adresse 131.107.21.231 ist, sollte der SPF-Eintrag für contoso.com sein:

```
v=spf1 ip4:10.10.10.1 ip4:131.107.21.231 include:spf.protection.outlook.com -all
```

Alternativ müssen Sie je nach den Anforderungen des Drittanbieters ggf. die Domäne des Drittanbieters hinzufügen, wie im folgenden Beispiel dargestellt:

```
v=spf1 ip4:131.107.21.231 include:spf.protection.outlook.com include:third_party_cloud_service.com -all
```

## See also

[Bewährte Methoden für die Nachrichtenübermittlung für Exchange Online und Office 365 \(Übersicht\)](#)

[Verwalten aller Postfächer und des Nachrichtenflusses mithilfe von Office 365](#)

[Verwalten des E-Mail-Flusses mithilfe eines Drittanbieter-Clouddiensts mit Office 365](#)

[Verwalten des E-Mail-Flusses mit Postfächern an mehreren Speicherorten \(Office 365 und lokal\)](#)

[Beheben von Problemen beim Office 365-Nachrichtenfluss](#)

[Testen der Nachrichtenübermittlung durch Überprüfen der Office 365-Connectors](#)

# Einrichten eines Multifunktionsgeräts oder einer Anwendung zum Senden von E-Mails mithilfe von Office 365

18.12.2018 • 32 minutes to read

[] Voraussetzungen: Office 365-Abonnement, [Exchange Online-Pläne](#)

Aus dem 1. September 2018 ist Office 365 langsam, Änderungen auf SMTP-Client-Übermittlung (auch bekannt als SMTP-authentifiziert Übermittlung) parallelen die Ihrer Geräte und Anwendungen, die e-Mails senden beeinträchtigen können. Besuchen Sie, um weitere Informationen finden Sie im KB-Artikel [Verbesserungen bei der authentifizierte SMTP-Übermittlung Clientprotokoll](#) aus.

In diesem Artikel wird erläutert, wie Sie E-Mails von Geräten und Geschäftsanwendungen senden können, wenn sich alle Ihre Postfächer in Office 365 befinden. Beispiel:

- Sie verfügen über einen Scanner und möchten gescannte Dokumenten per E-Mail an sich selbst oder eine andere Person senden.
- Sie verfügen über eine LOB-Anwendung (Branchenanwendung), die Termine verwaltet, und Sie möchten Terminerinnerungen per E-Mail an Kunden senden.

## NOTE

Ab dem 1. September 2018 ist Office 365 langsam, Änderungen auf SMTP-Client-Übermittlung (auch bekannt als SMTP-authentifiziert-Übermittlung) parallelen die Ihrer Geräte und Anwendungen, die e-Mails senden beeinträchtigen können. Weitere Informationen finden Sie im KB-Artikel [Verbesserungen an der Clientprotokoll authentifiziert SMTP-Übermittlung](#).

**Option 1 (empfohlen): Authentifizieren Sie das Gerät oder die Anwendung direkt mit einem Office 365-Postfach, und senden Sie E-Mails mithilfe der SMTP-Clientübermittlung.**

Diese Option unterstützt die meisten Nutzungsszenarien und kann am einfachsten eingerichtet werden. Wählen Sie diese Option für Folgendes aus:

- Sie möchten E-Mails von einer Anwendung, einem Dienst oder einem Gerät senden, die/der/das von einem Drittanbieter gehostet wird.
- Sie möchten E-Mails an Personen innerhalb und außerhalb Ihres Unternehmens senden.

Zum Konfigurieren Ihres Geräts oder der Anwendung stellen Sie mithilfe des Endpunkts für die SMTP-Clientübermittlung **smtp.office365.com** eine direkte Verbindung mit Office 365 her.

Jedes Gerät-Anwendung muss mit Office 365 zu authentifizieren. Die e-Mail-Adresse des Kontos, das zur Authentifizierung mit Office 365 verwendet wird, wird als Absender der Nachrichten aus der Geräte-Anwendung angezeigt.

## Einrichten der SMTP-Clientübermittlung

Geben Sie die folgenden Einstellungen **gemäß der Anweisung im Leitfaden** direkt auf Ihrem Gerät oder in der Anwendung ein (möglicherweise wird eine andere Terminologie als in diesem Artikel verwendet). Solange Ihr

Szenario die Anforderungen für die SMTP-Clientübermittlung erfüllt, ermöglichen es Ihnen die folgenden Einstellungen, E-Mails von Ihrem Gerät oder aus der Anwendung zu senden.

EINSTELLUNG FÜR GERÄT ODER ANWENDUNG	WERT
Server/Smarthost	SMTP.Office365.com
Port	Port 587 (empfohlen) oder Port 25
TLS/StartTLS	Aktiviert
Benutzername/E-Mail-Adresse und Kennwort	Geben Sie die Anmeldeinformationen für das verwendete gehostete Postfach ein

Erweitern Sie die folgenden Abschnitte, um weitere Informationen zu erhalten.

#### **TLS und andere Verschlüsselungsoptionen**

Ermitteln Sie, welche TLS-Version Ihr Gerät unterstützt, indem Sie das Handbuch des Geräts überprüfen oder den Anbieter fragen. Wenn Ihr Gerät oder die Anwendung TLS 1.0 oder höher nicht unterstützt:

- Verwenden Sie stattdessen das direkte Senden (Option 2) oder Office 365 SMTP-Relay (Option 3) zum Senden von Nachrichten (je nach Ihren Anforderungen).
- Wenn es zwingend erforderlich ist, die SMTP-Clientübermittlung zu verwenden, und Ihr Drucker nur SSL 3.0 unterstützt, können Sie eine alternative Konfiguration einrichten, die als "indirekte SMTP-Clientübermittlung" bezeichnet wird. Dabei wird ein lokaler SMTP-Relayserver verwendet, um die Verbindung mit Office 365 herzustellen. Diese Einrichtung ist wesentlich komplexer. Anweisungen finden Sie hier: [Konfigurieren von IIS für Relay mit Office 365](#).

#### **NOTE**

Wenn Ihr Gerät Port 465 empfiehlt oder standardmäßig verwendet, unterstützt es keine SMTP-Clientübermittlung.

#### **Funktionsweise der SMTP-Clientübermittlung**

Das folgende Diagramm bietet eine konzeptionelle Übersicht über das Aussehen Ihrer Umgebung.



#### **Features der SMTP-Clientübermittlung**

- Die SMTP-Clientübermittlung gestattet es Ihnen, E-Mails an Personen in Ihrem Unternehmen sowie an externe Personen zu senden.
- Bei dieser Methode werden die meisten Prüfungen auf Spam für E-Mails umgangen, die an Personen in Ihrem Unternehmen gesendet wurden. Dies kann dabei helfen, dass die IP-Adressen Ihres Unternehmens davor geschützt sind, von einer Spam-Liste blockiert zu werden.
- Mit dieser Methode können Sie E-Mails von einem beliebigen Ort oder von einer beliebigen IP-Adresse senden, einschließlich des Netzwerks in Ihrem Unternehmen (lokal) oder eines Cloud-Hostingdiensts eines Drittanbieters, z. B. Microsoft Azure.

#### **Anforderungen für die SMTP-Clientübermittlung**

- **Authentifizierung:** Sie müssen möglicherweise einen Benutzernamen und das Kennwort zum Senden von e-Mail auf dem Gerät zu konfigurieren.
- **Mailbox:** benötigen Sie eine lizenzierte Office 365-Postfach senden von E-Mails aus.
- **Transport Layer Security (TLS):** das Gerät muss in der Lage, für TLS verwenden Sie Version 1.0 und

höher sein.

- **Port:** Port 587 (empfohlen) oder Port 25 ist erforderlich und muss nicht mehr in Ihrem Netzwerk blockiert werden. Einige Netzwerk-Firewalls oder Internetdienstanbieter blockieren Ports – insbesondere port 25.

#### NOTE

Weitere Informationen zu TLS finden Sie unter [So sichert Exchange Online mithilfe von TLS E-Mail-Verbindungen in Office 365](#). Ausführliche technische Informationen dazu, wie TLS von Exchange Online mit Verschlüsselungssammlungsreihenfolge verwendet wird, finden Sie unter [Verbessern der Nachrichtenflusssicherheit für Exchange Online](#).

#### Einschränkungen der SMTP-Clientübermittlung

Sie können nur von einer E-Mail-Adresse senden, es sei denn, Ihr Gerät kann Anmeldeinformationen für mehrere Office 365-Postfächer speichern. Office 365 legt einen Grenzwert von 30 Nachrichten pro Minute sowie von 10.000 Empfängern pro Tag fest.

## Option 2: Direktes Senden von E-Mails von einem Drucker oder einer Anwendung an Office 365

Wählen Sie diese Option für Folgendes aus:

- Die SMTP-Clientübermittlung (Option 1) ist mit Ihren Geschäftsanforderungen oder mit Ihrem Gerät nicht kompatibel. Beispielsweise, wenn Ihr Gerät oder die Anwendung die Anforderungen der SMTP-Clientübermittlung nicht erfüllt, z. B. die Unterstützung von TLS.
- Sie müssen Nachrichten nur an Empfänger im eigenen Unternehmen senden, die über Postfächer in Office 365 verfügen. Sie müssen keine E-Mails an externe Empfänger senden.

Andere Szenarien, für die das direkte Senden möglicherweise die beste Wahl darstellt:

- Sie möchten, dass das Gerät oder die Anwendung über die E-Mail-Adresse der einzelnen Benutzer sendet und möchten nicht, dass die Anmeldeinformationen für das Postfach der einzelnen Benutzer für die Verwendung der SMTP-Clientübermittlung konfiguriert wird. Das direkte Senden gestattet es den einzelnen Benutzern in Ihrem Unternehmen, die E-Mails über ihre eigene Adresse zu senden.

Vermeiden Sie die Verwendung eines einzelnen Postfachs mit der Berechtigung "Senden als" für alle Benutzer. Diese Methode wird aufgrund der Komplexität und potenziellen Probleme nicht unterstützt.

- Sie möchten massenweise E-Mails oder Newsletter senden. Office 365 gestattet es Ihnen nicht, dies über die SMTP-Clientübermittlung vorzunehmen. Das direkte Senden ermöglicht es Ihnen, eine große Anzahl von Nachrichten zu senden.

Beachten Sie, dass das Risiko besteht, dass Ihre E-Mails von Office 365 als Spam gekennzeichnet werden. Sie sollten möglicherweise die Unterstützung eines Anbieters von Massen-E-Mails anfordern. Diese können Ihnen z. B. dabei helfen, die bewährten Methoden zu beachten und somit sicherstellen, dass Ihre Domänen und IP-Adressen nicht von anderen im Internet blockiert werden.

#### Einstellungen für das direkte Senden

Geben Sie die folgenden Einstellungen direkt auf dem Gerät oder in der Anwendung ein.

EINSTELLUNG FÜR GERÄT ODER ANWENDUNG	WERT
Server/Smarthost	Ihr MX-Endpunkt z. B. contoso-com.mail.protection.outlook.com

EINSTELLUNG FÜR GERÄT ODER ANWENDUNG	WERT
Port	Port 25
TLS/StartTLS	Aktiviert
E-Mail-Adresse	Eine beliebige E-Mail-Adresse für eine Ihrer akzeptierten Office 365-Domänen. Diese E-Mail-Adresse erfordert kein Postfach.

Es wird empfohlen, einen SPF-Eintrag hinzuzufügen, um zu verhindern, dass Nachrichten als Spam gekennzeichnet werden. Wenn Sie über eine statische IP-Adresse senden, fügen Sie diese zu Ihrem SPF-Eintrag in den DNS-Einstellungen Ihrer Domänenregistrierungsstelle wie folgt hinzu:

DNS-EINTRAG	WERT
SPF	v=spf1 ip4:<Static IP Address> include:spf.protection.outlook.com ~all

### Schrittweise Anleitungen zum direkten Senden

1. Wenn Ihr Gerät oder die Anwendung über eine statische öffentliche IP-Adresse senden kann, ermitteln Sie diese IP-Adresse und notieren Sie sie. Sie können Ihre statische IP-Adresse mit anderen Geräten und Benutzern teilen, aber nicht für Personen außerhalb Ihres Unternehmens freigeben. Ihr Gerät oder die Anwendung kann über eine dynamische oder freigegebene IP-Adresse senden, aber die Nachrichten sind dann anfälliger für Antispamfilter.
2. [Melden Sie sich bei Office 365 an.](#)
3. Stellen Sie sicher, dass Ihre Domäne, z. B. "contoso.com", aktiviert ist. Klicken Sie auf **DNS verwalten**, und suchen Sie den MX-Eintrag. Der MX-Eintrag verfügt über den Wert **VERWEIST AUF DIE ADRESSE**, der "cohowneinc-com.mail.protection.outlook.com" ähnlich ist, wie im folgenden Screenshot veranschaulicht. Notieren Sie den Wert für **VERWEIST AUF DIE ADRESSE** des MX-Eintrags, auf den wir uns als Ihren MX-Endpunkt beziehen.
4. Wechseln Sie wieder zum Gerät, und geben Sie in den Einstellungen unter der Option, die normalerweise als **Server** oder **Smarthost** bezeichnet wird, den Wert für **VERWEIST AUF DIE ADRESSE** des MX-Eintrags ein, den Sie in Schritt 3 aufgezeichnet haben.
5. Nachdem Sie die Konfiguration Ihrer Geräteeinstellungen abgeschlossen haben, wechseln Sie zur Website der Domänenregistrierungsstelle, um Ihre DNS-Einträge zu aktualisieren. Bearbeiten Sie Ihren SPF-Eintrag (Sender Policy Framework). Beziehen Sie in den Eintrag die IP-Adresse ein, die Sie sich in Schritt 1 notiert haben. Die fertige Zeichenfolge ähnelt dem Folgenden:

```
v=spf1 ip4:10.5.3.2 include:spf.protection.outlook.com ~all
```

Dabei gibt "10.5.3.2" Ihrer öffentlichen IP-Adresse an.

#### NOTE

Wenn Sie diesen Schritt überspringen, kann dies dazu führen, dass die E-Mails in die Ordner für Junk-E-Mails des Empfängers gesendet werden.

6. Senden Sie zum Testen der Konfiguration eine Test-E-Mail von Ihrem Gerät oder der Anwendung, und

bestätigen Sie, dass der Empfänger sie erhalten hat.

## So funktioniert das direkte Senden

Im folgenden Diagramm verwendet die Anwendung oder das Gerät im Netzwerk Ihres Unternehmens das direkte Senden und den Office 365-MX-Endpunkt, um E-Mails an Empfänger in Ihrem Unternehmen zu senden. Sie können den MX-Endpunkt einfach in Office 365 finden, wenn Sie diesen ermitteln müssen.

Sie können das Gerät so konfigurieren, dass E-Mails direkt an Office 365 gesendet werden. Verwenden Sie das direkte Senden, um E-Mails per Relay an Empfänger mit Office 365-Postfächern in Ihrer Organisation weiterzuleiten. Das direkte Senden funktioniert auch bei externen Empfängern mit Postfächern in Office 365. Wenn Ihr Gerät das direkte Senden verwendet, um eine E-Mail per Relay an einen Empfänger weiterzuleiten, der kein Office 365-Postfach besitzt, wird die E-Mail zurückgewiesen.

### NOTE

Wenn Ihr Gerät oder die Anwendung über die Möglichkeit verfügt, als E-Mail-Server zu fungieren und an Office 365 sowie an andere E-Mail-Provider zu übermitteln, ziehen Sie die Anleitung des Geräts oder der Anwendung zurate. Es sind für dieses Szenario keine Office 365-Einstellungen erforderlich.

## Features für das direkte Senden

- Verwendet Office 365 zum Senden von E-Mails, aber erfordert kein dediziertes Office 365-Postfach.
- Erfordert keine statische IP-Adresse für das Gerät oder die Anwendung. Dies wird nach Möglichkeit aber empfohlen.
- Funktioniert nicht mit einem Verbinden. Konfigurieren Sie für ein Gerät niemals die Verwendung eines Verbinders für das direkte Senden, da dies zu Problemen führen kann.
- Erfordert von Ihrem Gerät nicht die Unterstützung von TLS.

Das direkte Senden weist höhere Sendegrenzwerte als die SMTP-Clientübermittlung auf. Absender sind nicht an den Grenzwert von 30 Nachrichten pro Minute oder 10.000 Empfänger pro Tag gebunden.

## Anforderungen für das direkte Senden

- **Port:** Port 25 ist erforderlich und muss in Ihrem Netzwerk freigegeben werden.
- **Statische IP-Adresse wird empfohlen:** eine statische IP-Adresse wird empfohlen, sodass ein SPF-Datensatz für Ihre Domäne erstellt werden kann. Dadurch vermieden Ihre Nachrichten als Spam gekennzeichnet wird.
- Keine erforderlich ein Office 365-Postfach mit einer Lizenz.

## Einschränkungen für das direkte Senden

- Das direkte Senden kann nicht zum Übermitteln von E-Mails an externe Empfänger verwendet werden, z. B. an Empfänger mit Adressen von Yahoo oder Gmail.
- Ihre Nachrichten werden Antispamprüfungen unterzogen.
- Gesendete E-Mail werden möglicherweise unterbunden, wenn Ihre IP-Adressen von einer Spameiste blockiert werden.
- Office 365 verwendet Einschränkungsrichtlinien zum Schutz der Leistung des Diensts.

## Option 3: Konfigurieren eines Verbinders zum Senden von E-Mails

## mithilfe des Office 365-SMTP-Relay

Diese Option ist schwieriger zu implementieren als die anderen. Wählen Sie diese Option nur für folgende Situationen aus:

- Die SMTP-Clientübermittlung (Option 1) ist mit Ihren Geschäftsanforderungen oder mit Ihrem Gerät nicht kompatibel
- Sie können das direkte Senden (Option 2) nicht verwenden, da Sie E-Mails an externe Empfänger senden müssen

Das SMTP-Relay gestattet Office 365 das Weiterleiten von E-Mails in Ihrem Namen über Ihre öffentliche IP-Adresse (oder ein Zertifikat) zur Authentifizierung von Office 365. Zu diesem Zweck müssen Sie einen Verbinder für Ihr Office 365-Konto einrichten, wodurch dies zu einer komplizierteren Konfiguration wird.

### Einstellungen für Office 365-SMTP-Relay

EINSTELLUNG FÜR GERÄT ODER ANWENDUNG	WERT
Server/Smarthost	Ihr MX-Endpunkt, z. B. yourcontosodomain-com.mail.protection.outlook.com
Port	Port 25
TLS/StartTLS	Aktiviert
E-Mail-Adresse	Eine beliebige E-Mail-Adresse für eine Ihrer überprüften Office 365-Domänen. Diese E-Mail-Adresse erfordert kein Postfach.

Wenn Sie eingerichtet Exchange Hybrid eingerichtet oder einen Verbinder für den Nachrichtenfluss von Ihrem E-Mail-Server zu Office 365 konfiguriert haben, ist es wahrscheinlich, dass für dieses Szenario keine zusätzlichen Einrichtungsschritte ausgeführt werden müssen. Andernfalls erstellen Sie einen Nachrichtenflussverbinder, um dieses Szenario zu unterstützen:

VERBINDEREINSTELLUNG	WERT
Von	E-Mail-Server Ihrer Organisation
An	Office 365
Domäneneinschränkungen: IP-Adresse/Bereich	Ihre lokale IP-Adresse oder Adresse an, der das Gerät oder einer Anwendung für die Verbindung zu Office 365 verwenden soll

Es wird empfohlen, einen SPF-Eintrag hinzuzufügen, um zu verhindern, dass Nachrichten als Spam gekennzeichnet werden. Wenn Sie über eine statische IP-Adresse senden, fügen Sie diese zu Ihrem SPF-Eintrag in den DNS-Einstellungen Ihrer Domänenregistrierungsstelle wie folgt hinzu:

DNS-EINTRAG	WERT
SPF	v=spf1 ip4:<Static IP Address> include:spf.protection.outlook.com ~all

### Schrittweise Konfigurationsanleitung für SMTP-Relay

1. Ermitteln Sie die öffentliche (statische) IP-Adresse, über die das Gerät oder die Anwendung senden wird.

Eine dynamische IP-Adresse wird nicht unterstützt oder ist nicht zulässig. Sie können Ihre statische IP-Adresse mit anderen Geräten und Benutzern teilen, aber nicht für Personen außerhalb Ihres Unternehmens freigeben. Notieren Sie sich diese IP-Adresse für später.

2. [Melden Sie sich bei Office 365 an.](#)
3. Wählen Sie **Domänen** aus. Stellen Sie sicher, dass Ihre Domäne, z. B. "contoso.com", aktiviert ist. Klicken Sie auf **DNS verwalten**, und suchen Sie den MX-Eintrag. Der MX-Eintrag verfügt über den Wert **VERWEIST AUF DIE ADRESSE**, der "cohownineinc-com.mail.protection.outlook.com" ähnlich ist, wie im folgenden Screenshot veranschaulicht. Notieren Sie den Wert für **VERWEIST AUF DIE ADRESSE** des MX-Eintrags. Dieser ist später erforderlich.



4. Überprüfen Sie, ob die Domänen verifiziert wurden, an die die Anwendung oder das Gerät senden wird. Wenn die Domäne nicht verifiziert wurde, können E-Mails verloren gehen, und Sie sind dann nicht in der Lage, sie mit dem Exchange Online-Tool für die Nachrichtenablaufverfolgung zu verfolgen.
5. Klicken Sie in Office 365 auf **Admin** und dann auf **Exchange**, um zum Exchange Admin Center zu wechseln.
6. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Mit Flow > Connectors**.
7. Überprüfen Sie die Liste der Verbindungen, die für Ihr Unternehmen eingerichtet sind. Wenn kein Verbindung vom E-Mail-Server in Ihrem Unternehmen zu Office 365 aufgeführt ist, erstellen Sie einen.
8. Klicken Sie auf das Pluszeichen, +, um den Assistenten zu starten. Wählen Sie auf dem ersten Bildschirm die Optionen aus, die im folgenden Screenshot dargestellt sind:



Klicken Sie auf **Weiter**, und benennen Sie den Verbindung.

9. Wählen Sie auf dem nächsten Bildschirm die Option **Durch das Überprüfen, ob die IP-Adresse des sendenden Servers mit einer dieser IP-Adressen übereinstimmt, die zu Ihrer Organisation gehören** aus, und fügen Sie die IP-Adresse aus Schritt 1 hinzu.
10. Belassen Sie in allen anderen Feldern die Standardwerte, und wählen Sie **Speichern** aus.
11. Nun, dass Sie mit der Konfiguration Ihrer Einstellungen für Office 365 abgeschlossen haben, fahren Sie mit der Website Ihrer Domänenregistrierungsstelle Ihrer DNS-Einträge aktualisieren. Bearbeiten Sie Ihren SPF-Eintrags. Einschließen Sie die IP-Adresse, die Sie notiert haben in Schritt 1. Die Zeichenfolge nach Abschluss des Vorgangs sollte etwa wie folgt aussehen  
`v=spf1 ip4:10.5.3.2 include:spf.protection.outlook.com ~all`, wobei 10.5.3.2 Ihre öffentliche IP-Adresse ist. Überspringen diesen Schritt kann dazu führen, dass E-Mails an Empfänger Junk-e-Mail-Ordner gesendet werden.
12. Wechseln Sie jetzt wieder zum Gerät, und geben Sie in den Einstellungen unter dem Server oder Smarthost den Wert für **VERWEIST AUF DIE ADRESSE** des MX-Eintrags ein, den Sie in Schritt 3 aufgezeichnet haben.
13. Senden Sie zum Testen der Konfiguration eine Test-E-Mail von Ihrem Gerät oder der Anwendung, und bestätigen Sie, dass sie vom Empfänger empfangen wurde.

### So funktioniert das Office 365-SMTP-Relay

Im folgenden Diagramm verwendet die Anwendung oder das Gerät im Netzwerk Ihres Unternehmens einen Verbindung für das SMTP-Relay, um E-Mails an Empfänger in Ihrem Unternehmen zu senden.



- Der von Ihnen konfigurierte Office 365-Verbinder authentifiziert Ihr Gerät oder die Anwendung unter Verwendung einer IP-Adresse mit Office 365. Ihr Gerät oder die Anwendung kann E-Mails über eine beliebige Adresse senden (einschließlich von Adressen, die keine E-Mails empfangen können), solange die Adresse eine Ihrer Domänen verwendet. Die E-Mail-Adresse muss keinem tatsächlichen Postfach zugeordnet sein. Wenn Ihre Domäne z. B. "contoso.com" ist, könnten Sie über eine Adresse wie "do\_not\_reply@contoso.com" senden.
- Office 365 SMTP-Relay verwendet einen Verbinder, um die von Ihrem Gerät oder Ihrer Anwendung gesendeten E-Mails zu authentifizieren. Auf diese Weise kann Office 365 diese Nachrichten an Ihre eigenen Postfächer sowie an externe Empfänger weiterleiten. Office 365 SMTP-Relay ist dem direkten Senden sehr ähnlich, wobei hierbei jedoch E-Mails an externe Empfänger gesendet werden können.
- Aufgrund der erhöhten Komplexität durch die Konfiguration eines Verbinders wird das direkte Senden dem Office 365 SMTP-Relay vorgezogen, es sei denn, Sie müssen E-Mails an externe Empfänger senden. Ihr Gerät oder Anwendungsserver muss über eine statische IP-Adresse oder einen Adressbereich verfügen, um E-Mails über Office 365 SMTP-Relay senden zu können. Sie können mit SMTP-Relay keine E-Mails über einen gehosteten Dienst eines Drittanbieters wie Microsoft Azure direkt an Office 365 senden.

### **Features des Office 365-SMTP-Relay**

- Office 365 SMTP-Relay erfordert nicht die Verwendung eines lizenzierten Office 365-Postfachs zum Senden von E-Mails.
- Office 365 SMTP-Relay weist höhere Sendegrenzwerte als die SMTP-Clientübermittlung auf. Absender sind nicht an die Grenzwerte von 30 Nachrichten pro Minute oder 10.000 Empfängern pro Tag gebunden.

### **Anforderungen für Office 365-SMTP-Relay**

- Statische IP-Adresse oder Adressbereich:** die meisten Geräte oder Anwendungen können sich nicht um ein Zertifikat für die Authentifizierung verwenden. Um Ihr Gerät oder eine Anwendung zu authentifizieren, verwenden Sie eine oder mehrere statische IP-Adressen, die nicht gemeinsam mit einer anderen Organisation verwendet werden.
- Connector:** Sie müssen einen Connector in Exchange Online für von einem Gerät oder einer Anwendung gesendete e-Mail einrichten.
- Port:** Port 25 ist erforderlich und muss nicht bei Ihrem Internetdienstanbieter oder in Ihrem Netzwerk blockiert werden.
- Lizenzerung:** SMTP-Relay kein bestimmtes Office 365-Postfach verwenden, um e-Mail zu senden. Deshalb ist es wichtig ist, dass nur für lizenzierte Benutzer senden von E-Mails von Geräten oder Anwendungen für die SMTP-Relay konfiguriert sind. Wenn Sie mithilfe von Geräten oder branchenanwendungen Absender, die nicht über ein Office 365-Postfach-Lizenz verfügen verfügen, abrufen und Zuweisen einer Exchange Online Protection-Lizenzvertrags an jeden Absender nicht lizenzierten. Dies ist die kostengünstigste Zielauswahl Lizenz, die Sie zum Senden von e-Mail über Office 365 ermöglicht.

### **Einschränkungen des Office 365-SMTP-Relay**

- Gesendete E-Mail werden möglicherweise unterbunden, wenn Ihre IP-Adressen von einer Spamliste blockiert werden.
- Für das Senden werden angemessene Grenzwerte auferlegt. Weitere Informationen finden Sie unter [Zustellungspool mit höherem Risiko für ausgehende Nachrichten](#).
- Erfordert statische, nicht freigegebene IP-Adressen (sofern kein Zertifikat verwendet wird).

## **Vergleichen der Optionen**

Hier folgt ein Vergleich der einzelnen Konfigurationsoptionen und Features, die sie unterstützen.

	SMTP-CLIENTÜBERMITTLUNG	DIREKTES SENDEN	SMTP-RELAY
<b>Features</b>			
An Empfänger in Ihrer(n) Domäne(n) senden	Ja	Ja	Ja
Weiterleitung zum Internet über Office 365	Ja	Nein. Nur direkte Zustellung.	Ja
Umgeht Antispam	Ja, wenn die E-Mail-Nachrichten für ein Office 365-Postfach bestimmt sind.	Nein. Verdächtige E-Mails werden möglicherweise gefiltert. Es wird ein SPF-Eintrag (Sender Policy Framework) empfohlen.	Nein. Verdächtige E-Mails können gefiltert werden. Wir empfehlen einen benutzerdefinierten SPF-Eintrag.
Unterstützt E-Mail-Versand aus Anwendungen, die von einem Drittanbieter gehostet werden.	Ja	Nein	Nein
<b>Anforderungen</b>			
Offener Netzwerkport	Port 587 oder Port 25	Port 25	Port 25
Gerät oder Anwendungsserver muss TLS unterstützen	Erforderlich	Optional	Optional
Erfordert Authentifizierung	Office 365-Benutzername und Kennwort erforderlich	Keine	Eine oder mehrere statische IP-Adressen Ihr Drucker oder der Server mit der LOB-App muss über eine statische IP-Adresse verfügen, die für die Authentifizierung mit Office 365 verwendet wird.
<b>Einschränkungen</b>			
Einschränkungsgrenzwerte	10.000 Empfänger pro Tag 30 Nachrichten pro Minute	Standardeinschränkung ist für den Schutz von Office 365 vorhanden	Angemessene Grenzwerte werden auferlegt Der Dienst kann nicht zum Senden von Spam oder von Massensendungen verwendet werden. Weitere Informationen zu angemessenen Grenzwerten finden Sie unter <a href="#">Zustellungspool mit höherem Risiko für ausgehende Nachrichten</a> .

Verwenden Ihres eigenen E-Mail-Servers zum Senden von E-Mails über Mehrfunktionsgeräte und Anwendungen

Wenn Sie in Office 365 über Postfächer und einen E-Mail-Server verfügen, den Sie verwalten (auch als lokaler E-Mail-Server bezeichnet), konfigurieren Sie die Geräte und Anwendungen immer für die Verwendung Ihres lokalen Netzwerks, und leiten Sie E-Mails über den eigenen E-Mail-Server weiter. Details zum Einrichten des Exchange-Servers für den Empfang von E-Mails von Systemen, die kein Exchange ausführen (z. B. Multifunktionsdrucker), finden Sie unter [Erstellen eines Empfangsconnectors für den Empfang von E-Mails von einem nicht Exchange ausführenden System](#).

## Verwandte Themen

[Beheben von Problemen mit Druckern, Scannern und LOB-Anwendungen, die E-Mails mithilfe von Office 365 senden](#)

[Konfigurieren von IIS für die Weiterleitung mit Office 365](#)

# Konfigurieren von IIS für Relay mit Office 365

18.12.2018 • 12 minutes to read

Wenn Sie ein Multifunktionsgerät oder eine Anwendung für das Senden von E-Mails über Office 365 einrichten, gibt es einige Situationen, in denen das Gerät oder die Anwendung keine direkte Verbindung zu Office 365 herstellen kann. In diesen Fällen müssen Sie Internetinformationsdienste (IIS) einrichten, um als Zwischenoption zu fungieren.

Sie können dies in folgenden Szenarien verwenden:

- Sie verfügen nicht länger über ein lokales Messaging-System
- Sie verfügen über LOB-Programme oder Geräte in einer lokalen Umgebung
- Ihre LOB-Programme und Geräte müssen E-Mails an Remotedomänen und Ihre Exchange Online-Postfächer senden

Bevor Sie fortfahren, lesen Sie [Einrichten eines Multifunktionsgeräts oder einer Anwendung zum Senden von E-Mails mithilfe von Office 365](#), da möglicherweise eine Option verfügbar ist, die keine Einrichtung eines zusätzlichen Servers zur Weiterleitung erfordert.

## NOTE

Diese Anweisungen können für andere SMTP-Relays geändert werden, über die Sie möglicherweise in Ihrem Unternehmen verfügen.

## Wissenswertes, bevor Sie anfangen

- Geschätzte Zeit zur Durchführung: 15 Minuten
- Ihre lokale Domäne muss in Office 365 als akzeptierte Domäne hinzugefügt werden. Wenn z. B. das Konto für die Weiterleitung "bob@tailspintoys.com" ist, müssen Sie "tailspintoys.com" in Office 365 als akzeptierte Domäne hinzufügen.
- Ihr lokales Konto muss zudem ein für Exchange Online lizenzierte Benutzer in Office 365 oder eine alternative E-Mail-Adresse eines für Exchange Online lizenzierten Benutzers sein. Wenn das Konto für die Weiterleitung z. B. "printer@tailspintoys.com" ist und Sie über "bob@contoso.com" (ein Office 365-Benutzer) weiterleiten möchten, müssen Sie "printer@tailspintoys.com" als alternative E-Mail-Adresse zu "bob@contoso.com" hinzufügen.

## Einrichten von Exchange Online als SMTP-Relay mit Windows Server 2012

1. **Installieren der Internetinformationsdienste (IIS)**
2. Wählen Sie im Server-Manager die Option **Rollen hinzufügen**.
3. Wählen Sie auf der Seite "Vorbereitung" im Assistenten zum Hinzufügen von Rollen die Option **Weiter** aus.
4. Wählen Sie auf der Seite "Installationstyp auswählen" die Option **Rollenbasierte oder featurebasierte Installation** aus.

5. Wählen Sie auf der Seite "Zielserver auswählen" die Option **Einen Server aus dem Serverpool auswählen** und dann den Server aus, der die SMTP-Dienste ausführen wird. Wählen Sie **Weiter** aus.
  6. Wählen Sie auf der Seite "Serverrollen auswählen" die Option **Webserver (IIS)** und dann **Weiter** aus. Wenn eine Seite angezeigt wird, die zusätzliche Features fordert, wählen Sie **Features hinzufügen** und dann **Weiter** aus.
  7. Klicken Sie auf der Seite Rollendienste auswählen stellen Sie sicher, dass Standardauthentifizierung unter Sicherheit aktiviert ist, und wählen Sie dann auf **Weiter**.
  8. Wählen Sie auf der Seite "Installationsschritte bestätigen" die Option **Installieren** aus.
- ## 9. **Installieren von SMTP**
10. Öffnen Sie den Server-Manager, und wählen Sie **Rollen und Features hinzufügen** aus.
  11. Wählen Sie **Serverauswahl** aus, und stellen Sie sicher, dass der Server, der den SMTP-Server ausführen wird, aktiviert ist. Wählen Sie dann "Features" aus.
  12. Wählen Sie auf dem Bildschirm "Features auswählen" die Option **SMTP-Server** aus. Sie werden möglicherweise aufgefordert, zusätzliche Komponenten zu installieren. Wählen Sie in diesem Fall **Erforderliche Features hinzufügen** und dann **Weiter** aus.
  13. Wählen Sie **Installieren** aus. Nach Abschluss der Installation müssen Sie möglicherweise den SMTP-Dienst über das Snap-In "Dienste" für die Microsoft Management Console (MMC) starten.
- ## 14. **Einrichten von SMTP**
15. Öffnen Sie den Server-Manager, wählen Sie **Tools** und dann **Internetinformationsdienste (IIS) 6.0** aus.
  16. Erweitern Sie den aktuellen Server, klicken Sie mit der rechten Maustaste auf den **virtuellen SMTP-Server**, und wählen Sie dann **Eigenschaften** aus.
  17. Wählen Sie auf der Registerkarte "Allgemein" die Option **Erweitert > Hinzufügen** aus.
  18. Geben Sie im Feld "IP-Adresse" die Adresse des Servers an, der den SMTP-Server hostet.
  19. Geben Sie in das Feld "Port" den Wert **587** ein, und wählen Sie **OK** aus.
  20. Führen Sie auf der Registerkarte "Zugriff" die folgenden Aktionen aus:
    21. Wählen Sie **Authentifizierung** aus, und stellen Sie sicher, dass **Anonymer Zugriff** aktiviert ist.
    22. Wählen Sie **Verbindung > Nur Computer in der Liste unten** aus, und geben Sie dann die IP-Adressen der Geräte an, die eine Verbindung mit dem SMTP-Server herstellen, z. B. Drucker.
    23. Wählen Sie **Relay > Nur Computer in der Liste unten** aus, und geben Sie dann die IP-Adresse der Geräte an, die über diesen SMTP-Server weiterleiten.
    24. Wählen Sie auf der Registerkarte "Übermittlung" die Option **Ausgehende Sicherheit** aus, und gehen Sie folgendermaßen vor:
    25. Wählen Sie **Standardauthentifizierung** aus.
    26. Geben Sie die Anmeldeinformationen für die Office 365-Benutzer ein, die Sie zum Weiterleiten von SMTP-E-Mails verwenden möchten.
    27. Wählen Sie **TLS-Verschlüsselung** aus.
    28. Wählen Sie **Ausgehende Verbindungen** aus, und geben Sie im Feld "TCP-Port" den Wert **587** ein, und wählen Sie dann **OK** aus.

29. Wählen Sie **Erweitert** aus, und geben Sie **SMTP.office365.com** als Smarthost ein.

30. **Starten Sie den IIS-Dienst und den SMTP-Dienst neu.**

## Einrichten von Exchange Online als SMTP-Relay mit Windows Server 2008

1. **Installieren der Internetinformationsdienste (IIS)**

2. Wählen Sie im Server-Manager die Option **Rollen hinzufügen**.

3. Wählen Sie auf der Seite "Vorbereitung" im Assistenten zum Hinzufügen von Rollen die Option **Weiter** aus.

4. Wählen Sie auf der Seite "Serverrollen auswählen" die Option **Webserver (IIS)** und dann **Installieren** aus.

5. Wählen Sie "Weiter" aus, bis Sie zur Seite "Rollendienste auswählen" gelangen.

6. Stellen Sie zusätzlich zur aktuellen Auswahl sicher, dass **ODBC-Protokollierung, IIS-Metabasiskompatibilität und IIS 6-Verwaltungskonsole** aktiviert sind, und wählen Sie dann **Weiter** aus.

7. Wenn Sie zum Installieren von IIS aufgefordert werden, wählen Sie "Installieren" aus. Sie müssen den Server möglicherweise neu starten, nachdem die Installation abgeschlossen ist.

8. **Installieren von SMTP**

9. Öffnen Sie den Server-Manager, und wählen Sie **Rollen und Features hinzufügen** aus.

10. Wählen Sie auf dem Bildschirm "Features auswählen" die Option **SMTP-Server** aus. Sie werden möglicherweise aufgefordert, zusätzliche Komponenten zu installieren. Wählen Sie in diesem Fall **Erforderliche Features hinzufügen** und dann **Weiter** aus.

11. Wählen Sie **Installieren** aus. Nach Abschluss der Installation müssen Sie möglicherweise den SMTP-Dienst über das Snap-In "Dienste" für die Microsoft Management Console (MMC) starten.

12. **Einrichten von SMTP**

13. Wählen Sie **Start > Verwaltung > Internetinformationsdienste (IIS) 6.0** aus.

14. Erweitern Sie den aktuellen Server, klicken Sie mit der rechten Maustaste auf den **virtuellen SMTP-Server**, und wählen Sie dann **Eigenschaften** aus.

15. Wählen Sie auf der Registerkarte "Allgemein" die Option **Erweitert > Hinzufügen** aus.

16. Geben Sie im Feld "IP-Adresse" die Adresse des Servers an, der den SMTP-Server hostet.

17. Geben Sie in das Feld "Port" den Wert **587** ein, und wählen Sie **OK** aus.

18. Führen Sie auf der Registerkarte "Zugriff" die folgenden Aktionen aus:

19. Wählen Sie "Authentifizierung" aus, und stellen Sie sicher, dass **Anonymer Zugriff** aktiviert ist.

20. Wählen Sie **Verbindung > Nur Computer in der Liste unten** aus, und geben Sie dann die IP-Adressen der Geräte an, die eine Verbindung mit dem SMTP-Server herstellen, z. B. Drucker.

21. Wählen Sie **Relay > Nur Computer in der Liste unten** aus, und geben Sie dann die IP-Adresse der Geräte an, die über diesen SMTP-Server weiterleiten.

22. Wählen Sie auf der Registerkarte "Übermittlung" die Option **Ausgehende Sicherheit** aus, und gehen Sie folgendermaßen vor:

23. Wählen Sie **Standardauthentifizierung** aus.
24. Geben Sie die Anmeldeinformationen für die Office 365-Benutzer ein, die Sie zum Weiterleiten von SMTP-E-Mails verwenden möchten.
25. Wählen Sie **TLS-Verschlüsselung** aus.
26. Wählen Sie **Ausgehende Verbindungen** aus, und geben Sie im Feld "TCP-Port" den Wert **587** ein, und wählen Sie dann **OK** aus.
27. Wählen Sie **Erweitert** aus, und geben Sie **SMTP.office365.com** als Smarthost ein.
28. **Starten Sie den IIS-Dienst und den SMTP-Dienst neu.**

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Sie können die SMTP-Relay-Dienste testen, ohne eine separate LOB-Anwendung oder ein Gerät zu verwenden.

Verwenden Sie die folgenden Schritte, um SMTP-Relay-Dienste zu testen.

1. Erstellen Sie eine Textdatei mit Notepad oder einem anderen Texteditor. Die Datei sollte den folgenden Code enthalten. Ersetzen Sie die Ausgangs- und Ziel-E-Mail-Adressen durch die Adressen, die Sie zur Weiterleitung von SMTP verwenden werden.

```
FROM: <source email address>
TO: <destination email address>
SUBJECT: Test email
This is a test email sent from my SMTP server
```

2. Speichern Sie die Datei als Email.txt.
3. Kopieren Sie die Datei "Email.txt" in den folgenden Ordner: C:\InetPub\MailRoot\Pickup.
4. Nach einer kurzen Zeit sollte die Datei automatisch in den Ordner "C:\InetPub\MailRoot\Queue" verschoben werden. Wenn der SMTP-Server die E-Mail übermittelt, wird die Datei automatisch aus dem lokalen Ordner gelöscht.

**Caution**

Wenn der SMTP-Server die Nachricht nicht übermitteln kann, wird ein Unzustellbarkeitsbericht (NDR) im Ordner "C:\InetPub\MailRoot\BadMail" erstellt. Mithilfe dieses Unzustellbarkeitsberichts können Sie Übermittlungsprobleme analysieren.

## Verwandte Themen

[Problembehandlung bei von Druckern und Geschäftsanwendungen gesendeten E-Mails](#)

[Einrichten eines Multifunktionsgeräts oder einer Anwendung zum Senden von E-Mails mithilfe von Office 365](#)

# Beheben von Problemen mit Drucken, Scannern und LOB-Anwendungen, die E-Mails mithilfe von Office 365 senden

18.12.2018 • 19 minutes to read

E-Mail-Clients stellen umsetzbare Fehlermeldungen bereit, wenn ein Problem auftritt. Das Senden von E-Mails von Geräten und Anwendungen ist weniger leicht zu beheben, und Sie erhalten möglicherweise keine eindeutigen Informationen. Dieser Artikel kann Sie bei der Problembehandlung unterstützen und er verwendet Druckerkonfigurationen als Beispiele.

**Überprüfen Sie als ersten Schritt zum Beheben von Problemen die Konfiguration.** Ausführliche Informationen zu den Konfigurationsoptionen finden Sie unter [Einrichten eines Multifunktionsgeräts oder einer Anwendung zum Senden von E-Mails mithilfe von Office 365](#).

## Mein Drucker ist bereits für E-Mails konfiguriert, aber ich weiß nicht, welche Konfigurationsoption verwendet wird

Nachfolgend finden Sie die drei Konfigurationsoptionen, die Ihnen dabei helfen zu erkennen, welche Konfiguration verwendet wird:

### 1. SMTP-Clientübermittlung (empfohlen)

- Ihr Drucker ist mit dem Office 365-Server "smtp.office365.com" verbunden.
- Sie haben eine E-Mail-Adresse und das Kennwort für das Druckerpostfach eingegeben.
- Der Drucker kann E-Mails an Personen innerhalb und außerhalb Ihres Unternehmens senden.

### 2. Direktes Senden

- Ihr Drucker ist mit einem Office 365-Server verbunden, dessen Name mit "mail.protection.outlook.com" endet.
- Es ist in Office 365 kein Verbinder für E-Mails eingerichtet, die über das Unternehmensnetzwerk gesendet werden.
- Der Drucker kann E-Mails nur an Personen in Ihrem Unternehmen senden. Es können keine E-Mails an Empfänger außerhalb des Unternehmens gesendet werden.

### 3. Office 365 SMTP-Relay

- Ihr Drucker ist mit einem Office 365-Server verbunden, dessen Name mit "mail.protection.outlook.com" endet.
- Es ist in Office 365 ein Verbinder für E-Mails eingerichtet, die über das Unternehmensnetzwerk an Office 365 gesendet werden.
- Der Drucker kann E-Mails an Personen innerhalb und außerhalb Ihres Unternehmens senden.

# Beheben von Problemen bei der SMTP-Clientübermittlung

**Ich habe meinen Drucker für die SMTP-Clientübermittlung eingerichtet, ich kann aber weiterhin keine E-Mails senden**

1. Überprüfen Sie die Einstellungen, die direkt in den Drucker eingegeben wurden:

Druckereinstellung Wert  :----- -----	Server/Smarthost
SMTP.Office365.com	
Port	
Port 587 (empfohlen) oder Port 25	
TLS/StartTLS	
Aktiviert	
Benutzername/E-Mail-Adresse und Kennwort	
Vom Drucker verwendete Anmeldeinformationen des Office 365-Postfachs	

2. Wenn der Drucker kein Kennwort für die eingegebene E-Mail-Adresse erfordert, versucht der Drucker, die E-Mails ohne Anmeldung bei Office 365 zu senden. Die SMTP-Clientübermittlung erfordert vom Drucker die Anmeldung bei Office 365. Das direkte Senden und das Office 365 SMTP-Relay erfordern keine Anmeldung. Erwägen Sie stattdessen eine dieser Optionen.
3. Der Drucker oder die Anwendung muss E-Mails über dieselbe Adresse senden, für die Sie während der E-Mail-Einrichtung die Anmeldeinformationen eingegeben haben. Wenn der Drucker oder die Anwendung versucht, E-Mails über ein anderes Konto zu senden, führt dies zu einem Fehler ähnlich dem Folgenden:

## **5.7.60 SMTP; Client does not have permissions to send as this sender.**

Wenn Sie z. B. Anmeldeinformationen für "sales@contoso.com" in Ihre Anwendungseinstellungen eingegeben haben, die Anwendung aber versucht, E-Mails von "salesperson1@contoso.com" zu senden, wird dies nicht unterstützt. Verwenden Sie für dieses Szenario stattdessen Office 365 SMTP-Relay.

4. Testen Sie den Benutzernamen und das Kennwort durch Anmeldung bei Outlook im Web, und versuchen Sie, eine Test-E-Mail zu senden, um sicherzustellen, dass das Konto nicht blockiert ist. Wenn der Benutzer blockiert ist, finden Sie Hilfe im Artikel [Entfernen eines Benutzers, einer Domäne oder einer IP-Adresse aus der Sperrliste nach dem Senden einer Spam-E-Mail](#).
5. Als nächstes testen Sie, ob Sie eine Verbindung mit Office 365 über Ihr Netzwerk herstellen können, indem Sie die folgenden Schritte ausführen:
6. Befolgen Sie die Anweisungen zum [Installieren des Telnet-Clienttools](#) auf einem Computer im gleichen Netzwerk wie das Gerät oder die Anwendung.
7. Führen Sie das Tool über die Befehlszeile aus, indem Sie **telnet** eingeben.
8. Geben Sie **open smtp.office365.com 587** ein (oder ersetzen Sie **25** für **587**, wenn Sie stattdessen diese Porteinstellung verwenden).
9. Wenn Sie erfolgreich mit einem Office 365-Server verbunden sind, erwarten Sie den Erhalt einer Antwortzeile, die der folgenden ähnelt:  
**220 BY1PR10CA0041.outlook.office365.com Microsoft ESMTP MAIL Service ready at Mon, 1 Jun 2015 12:00:00 +0000**
10. Wenn Sie keine Verbindung mit Office 365 herstellen können, wurde Port 587 oder 25 möglicherweise von Ihrer Netzwerkschutzmauer oder dem Internetdienstanbieter blockiert. Beheben Sie dies, damit Sie E-Mails von Ihrem Drucker senden können.

11. Wenn keines dieser Probleme auf Ihr Gerät zutrifft, erfüllt es möglicherweise nicht die Voraussetzungen für die TLS-Verschlüsselung (Transport Layer Security). Ihr Gerät muss TLS, Version 1.0 oder höher, unterstützen. Aktualisieren Sie die Firmware auf dem Gerät, um dieses Problem zu beheben, oder führen Sie eine der anderen Konfigurationsoptionen aus, bei denen TLS optional ist.

Weitere Informationen zu TLS finden Sie unter [So sichert Exchange Online mithilfe von TLS E-Mail-Verbindungen in Office 365](#). Ausführliche technische Informationen dazu, wie TLS von Exchange Online mit Verschlüsselungssammlungsreihenfolge verwendet wird, finden Sie unter [Verbessern der Nachrichtenflussicherheit für Exchange Online](#).

### **Ich habe einen Authentifizierungsfehler erhalten, als mein Gerät versucht hat, E-Mails zu senden**

Dies kann durch eine Reihe von Problemen verursacht werden:

1. Stellen Sie sicher, dass Sie den richtigen Benutzernamen und das zugehörige Kennwort eingegeben haben.
2. Versuchen Sie, sich mit dem Benutzernamen und Kennwort des Druckers bei OWA anzumelden. Senden Sie eine E-Mail, um sicherzustellen, dass das Postfach aktiv ist und nicht für das Senden von Spam blockiert wurde.
3. Überprüfen Sie, ob Ihr Gerät oder die Anwendung TLS, Version 1.0 oder höher, unterstützt. Die beste Möglichkeit, dies zu überprüfen, besteht darin, ein Upgrade für die Firmware auf dem Gerät durchzuführen oder die Anwendung, über die Sie E-Mails senden, auf die neueste Version zu aktualisieren. Wenden Sie sich an den Gerätehersteller, um zu bestätigen, dass dieser TLS, Version 1.0 oder höher, unterstützt.

### **Fehler: 5.7.60 SMTP; Client ist nicht berechtigt, als dieser Absender zu senden**

Dieser Fehler weist darauf hin, dass das Gerät versucht, eine E-Mail über eine Adresse zu senden, die nicht den Anmeldeinformationen entspricht. Ein Beispiel wäre, wenn Sie Anmeldeinformationen für "sales@contoso.com" in Ihre Anwendungseinstellungen eingegeben haben, die Anwendung aber versucht, E-Mails von "salesperson1@contoso.com" zu senden. Wenn sich die Anwendung oder der Drucker auf diese Weise verhält, verwenden Sie Office 365 SMTP-Relay, da dieses Szenario nicht von der SMTP-Clientübermittlung unterstützt wird.

### **Fehler: Client wurde nicht authentifiziert, um bei "E-MAIL VON" anonyme E-Mails zu senden**

Dieser Fehler weist darauf hin, dass Ihr Drucker eine Verbindung mit dem Endpunkt der SMTP-Clientübermittlung (smtp.office365.com) herstellt. Ihr Drucker muss sich jedoch auch bei einem Postfach anmelden, um eine E-Mail senden zu können. Dieser Fehler tritt auf, wenn Sie keine Anmeldeinformationen für ein Postfach in den Druckereinstellungen eingegeben haben. Ist keine Option zum Eingeben von Anmeldeinformationen verfügbar, unterstützt dieser Drucker die SMTP-Clientübermittlung nicht. Verwenden Sie stattdessen entweder das direkte Senden oder Office 365 SMTP-Relay. Weitere Informationen finden Sie unter [Einrichten eines Multifunktionsgeräts oder einer Anwendung zum Senden von E-Mails mithilfe von Office 365](#).

### **Fehler: 550 5.1.8 Falscher ausgehender Absender**

Dieser Fehler weist darauf hin, dass das Gerät versucht, eine E-Mail aus einem Office 365-Postfach zu senden, das sich auf einer Liste "Blockieren" für Spam befindet. Hilfe hierzu finden Sie unter [Entfernen eines Benutzers, einer Domäne oder einer IP-Adresse von einer Liste "Blockieren" nach dem Senden von Spam-E-Mails](#).

## **Beheben von Problemen beim direkten Senden**

### **Ich habe meinen Drucker für das direkte Senden eingerichtet und er sendet keine E-Mails - oder - Mein Gerät hat E-Mails über direktes Senden gesendet, aber dann den Vorgang abgebrochen**

Dies kann durch eine Reihe von Problemen verursacht werden:

1. Eine häufige Ursache für Probleme beim direkten Senden ist eine blockierte IP-Adresse. Wenn Antispamtools von Ihrem Unternehmen ausgehende Spammnachrichten erkennen, kann Ihre IP-Adresse durch eine Liste "Blockieren" für Spam blockiert werden. Überprüfen Sie mit einem Drittanbieterdienst wie

MXToolbox oder WhatIsMyIPAddress, ob sich Ihre IP-Adresse auf einer Liste "Blockieren" befindet. Wenden Sie sich an das Unternehmen, dass Ihre IP-Adresse zur Liste "Blockieren" hinzugefügt hat. Office 365 verwendet diese Listen, um unseren Dienst zu schützen. Hilfe hierzu finden Sie unter [Entfernen eines Benutzers, einer Domäne oder einer IP-Adresse von einer Liste "Blockieren" nach dem Senden von Spam-E-Mails.](#)

- Um ein Problem mit Ihrem Gerät auszuschließen, senden Sie eine Test-E-Mail, um die Verbindung mit Office 365 zu prüfen. Befolgen Sie zum Senden einer Test-E-Mail die Schritte im Artikel [Verwenden von Telnet zum Testen der SMTP-Kommunikation](#). Wenn Sie keine Verbindung mit Office 365 herstellen können, wurde die Kommunikation über Port 25 möglicherweise von Ihrem Netzwerk oder Internetdienstanbieter blockiert. Wenn Sie dies nicht rückgängig machen können, verwenden Sie stattdessen die SMTP-Clientübermittlung.

#### **Fehler: Client wurde nicht authentifiziert, um bei "E-MAIL VON" anonyme E-Mails zu senden**

Dies weist darauf hin, dass Sie eine Verbindung mit dem Endpunkt der SMTP-Clientübermittlung (smtp.office365.com) herstellen, der nicht für direktes Senden verwendet werden kann. Verwenden Sie für das direkte Senden den MX-Endpunkt für Ihren Office 365-Mandanten, der mit "mail.protection.outlook.com" endet. Befolgen Sie die Schritte in [Option 2: Direktes Senden von E-Mails von einem Drucker oder einer Anwendung an Office 365](#), um Ihren MX-Endpunkt zu finden.

#### **Meine E-Mails werden nicht an Empfänger außerhalb meines Unternehmens gesendet**

Dies ist beabsichtigt. Beim direkten Senden dürfen E-Mails nur an Empfänger in Ihrem Unternehmen gesendet werden, die in Office 365 gehostet werden. Wenn Sie E-Mails an externe Empfänger senden müssen, verwenden Sie die SMTP-Clientübermittlung oder Office 365 SMTP-Relay.

#### **Der MX-Endpunkt ist für das Feld der Druckereinstellung zu lang. Kann ich stattdessen eine IP-Adresse verwenden?**

Es ist nicht möglich, eine IP-Adresse anstelle eines MX-Endpunkts zu verwenden. Dies kann dazu führen, dass Sie zukünftig keine Nachrichten mehr senden können. Wenn der MX-Endpunkt zu lang ist, erwägen Sie die Verwendung der SMTP-Clientübermittlung, die einen kürzeren Endpunkt (smtp.office365.com) aufweist.

#### **E-Mails von meinem Gerät werden von Office 365 als Junk-E-Mails gekennzeichnet.**

Für das direkte Senden wird die Verwendung eines Geräts empfohlen, das über eine statische IP-Adresse sendet. Dadurch können Sie einen SPF-Eintrag (Sender Policy Framework) einrichten, der Sie dabei unterstützt zu verhindern, dass E-Mails als Spam gekennzeichnet werden. Überprüfen Sie, ob der SPF-Eintrag mit Ihrer statischen IP-Adresse eingerichtet ist. Eine Änderung beim Netzwerk oder Internetdienstanbieter könnte Ihre statische IP-Adresse ändern. Aktualisieren Sie den SPF-Eintrag, um diese Änderung widerzuspiegeln. Wenn Sie nicht über eine eigene statische IP-Adresse senden, sollten Sie stattdessen die SMTP-Clientübermittlung erwägen.

## **Beheben von Problemen mit Office 365 SMTP-Relay**

#### **Ich habe meinen Drucker für Office 365 SMTP-Relay eingerichtet und er sendet keine E-Mails - oder - Mein Gerät hat E-Mails über SMTP-Relay gesendet, aber dann den Vorgang abgebrochen**

Dies kann durch eine Reihe von Problemen verursacht werden.

- Eine häufige Ursache für Probleme beim Office 365 SMTP-Relay ist eine blockierte IP-Adresse. Wenn Antispamtools von Ihrem Unternehmen ausgehende Spammnachrichten erkennen, kann Ihre IP-Adresse durch eine Liste "Blockieren" für Spam blockiert werden. Überprüfen Sie mit einem Drittanbieterdienst wie MXToolbox oder WhatIsMyIPAddress, ob sich Ihre IP-Adresse auf einer Liste "Blockieren" befindet. Wenden Sie sich an das Unternehmen, dass Ihre IP-Adresse zur Liste "Blockieren" hinzugefügt hat. Office 365 verwendet diese Listen, um unseren Dienst zu schützen. Hilfe hierzu finden Sie unter [Entfernen eines Benutzers, einer Domäne oder einer IP-Adresse von einer Liste "Blockieren" nach dem Senden von Spam-E-Mails.](#)
- Um ein Problem mit Ihrem Gerät auszuschließen, senden Sie eine Test-E-Mail, um die Verbindung mit

Office 365 zu prüfen. Befolgen Sie zum Senden einer Test-E-Mail die Schritte im Artikel [Verwenden von Telnet zum Testen der SMTP-Kommunikation](#). Wenn Sie keine Verbindung mit Office 365 herstellen können, wurde die Kommunikation über Port 25 möglicherweise von Ihrem Netzwerk oder Internetdienstanbieter blockiert. Wenn Sie dies nicht rückgängig machen können, verwenden Sie stattdessen die SMTP-Clientübermittlung.

#### **E-Mails werden nicht mehr an externe Empfänger gesendet**

Änderungen am Netzwerk oder beim Internetdienstanbieter könnten Ihre statische IP-Adresse ändern. Dies führt dazu, dass Ihr Verbinder die Nachrichten an externe Empfänger nicht erkennt und nicht weiterleitet. Aktualisieren Sie den Verbinder und den SPF-Eintrag mit der neuen IP-Adresse. Führen Sie die Schritte in [Option 3: Konfigurieren eines Verbinders zum Senden von E-Mails mithilfe des Office 365-SMTP-Relay](#) aus, um die vorhandenen Einstellungen des Verbinders zu bearbeiten.

#### **E-Mails von meinem Gerät werden von Office 365 als Junk-E-Mails gekennzeichnet.**

Office 365 SMTP-Relay erfordert von Ihrem Gerät, dass E-Mails über eine statische IP-Adresse gesendet werden. Überprüfen Sie, ob der SPF-Eintrag mit Ihrer statischen IP-Adresse eingerichtet ist. Eine Änderung beim Netzwerk oder Internetdienstanbieter könnte Ihre statische IP-Adresse ändern. Aktualisieren Sie den SPF-Eintrag, um diese Änderung widerzuspiegeln. Wenn Sie nicht über eine eigene statische IP-Adresse senden, sollten Sie stattdessen die SMTP-Clientübermittlung erwägen.

## Siehe auch

[Konfigurieren von IIS für Relay mit Office 365](#)

# Empfänger in Exchange Online

18.12.2018 • 2 minutes to read

In Exchange Online wurde im Exchange Administrationscenter (EAC) als das GUI-basiertes Verwaltungstool zum Verwalten von Empfängern Cloud-basierten Exchange Control Panel (ECP) ersetzt. Der Exchange-Verwaltungskonsole ersetzt auch die Exchange-Verwaltungskonsole in Exchange Server. Weitere Informationen finden Sie unter [Exchange-Verwaltungskonsole](#).

## Verwalten von Empfängern in Exchange Online

Obwohl der Exchange-Verwaltungskonsole eine unterschiedliche Aussehen und Verhalten, als die ECP verfügt, ähnelt Verwalten von Exchange Online-Empfänger in der Exchange-Verwaltungskonsole zum Verwalten von Empfängern in der aktuellen Version von Exchange Online. Und da Sie die Exchange-Verwaltungskonsole in beiden Exchange Online verwenden und lokale Exchange-Organisationen, Verwalten von Empfängern Cloud-basierten vergleichbar mit der Verwaltung von lokalen Empfänger ist. Weitere Informationen zum Verwalten von einige der verschiedenen Typen von Empfängern in Exchange Online finden Sie unter den folgenden Artikeln:

- [Erstellen von Benutzerpostfächern in Exchange Online](#)
- [Verwalten von Berechtigungen für Empfänger](#)
- [Erstellen und Verwalten von Verteilergruppen](#)
- [Verwalten von E-Mail-aktivierten Sicherheitsgruppen](#)
- [Verwalten dynamischer Verteilergruppen](#)
- [Verwalten von E-Mail-Kontakten](#)
- [Verwalten von E-Mail-Benutzern](#)
- [Erstellen und Verwalten von Raumpostfächern](#)
- [Verwalten von Gerätewebpostfächern](#)
- [Verwalten von Berechtigungen für Empfänger](#)

# Grenzwerte für Nachrichten und Empfänger in Exchange Online

18.12.2018 • 2 minutes to read

Die Inhalte in diesem Thema wurden in ein anderes Thema verschoben. Das neue Thema finden Sie unter [Exchange Online-Begrenzungen](#).

# Erstellen von Benutzerpostfächern in Exchange Online

18.12.2018 • 4 minutes to read

Sie müssen das Office 365 Administrationscenter oder Exchange Online PowerShell verwenden, um ein Exchange Online-Benutzerpostfach zu erstellen. Sie können keine neuen Benutzerpostfächer mithilfe der Exchange-Verwaltungskonsole (EAC) erstellen. Nachdem Exchange Online-Postfächern erstellt wurden, können Sie sie mithilfe der Exchange-Verwaltungskonsole verwalten.

## NOTE

Nach dem Erstellen eines neuen Postfachs von Exchange Online PowerShell, Sie haben eine Exchange Online-Lizenz zuweisen oder wird deaktiviert werden, wenn der 30-Tage-Nachfrist.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berechtigungen für die Empfängerbereitstellung" im Thema [Mailbox Permissions](#).
- Es empfiehlt sich, sichere Kennwörter zu verwenden, die mindestens acht Zeichen lang sind und aus Groß- und Kleinbuchstaben, Zahlen und Symbolen bestehen.
- Wie Sie mit Windows PowerShell eine Verbindung mit Exchange Online herstellen, können Sie unter [Herstellen einer Verbindung mit Exchange Online PowerShell](#) nachlesen.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Was möchten Sie machen?

### Verwenden von Office 365 Admin Center zum Erstellen eines neuen Postfachs

Mithilfe der Office 365 Admin Center können Sie ein neues Benutzerkonto erstellen. Wenn Sie dem Benutzerkonto eine Lizenz für Exchange Online zuweisen, wird automatisch ein Postfach für den Benutzer erstellt. Weitere Informationen zum Erstellen neuer Benutzerkonten über die Office 365 Admin Center finden Sie in den folgenden Themen:

- [Erstellen oder Bearbeiten von Benutzern](#)
- [Hinzufügen mehrerer Benutzer mit einer CSV-Datei](#)

### Verwenden von Exchange Online PowerShell zum Erstellen eines neuen Postfachs

Dieses Beispiel erstellt ein Exchange Online-Postfach und ein Benutzerkonto für Office 365 für Holly Holt. Der

optionale Parameter *ResetPasswordOnNextLogon* erfordern, dass den Benutzer ihr Kennwort zurücksetzen der ersten bei Office 365 Anmeldung.

```
New-Mailbox -Alias hollyh -Name hollyh -FirstName Holly -LastName Holt -DisplayName "Holly Holt" -  
MicrosoftOnlineServicesID hollyh@corp.contoso.com -Password (ConvertTo-SecureString -String 'P@ssw0rd' -  
AsPlainText -Force) -ResetPasswordOnNextLogon $true
```

Nachdem Sie ein Postfach mithilfe des zuvor aufgeführten Befehls erstellt haben, wird außerdem ein Office 365-Benutzerkonto erstellt. Sie müssen dieses Benutzerkonto aktivieren, indem Sie ihm eine Lizenz zuweisen. Informationen zum Zuweisen einer Lizenz in der Office 365 Admin Center finden Sie unter [Zuweisen oder Entfernen einer Lizenz](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um die Erstellung eines neuen Postfachs zu überprüfen:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**. Das neue Benutzerpostfach wird in der Postfachliste angezeigt. Unter **Postfachtyp** lautet der Typ **Benutzer**. Klicken Sie auf **Aktualisieren** Wenn das neue Postfach zuerst nicht angezeigt wird.
- Überprüfen Sie in der Office 365 Admin Center, ob das neue Benutzerkonto aufgeführt und ihm eine Exchange Online-Lizenz zugewiesen ist.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um Informationen zum neuen Benutzerpostfach anzuzeigen.

```
Get-Mailbox <Name> | Format-List Name,RecipientTypeDetails,PrimarySmtpAddress,SKUAssigned
```

Wenn das Postfach eine Lizenz zugewiesen ist, ist der Wert für die Eigenschaft *SKUAssigned* True . Wenn eine Lizenz zugewiesen wurde noch nicht, ist der Wert leer.

# Löschen oder Wiederherstellen von Benutzerpostfächern in Exchange Online

18.12.2018 • 14 minutes to read

Es gibt einige Überlegungen, die Sie in Betracht ziehen sollten, bevor Sie ein Benutzerpostfach löschen. Es gibt verschiedene Arten von Löschgängen, die Sie für ein Benutzerpostfach durchführen können, und bei einigen ist eine Wiederherstellung des Postfach nicht möglich. In diesem Artikel werden verschiedene Löschszenarien für Postfächer beschrieben. Des Weiteren sind hier Informationen zum Löschen, Wiederherstellen und dauerhaften Entfernen eines Postfachs aus Exchange Online enthalten.

## Vorläufig gelöschte Benutzerpostfächer

Ein vorläufig gelöschten Benutzerpostfach ist ein Postfach, die von Office 365 Administrationscenter oder das Cmdlet **Remove-Mailbox** in Exchange Online PowerShell gelöscht wurde, und wurde noch im Papierkorb Azure active Directory (AD Azure) weniger als 30 Tage.

Ein gelösches Postfach gilt in folgenden Fällen als vorläufig gelösches Benutzerpostfach:

- Das mit dem Benutzerpostfach verknüpfte Azure Active Directory-Benutzerkonto wird vorläufig gelöscht.  
(Das Azure Active Directory-Benutzerobjekt liegt außerhalb des Gültigkeitsbereichs oder im Papierkorbcontainer.)
- Das mit dem Benutzerpostfach verknüpfte Azure Active Directory-Benutzerkonto wurde dauerhaft gelöscht, für das Exchange Online-Postfach jedoch das Beweissicherungsverfahren oder der eDiscovery-Speicher aktiviert ist.
- Das dem Postfach des Benutzers zugeordnete Azure Active Directory-Benutzerkonto wurde innerhalb der letzten 30 Tage gelöscht. Dies ist die Aufbewahrungszeit, für die Exchange Online das Postfach in einem vorläufig gelöschten Zustand beibehält, bevor es endgültig gelöscht wird und nicht mehr wiederhergestellt werden kann.

### NOTE

Wenn Sie mit dem Azure-Cmdlet ausführen `Remove-MsolUser` mit der `-RemoveFromRecycleBin` Parameter, um einen Benutzer aus dem Papierkorb Azure AD entfernen ein vorhandenes Exchange Online-Postfach Azure AD-Benutzer in einem vorläufig gelöschten Zustand zugeordnet wird immer versetzt, solange die Lizenz des Benutzers wurde keine entfernt. Wenn Sie die Lizenz des Benutzers vor dem Entfernen des Benutzers aus dem Papierkorb entfernen, wird der Benutzer jedoch nicht in einem vorläufig gelöschten Postfach Benutzerstatus wechseln.

Wenn während dieser Dauer von 30 Tagen ein neuer Azure Active Directory-Benutzer aus dem ursprünglichen lokalen Empfängerkontos mit der gleichen ExchangeGuid oder ArchiveGuid synchronisiert wird, führt dies zu einem Fehler bei der ExchangeGuid-Überprüfung.

Checken Sie weitere Informationen zum Erstellen eines inaktiven Postfachs durch Platzieren einer Aufbewahrung für eventuelle Rechtsstreitigkeiten für ein Postfach, vor dem Löschen von [Übersicht über inaktiver Postfächer in Office 365](#).

## Dauerhaft gelöschte Benutzerpostfächer

Ein gelösches Postfach gilt in folgenden Fällen als dauerhaft gelösches Benutzerpostfach:

- Das Postfach wurde vor mehr als 30 Tagen vorläufig gelöscht und der verknüpfte Azure Active Directory-Benutzer wurde dauerhaft gelöscht. Führen Sie das **Remove-MsolUser**-Cmdlet durch. Alle Postfachinhalte wie E-Mails, Kontakte und Dateien werden dauerhaft gelöscht.
- Das dem Postfach des Benutzers zugeordnete Azure Active Directory-Benutzerkonto wurde in Azure Active Directory dauerhaft gelöscht. Das Postfach des Benutzers ist jetzt in Exchange Online vorläufig gelöscht und verbleibt für 30 Tage in diesem Zustand. Wenn während dieser Dauer von 30 Tagen ein neuer Azure Active Directory-Benutzer aus dem ursprünglichen lokalen Empfängerkonto mit der gleichen ExchangeGuid oder ArchiveGuid synchronisiert wird, und dieses neue Konto für Exchange Online lizenziert ist, führt dies zur dauerhaften Löschung des ursprünglichen Benutzerpostfachs. Der gesamte Inhalt des Postfachs, z. B. E-Mail-Nachrichten, Kontakte und Dateien, werden unwiederbringlich gelöscht.
- Weiche gelöschten Postfachs wurde verwenden das Cmdlet **Remove-Mailbox** mit dem Parameter *PermanentlyDelete* in Exchange Online PowerShell gelöscht.

In den oben genannten Szenarien wird davon ausgegangen, dass für das Benutzerpostfach keine Aufbewahrung festgelegt wurde wie das Beweissicherungsverfahren oder der eDiscovery-Speicher. Wenn eine Art der Aufbewahrung für das Benutzerpostfach aktiviert ist, kann das Postfach nicht aus Exchange Online entfernt werden. Bei Typen von E-Mail-Benutzerempfängern werden das Beweissicherungsverfahren oder der eDiscovery-Speicher ignoriert und haben keine Auswirkungen auf die vorläufigen und dauerhaften Löschvorgänge von E-Mail-Benutzern. Das E-Mail-Benutzerobjekt kann nicht gelöscht werden, wenn es mit einem Journalpostfach verknüpft ist. Sie können die Journalfunktion für den E-Mail-Benutzer mit dem **Disable-JournalArchiving**-Cmdlet deaktivieren.

## Löschen eines Benutzerpostfachs

### **Verwenden des Office 365 Admin Center zum Löschen eines Benutzerkontos**

Wenn Sie ein Office 365-Benutzerkonto löschen, wird das entsprechende Exchange Online-Postfach gelöscht und aus der Liste der Postfächer in der Exchange-Verwaltungskonsole entfernt. Nachdem das Benutzerkonto gelöscht wurde, wird es im Office 365 Admin Center auf der Seite **Gelöschte Benutzer** aufgeführt. Es kann nach dem Löschen innerhalb von 30 Tagen wiederhergestellt werden. Nach 30 Tagen werden das Benutzerkonto und das Postfach endgültig gelöscht, und sie können nicht wiederhergestellt werden.

Weitere Informationen zum Löschen eines Office 365-Geschäfts- oder Schulkontos finden Sie unter [Löschen oder Wiederherstellen von Benutzern](#).

### **Verwenden von Exchange Online PowerShell zum Löschen eines Postfachs**

- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berechtigungen für die Empfängerbereitstellung" im Thema [Recipients permissions](#).
- Wie Sie mit Windows PowerShell eine Verbindung mit Exchange Online herstellen, können Sie unter [Herstellen einer Verbindung mit Exchange Online PowerShell](#) nachlesen.

Wenn Sie ein Exchange Online-Postfach über Exchange Online PowerShell löschen, wird die entsprechende Office 365-Benutzer gelöscht und aus der Liste der Benutzer im Office 365 Administrationscenter entfernt. Der Benutzer wird für 30 Tage weiterhin wiederhergestellt werden. Nachdem das Zeitlimit 30 Tage ist der Benutzer dauerhaft gelöscht.

Bei diesem Beispiel werden ein Exchange Online-Postfach und das entsprechende Office 365-Benutzerkonto für Walter Harp gelöscht.

```
Remove-Mailbox -Identity "Walter Harp"
```

### **Verwenden von Windows Powershell zum dauerhaften Löschen eines Benutzerpostfachs**

In diesem Beispiel wird das Benutzerkonto für Walter Harp aus Azure Active Directory gelöscht.

```
Remove-MsolUser -UserPrincipalName <Walter Harp> -RemoveFromRecycleBin true
```

Weitere Informationen dazu finden Sie unter [Remove-MsolUser](#).

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie eine der folgenden Aktionen aus, um sicherzustellen, dass Sie ein Exchange Online-Postfach erfolgreich gelöscht haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**. Das gelöschte Postfach wurde aus der Postfachliste entfernt.

Klicken Sie auf **Aktualisieren** ⓘ Wenn das gelöschte Postfach weiterhin angezeigt wird.

- Wenn Sie das Office 365-Benutzerkonto gelöscht haben, stellen Sie sicher, dass das Benutzerkonto im Office 365 Admin Center nicht auf der Seite **Aktive Benutzer**, sondern auf der Seite **Gelöschte Benutzer** aufgeführt wird.
- Verwenden Sie in Exchange Online PowerShell die folgende Syntax, um sicherzustellen, dass das Postfach gelöscht wurde.

```
Get-Mailbox <identity>
```

Der Befehl gibt einen Fehler zurück, der angibt, dass das Postfach nicht gefunden wurde. Dies bestätigt, dass das Postfach gelöscht wurde.

- Wenn Sie das Benutzerpostfach endgültig gelöscht haben, stellen Sie sicher, dass das Benutzerpostfach nicht mehr im Papierkorb von Azure Active Directory angezeigt wird.

## Wiederherstellen eines Benutzerpostfachs

Wenn Sie ein Postfach löschen, bleibt das Postfach und sämtliche Inhalte in Exchange Online bis zum Ablauf der Aufbewahrungszeit von 30 Tagen für das gelöschte Postfach erhalten. Nach 30 Tagen wird das Postfach endgültig gelöscht und kann nicht wiederhergestellt werden. Das Verfahren zum Wiederherstellen eines Postfachs hängt davon ab, ob das Postfach durch Löschen des Office 365-Benutzerkontos oder durch Entfernen der Exchange Online-Lizenz gelöscht wurde.

### Verwenden des Office 365 Admin Center zum Wiederherstellen eines Benutzerkontos

Wenn das Postfach durch Löschen des entsprechenden Office 365-Benutzerkontos gelöscht wurde, können Sie das Postfach wiederherstellen, indem Sie das Benutzerkonto im Office 365 Admin Center wiederherstellen.

Weitere Informationen zum Wiederherstellen eines Office 365-Benutzerkontos finden Sie unter [Löschen oder Wiederherstellen von Benutzern](#).

### Verwenden von Exchange Online PowerShell zum Wiederherstellen eines Benutzerkontos

Sie können vorläufig gelöschte Postfächer mithilfe des PowerShell-Cmdlets weiter unten wiederherstellen. Das folgende Cmdlet-Beispiel stellt das Postfach für Allie Bellew wieder her.

1. [Herstellen einer Verbindung mit Exchange Online mithilfe der Remote-PowerShell](#).
2. Führen Sie das Cmdlet **Rückgängig-SoftDeletedMailbox**.

```
Undo-SoftDeletedMailbox allieb@contoso.com -WindowsLiveID allieb@contoso.com -Password (ConvertTo-SecureString -String 'Pa$$word1' -AsPlainText -Force)
```

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie folgendermaßen vor, um sicherzustellen, dass Sie ein Postfach erfolgreich wiederhergestellt haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**. Das wiederhergestellte Postfach wird in der Postfachliste angezeigt.
- Klicken Sie auf **Aktualisieren** Wenn das Postfach zuerst nicht angezeigt wird.
- Verwenden Sie in Exchange Online PowerShell die folgende Syntax, um sicherzustellen, dass das Postfach wiederhergestellt wurde.

```
Get-Mailbox <Identity>
```

## Wiederherstellen eines Benutzers in einem Hybridszenario

Für Benutzerpostfächer in einer Hybrid-Szenario, wenn das Postfach vorläufig gelöscht wurde und der Azure active Directory-Benutzer, die dem Postfach zugeordnet wurde von Azure Active Directory Festplatte gelöscht wurde, können **New-MailboxRestoreRequest** zum Wiederherstellen der Postfach. [Konfigurieren von Office 365-Gruppen mit der lokale Exchange Hybrid](#) für Weitere Informationen zu lesen. Die Verfahren in diesem Abschnitt wird erläutert, wie das Postfach eines Benutzers vorläufig gelöschten wiederherstellen.

1. [Herstellen einer Verbindung mit Exchange Online mithilfe der Remote-PowerShell](#).
2. Führen Sie das folgende Cmdlet aus, um das vorläufig gelöschte Postfach zu identifizieren, das Sie wiederherstellen möchten.

```
Get-Mailbox -SoftDeletedMailbox | Select-Object Name,ExchangeGuid
```

Beachten Sie für das vorläufig gelöschte Postfach, das Sie wiederherstellen möchten den GUID-Wert (Sie können den Wert in Schritt 4 verwenden).

3. Erstellen eines neuen Postfachs Ziel für das wiederhergestellte Postfach an. Weitere Informationen finden Sie unter [Erstellen von Benutzerpostfächern in Exchange Online](#). Nachdem der Zielpostfach erstellt wurde, führen Sie den folgenden Befehl an den GUID-Wert, der das Zielpostfach abrufen, die Sie im nächsten Schritt benötigen.

```
Get-Mailbox -Identity <NameOrAliasOfNewTargetMailbox> | Format-List ExchangeGuid
```

4. Ersetzen Sie <SoftDeletedMailboxGUID> mit der GUID-Wert aus Schritt2 und <NewTargetMailboxGUID> mit der GUID-Wert aus Schritt 3, und führen Sie das folgende Cmdlet, um das Postfach wiederherzustellen:

```
New-MailboxRestoreRequest -SourceMailbox <SoftDeletedMailboxGUID> -TargetMailbox <NewTargetMailboxGUID>
```

## Lizenzenfernung

Informationen zum Entfernen einer Lizenz eines Benutzers in Office 365 und Exchange Online finden Sie unter [Änderung des Verhaltens für Benutzer ohne Exchange Online-Lizenz](#).

## Weitere Informationen

- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Verwalten von Benutzerpostfächern

18.12.2018 • 46 minutes to read

Nachdem Sie ein Benutzerpostfach erstellt haben, können Sie Änderungen vornehmen und mithilfe der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell zusätzliche Eigenschaften festlegen.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen dieser Aufgabe für jedes Benutzerpostfach: 2 bis 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berechtigungen für die Empfängerbereitstellung" im Thema [Mailbox Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern von Eigenschaften des Benutzerpostfachs

### Ändern von Benutzerpostfacheigenschaften mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Liste der Benutzerpostfächer, klicken Sie auf das Postfach, dem Sie die Eigenschaften ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Eigenschaftenseite des Postfachs können Sie die folgenden Eigenschaften ändern.

- **Allgemein**
- **Postfachnutzung**
- **Kontaktinformationen**
- **Organization (Organisation)**
- **E-Mail-Adresse**
- **Postfachfeatures**
- **Mitglied von**
- **E-Mail-Info**
- **Stellvertretung für Postfächer**

#### Allgemein

Klicken Sie auf den Abschnitt **Allgemein**, um grundlegende Informationen zum Benutzer anzuzeigen oder zu ändern.

- **Vorname, Initialen, Nachname**

- \*\*\* Namen\*\*: Dies ist der Name, der in Active Directory aufgeführt wird. Wenn Sie diesen Namen ändern, kann nicht die 64 Zeichen nicht überschreiten.
- \*\*\* Anzeigenamen\*\*: dieser Name erscheint im Adressbuch Ihrer Organisation, in der: und aus: Zeilen in e-Mail- und in der Liste der Postfächer. Dieser Name kann nicht leere Leerzeichen vor oder nach dem Anzeigenamen enthalten.
- \*\*\* Alias\*\*: Gibt den e-Mail-Alias für den Benutzer an. Alias des Benutzers ist der Teil der e-Mail-Adresse auf dem linken Rand der am (@) Symbol. Es muss in der Gesamtstruktur eindeutig sein.
- \*\*\* Benutzeranmeldenamen\*\*: Dies ist der Name, die der Benutzer So melden Sie sich mit ihrem Postfach und für die Anmeldung bei der Domäne verwendet. In der Regel Anmeldenamen des Benutzers besteht aus dem Alias des Benutzers auf der linken Seite des der @-Zeichen und den Namen der Domäne, in der sich das Benutzerkonto befindet, klicken Sie auf der rechten Seite des, dem @-Zeichen.

**NOTE**

In diesem Feld wird **Benutzer-ID** im Exchange Online mit der Bezeichnung.

- **Bei der nächsten Anmeldung kennwortänderung anfordern:** Aktivieren Sie dieses Kontrollkästchen, wenn das nächste Mal ihr Kennwort zurücksetzen der Anmeldung mit ihrem Postfach den Benutzer angezeigt werden soll.

**NOTE**

Dieses Kontrollkästchen ist nicht in Exchange Online verfügbar.

- **Ausblenden von Adresslisten:** Aktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass den Empfänger angezeigt werden, in dem Adressbuch und andere Adresslisten, die in Ihrer Exchange-Organisation definiert sind. Nachdem Sie dieses Kontrollkästchen aktivieren, können Benutzer weiterhin Nachrichten an den Empfänger senden mithilfe der e-Mail-Adresse.

Klicken Sie auf **Weitere Optionen**, um diese zusätzlichen Eigenschaften anzuzeigen oder zu ändern:

- **Organisationseinheit:** Dieses schreibgeschützte Feld zeigt die Organisationseinheit (OU), die das Benutzerkonto enthält. Sie müssen Active Directory-Benutzer und-Computer verwenden, um das Benutzerkonto in eine andere Organisationseinheit verschieben.

**NOTE**

Dieses Feld ist nicht in Exchange Online verfügbar.

- **Postfachdatenbank:** Dieses schreibgeschützte Feld zeigt den Namen der Postfachdatenbank an, der das Postfach hostet. Wenn das Postfach in eine andere Datenbank verschieben möchten, wählen Sie ihn in der Liste der Postfächer, und klicken Sie dann im Detailbereich auf **Postfach in eine andere Datenbank verschieben**.

**NOTE**

Diese Option ist nicht in Exchange Online verfügbar.

- **Benutzerdefinierte Attribute:** in diesem Abschnitt werden die benutzerdefinierten Attribute für das

Benutzerpostfach definiert ist. Um benutzerdefinierte Attributwerte anzugeben, klicken Sie auf **Bearbeiten**. Sie können bis zu 15 benutzerdefinierte Attribute für den Empfänger angeben.

#### Postfachnutzung

Verwenden Sie den Abschnitt **Postfachnutzung**, um das Postfachspeicherkontingent und die Aufbewahrungseinstellungen für gelöschte Elemente für das Benutzerpostfach anzuzeigen und zu ändern. Diese Einstellungen werden standardmäßig bei der Erstellung des Postfachs konfiguriert. Dabei werden die Werte verwendet, die für die Postfachdatenbank konfiguriert sind und für alle Postfächer in der Datenbank gelten. Sie können diese Einstellungen für jedes Postfach anpassen, anstatt die Standardwerte der Postfachdatenbank zu verwenden.

- **Letzte Anmeldung:** Dieses schreibgeschützte Feld zeigt die letzte Zeit, bei denen der Benutzer ihrem Postfach angemeldet.
- **Postfachnutzung:** in diesem Bereich werden die Gesamtgröße des Postfachs und der Prozentsatz der insgesamt Postfachkontingent, das verwendet wurde.

#### NOTE

Die Exchange-Verwaltungskonsole fragt die Postfachdatenbank ab, in der das Postfach gehostet wird, um die in diesem Feld angezeigten Informationen abzurufen. Wenn die Exchange-Verwaltungskonsole nicht mit dem Exchange-Speicher kommunizieren kann, der die Postfachdatenbank enthält, sind diese Felder leer. Eine Warnmeldung wird angezeigt, wenn sich der Benutzer noch nicht erstmalig beim Postfach angemeldet hat.

Klicken Sie auf **Weitere Optionen**, um das Speicherkontingent des Postfachs und die Einstellungen für die Aufbewahrungszeit für gelöschte Elemente für dieses Postfach anzuzeigen.

#### NOTE

In Exchange Online sind diese Einstellungen in der Exchange-Verwaltungskonsole nicht verfügbar.

- **Einstellungen für Speicherkontingente:** zum Anpassen dieser Einstellungen für das Postfach und die Standardwerte für Postfachdatenbank nicht verwenden, klicken Sie auf **Anpassen der Einstellungen für dieses Postfach**, geben Sie einen neuen Wert ein, und klicken Sie dann auf **Speichern**.

Der Wertebereich für alle Einstellungen für Speicherkontingente liegt zwischen 0 und 2047 GB.

- **Problem eine Warnung an (GB):** Dieses Feld zeigt den maximalen Speichergrenzwert, bevor dem Benutzer eine Warnung ausgegeben wird. Wenn die Größe des Postfachs erreicht oder den angegebenen Wert überschreitet, sendet Exchange eine Warnmeldung an den Benutzer.
  - **Senden verbieten ab (GB):** Dieses Feld zeigt den Kontingent senden Grenzwert für das Postfach an. Wenn die Größe des Postfachs erreicht oder den angegebenen Grenzwert überschreitet, Exchange verhindert, dass Benutzer keine neuen Nachrichten senden und eine beschreibende Fehlermeldung angezeigt.
  - **Senden und empfangen (GB) verbieten ab:** Dieses Feld zeigt das Senden verbieten ab und Grenzwert für das Postfach empfangen. Wenn die Größe des Postfachs erreicht oder den angegebenen Grenzwert überschreitet, Exchange verhindert, dass den Postfachbenutzer neue Nachrichten senden und werden keine neuen Nachrichten an das Postfach übermitteln. Alle Nachrichten, die an das Postfach gesendet werden mit einer beschreibenden Fehlermeldung an den Absender zurückgegeben.
- **Deleted Element beibehaltungseinstellungen:** zum Anpassen dieser Einstellungen für das Postfach und die Standardwerte für Postfachdatenbank nicht verwenden, klicken Sie auf **Anpassen der**

**Einstellungen für dieses Postfach**, geben Sie einen neuen Wert ein, und klicken Sie dann auf **Speichern**.

- **Gelöschte Objekte aufbewahren für (Tage)**: Dieses Feld zeigt die Zeitdauer, die gelöschte Objekte werden beibehalten, bevor sie endgültig gelöscht werden und können nicht wiederhergestellt werden, durch den Benutzer. Wenn das Postfach erstellt wird, basiert dieser Wert auf die gelöschte Elemente Beibehaltungseinstellungen für die Postfachdatenbank konfiguriert. Standardmäßig wird eine Postfachdatenbank so konfiguriert, dass gelöschte Elemente 14 Tage lang aufbewahrt. Der Wertebereich für diese Eigenschaft wird von 0 bis 24855 Tage.
- **Objekte, bis die Datenbank gesichert ist nicht dauerhaft löschen**: Aktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass Postfächer und e-Mail-Nachrichten erst gelöscht wird, nachdem die Postfachdatenbank auf dem sich das Postfach befindet gesichert wurde.

#### Kontaktinformationen

Verwenden Sie den Abschnitt **Kontaktinformationen**, um die Kontaktinformationen des Benutzers anzuzeigen oder zu ändern. Die Informationen auf dieser Seite werden im Adressbuch angezeigt. Klicken Sie auf **Weitere Optionen**, um zusätzliche Felder anzuzeigen.

##### TIP

Sie können das Feld **Bundesland/Kanton** verwenden, um Empfängerbedingungen für dynamische Verteilergruppen, Richtlinien für E-Mail-Adressen oder Adresslisten zu erstellen.

Postfachbenutzer können ihre eigenen Kontaktinformationen mit Outlook oder Outlook Web App anzeigen und ändern. Sie können jedoch nicht die Informationen in den Feldern **Notizen** und **Webseite** ändern.

#### Organization (Organisation)

Verwenden Sie den Abschnitt **Organisation**, um ausführliche Informationen zur Rolle des Benutzers in der Organisation aufzuzeichnen. Diese Informationen werden im Adressbuch angezeigt. Sie können auch ein virtuelles Organisationsdiagramm erstellen, auf das von E-Mail-Clients wie Outlook zugegriffen werden kann.

- **Titel**: Verwenden Sie dieses Feld zum Anzeigen oder Ändern der Titel des Empfängers.
- **Abteilung**: Verwenden Sie dieses Feld zum Anzeigen oder Ändern der Abteilung, in dem der Benutzer arbeitet. Verwenden Sie dieses Feld, um Empfängerbedingungen für dynamische Verteilergruppen, E-Mail-Adressrichtlinien oder Adresslisten zu erstellen.
- **Unternehmen**: Verwenden Sie dieses Feld zum Anzeigen oder Ändern des Unternehmens, für das der Benutzer arbeitet. Verwenden Sie dieses Feld, um Empfängerbedingungen für dynamische Verteilergruppen, E-Mail-Adressrichtlinien oder Adresslisten zu erstellen.
- **Manager**: Wenn einen Manager hinzufügen möchten, klicken Sie auf **Durchsuchen**. Wählen Sie im **Select Manager** eine Person aus, und klicken Sie dann auf **OK**.
- **Mitarbeiter**: In diesem Feld können nicht geändert werden. Ein direkter Mitarbeiter ist ein Benutzer, der einem bestimmten Vorgesetzten unterstellt. Wenn Sie einen Manager für den Benutzer angegeben haben, wird der Benutzer als Direct Bericht die Details des Postfachs des Managers angezeigt. Beispielsweise verwaltet Marlies Chris und Kate, Marlies' Postfach im Feld **Manager** Chris' Postfach- und Kates Postfach angegeben ist, und Chris und Kate werden im Feld **Mitarbeiter** in den Eigenschaften des Postfachs des Marlies angezeigt.

#### E-Mail-Adresse

Im Abschnitt **E-Mail-Adresse** können Sie die E-Mail-Adressen anzeigen und ändern, die dem Benutzerpostfach zugeordnet sind. Dazu gehören die primäre SMTP-Adresse des Benutzers sowie alle zugeordneten Proxyadressen. Die primäre SMTP-Adresse (auch als Standardantwortadresse bezeichnet) wird fettgedruckt in

der Adressliste angezeigt. Der Wert **SMTP** in der Spalte **Typ** wird dabei in Großbuchstaben angegeben.

- **Hinzufügen:** Klicken Sie auf **Add**  So fügen Sie eine neue e-Mail-Adresse für dieses Postfach hinzu. Wählen Sie eine der folgenden Adresstypen:
  - **SMTP:** Dies ist die Adresse. Klicken Sie auf diese Schaltfläche, und geben Sie dann die neue SMTP-Adresse in der \*\* \* E-Mail-Adresse\*\* Feld.
  - **EUM:** Adresse eines EUM (Exchange Unified Messaging) wird vom Microsoft Exchange Unified Messaging-Dienst verwendet, um die UM-aktivierten Benutzer in einer Exchange-Organisation zu suchen. EUM Adressen bestehen die Durchwahlnummer und die UM-Wähleinstellungen für den UM-aktivierten Benutzer. Klicken Sie auf diese Schaltfläche, und geben Sie im Feld **Adresse/Erweiterung** die Durchwahlnummer ein. Klicken Sie dann auf **Durchsuchen**, und wählen Sie einen Wählplan für den Benutzer aus.
  - **Benutzerdefinierte Adresstyp:** Klicken Sie auf diese Schaltfläche, und geben Sie einen der unterstützten nicht-SMTP-e-Mail-Adresstypen in der \*\* \* E-Mail-Adresse\*\* Feld.

**NOTE**

Mit Ausnahme von X.400-Adressen überprüft Exchange benutzerdefinierte Adressen nicht auf ordnungsgemäße Formatierung. Sie müssen sicherstellen, dass die von Ihnen angegebene benutzerdefinierte Adresse die Formatanforderungen für den jeweiligen Adresstyp erfüllt.

- **Die Antwortadresse machen:** In Exchange Online, Sie können wählen Sie dieses Kontrollkästchen, um das neue e-Mail-Adresse die primäre SMTP-Adresse für das Postfach zu machen. Dieses Kontrollkästchen nicht in der Exchange-Verwaltungskonsole in Exchange Server zur Verfügung.
- **E-Mail-Adressen basierend auf der e-Mail-Adressrichtlinie angewendet an diesen Empfänger automatisch aktualisieren:** Aktivieren Sie dieses Kontrollkästchen, um dem Empfänger der e-Mail-Adressen automatisch aktualisierte basierend auf Änderungen an e-Mail-Adressrichtlinien in Ihrer Organisation. Dieses Feld ist standardmäßig aktiviert.

**NOTE**

Dieses Kontrollkästchen ist nicht in Exchange Online verfügbar.

- **Diese Adresse als Antwortadresse verwenden**

#### **Postfachfeatures**

Im Abschnitt **Postfachfeatures** können Sie die folgenden Postfachfeatures und -einstellungen anzeigen oder ändern:

- **Freigaberichtlinie:** Dieses Feld zeigt die Freigaberichtlinie auf das Postfach angewendet. Eine Freigaberichtlinie zu steuert, wie Benutzer in Ihrer Organisation, Kalender und Kontaktinformationen für Benutzer außerhalb Ihrer Exchange-Organisation freigeben können. Die Standardfreigaberichtlinie wird bei der Erstellung Postfächer zugewiesen. Um die Freigaberichtlinie zu ändern, die dem Benutzer zugewiesen ist, wählen Sie aus der Dropdownliste eine andere aus.
- **Rollenzuweisungsrichtlinie:** Dieses Feld zeigt die rollenzuweisungsrichtlinie, das Postfach zugewiesen sind. Die rollenzuweisungsrichtlinie gibt die rollenbasierten Zugriffssteuerung (RBAC) Rollen, die dem Benutzer zugewiesen werden und steuern, was bestimmte Postfächer und Verteilerlisten Configuration Settings GruppenBenutzer ändern können. Um die Zuweisungsrichtlinie ändern, die dem Benutzer zugewiesen ist, wählen Sie aus der Dropdownliste eine andere.

- **Aufbewahrungsrichtlinie:** Dieses Feld zeigt die Aufbewahrungsrichtlinie an das Postfach zugewiesen. Eine Aufbewahrungsrichtlinie ist eine Gruppe von aufbewahrungstags, die auf das Postfach des Benutzers angewendet werden. Sie können Sie steuern, wie lange Elemente in den Postfächer der Benutzer lassen und definieren, welche Aktion für Elemente, die einem bestimmten Alter erreicht haben. Eine Aufbewahrungsrichtlinie wird nicht Postfächer bei der Erstellung zugewiesen. Wenn eine Aufbewahrungsrichtlinie für den Benutzer zuweisen möchten, wählen Sie aus der Dropdown Liste.
- **Adressbuchrichtlinie:** Dieses Feld zeigt die adressbuchrichtlinie an das Postfach angewendet. Eine adressbuchrichtlinie ermöglicht es Ihnen zu Segment Benutzer in bestimmten Gruppen können Sie benutzerdefinierte Ansichten des Adressbuchs bereitstellen. Zum Anwenden oder Ändern der adressbuchrichtlinie an das Postfach angewendet, wählen Sie aus der Dropdown Liste.
- **Unified Messaging:** dieses Feature ist standardmäßig deaktiviert. Wenn Sie Unified Messaging (UM) aktivieren, ist der Benutzer Ihrer Organisation UM Features verwenden können, und ein Standardsatz von UM-Eigenschaften auf den Benutzer angewendet werden. Klicken Sie auf **Aktivieren**, um UM für das Postfach zu aktivieren. Informationen dazu, wie Sie UM aktivieren finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).

**NOTE**

Bevor Sie UM aktivieren können, müssen ein UM-Wählplan und eine UM-Postfachrichtlinie vorhanden sein.

- **Mobile-Geräten:** Verwenden Sie diesen Bereich zum Anzeigen und Ändern der Einstellungen für Exchange ActiveSync, die standardmäßig aktiviert ist. Exchange ActiveSync ermöglicht den Zugriff auf ein Exchange-Postfach mithilfe eines mobilen Geräts. Klicken Sie auf **Exchange ActiveSync deaktivieren**, um dieses Feature für das Postfach zu deaktivieren.
- **Outlook Web App:** dieses Feature ist standardmäßig aktiviert. Outlook Web App ermöglicht den Zugriff auf ein Exchange-Postfach über einen Webbrowser. Klicken Sie auf **Deaktivieren**, um Outlook Web App für das Postfach zu deaktivieren. Klicken Sie auf **Bearbeiten der Details** zum Hinzufügen oder Ändern einer Outlook Web App-Postfachrichtlinie für das Postfach.
- **IMAP:** dieses Feature ist standardmäßig aktiviert. Klicken Sie auf **Deaktivieren**, um IMAP für das Postfach zu deaktivieren.
- **POP3:** dieses Feature ist standardmäßig aktiviert. Klicken Sie auf **Deaktivieren**, um POP3 für das Postfach zu deaktivieren.
- **MAPI:** dieses Feature ist standardmäßig aktiviert. MAPI ermöglicht den Zugriff auf ein Exchange-Postfach über einen MAPI-Client wie Outlook. Klicken Sie auf **Deaktivieren**, um MAPI für das Postfach zu deaktivieren.
- **Aufbewahrung für eventuelle Rechtsstreitigkeiten:** dieses Feature ist standardmäßig deaktiviert. Aufbewahrung für eventuelle Rechtsstreitigkeiten behält gelöschten Postfachs Elemente und Datensätze Änderungen an Postfachelemente. Gelöschte Elemente und alle Instanzen der geänderten Elemente werden in eine discoverysuche zurückgegeben. Klicken Sie auf **Aktivieren**, um das Postfach Rechtsstreitigkeiten gehalten wird. Wenn das Postfach beweissicherungsverfahren aktiviert ist, klicken Sie auf **Deaktivieren**, um die Aufbewahrung für eventuelle Rechtsstreitigkeiten zu entfernen. Postfächer beweissicherungsverfahren inaktiver Postfächer werden und können nicht gelöscht werden. Um das Postfach zu löschen, entfernen Sie die Aufbewahrung für eventuelle Rechtsstreitigkeiten. Wenn das Postfach beweissicherungsverfahren aktiviert ist, klicken Sie auf **Bearbeiten der Details** zum Anzeigen und ändern die folgenden Einstellungen der Aufbewahrung für eventuelle halten:
  - **Halten Sie Datum:** Dieses schreibgeschützte Feld gibt an, das Datum und Uhrzeit, wann wurde das Postfach beweissicherungsverfahren zu platzieren.

- **Halten von:** Dieses schreibgeschützte Feld gibt an, der Benutzer, der das Postfach Rechtsstreitigkeiten gehalten wird.
- **Hinweis:** Benachrichtigen des Benutzers über die Aufbewahrung für eventuelle Rechtsstreitigkeiten, wird erläutert, warum das Postfach beweissicherungsverfahren ist in diesem Feld können, oder geben Sie zusätzliche Anweisungen für den Benutzer, wie etwa informiert, dass die Aufbewahrung für eventuelle Rechtsstreitigkeiten die tägliche Verwendung von e-Mails beeinträchtigt.
- **URL:** in diesem Feld eine URL zu einer Website, die Informationen oder zum beweissicherungsverfahren bietet halten Sie für das Postfach bereitstellen können.

**NOTE**

Der Text in diesen Feldern wird im Postfach des Benutzers nur angezeigt, wenn dieser Outlook 2010 oder höher verwendet. In Outlook Web App oder anderen E-Mail-Clients wird die URL nicht angezeigt. Klicken Sie zum Anzeigen des Texts aus den Feldern **Hinweis** und **URL** in Outlook auf die Registerkarte **Datei**, und navigieren Sie auf der Seite Info zu Kontoeinstellungen.

- **Archivierung:** Wenn ein Archivpostfach für den Benutzer nicht vorhanden ist, ist dieses Feature deaktiviert. Um ein Archivpostfach zu aktivieren, klicken Sie auf **Aktivieren**. Wenn der Benutzer ein Archivpostfach, die Größe des archivpostfachs hat und Nutzungsstatistiken angezeigt werden. Klicken Sie auf **Bearbeiten der Details** zum Anzeigen und ändern die folgenden Archiv postfacheinstellungen:
  - **Status:** Dieses schreibgeschützte Feld gibt an, ob ein Archivpostfach vorhanden ist.
  - **Datenbank:** Dieses schreibgeschützte Feld zeigt den Namen der Postfachdatenbank an, die das Archivpostfach gehostet wird. Dieses Feld ist nicht verfügbar in Exchange Online.
  - **Name:** Geben Sie den Namen des archivpostfachs in dieses Feld ein. Dieser Name wird unter der Ordnerliste in Outlook oder Outlook Web App angezeigt.
  - **Archivierungskontingent (GB):** Dieses Feld zeigt die Gesamtgröße des archivpostfachs. Um die Größe zu ändern, geben Sie einen neuen Wert in das Feld, oder wählen Sie einen Wert aus der Dropdown-Liste.
  - **Warnung bei (GB):** Dieses Feld zeigt den maximalen Speichergrenzwert für das Archivpostfach, bevor dem Benutzer eine Warnung ausgegeben wird. Wenn Größe das Archivpostfach erreicht oder den angegebenen Wert überschreitet, sendet Exchange eine Warnmeldung an den Benutzer. Um diesen Grenzwert zu ändern, geben Sie einen neuen Wert in das Feld, oder wählen Sie einen Wert aus der Dropdown-Liste.

**NOTE**

In Exchange Online können Sie das Archivkontingent und das Kontingent für "Warnmeldung senden" für das Archivpostfach nicht ändern.

- **Optionen für die Übermittlung:** verwenden, um die forward-e-Mail-Nachrichten an den Benutzer an einen anderen Empfänger und die maximale Anzahl von Empfängern festlegen, die der Benutzer eine Nachricht senden kann. Klicken Sie auf **Details anzeigen**, um anzeigen und ändern Sie diese Einstellung.
  - **Weiterleitungsadresse:** Aktivieren Sie das Kontrollkästchen **Weiterleitung aktivieren**, und klicken Sie dann auf **Durchsuchen**, um die Seite **E-Mail-Benutzer auswählen und Postfach** anzuzeigen. Verwenden Sie diese Seite, um einen Empfänger auszuwählen, an die alle e-Mail-Nachrichten weiterleiten, die an dieses Postfach gesendet werden sollen.
  - **Nachricht an Weiterleitungsadresse und Postfach zu übermitteln:** Aktivieren Sie dieses

Kontrollkästchen, damit Nachrichten an die Weiterleitungsadresse und Postfach des Benutzers gespeichert werden.

- **Empfänger Grenzwert:** Diese Einstellung steuert die maximale Anzahl von Empfängern kann der Benutzer eine Nachricht zu senden. Aktivieren das Kontrollkästchen **Maximum Empfänger** zur Begrenzung der Anzahl der Empfänger im Feld an zulässig; Cc; und Bcc: Felder einer e-Mail-Nachrichten und geben Sie die maximale Anzahl von Empfängern.

**NOTE**

Für lokale Exchange-Organisationen ist die Empfängeranzahl unbegrenzt. Für Exchange Online-Organisationen ist die Anzahl auf 500 Empfänger begrenzt.

- **Nachricht Größeneinschränkungen:** Diese Einstellungen steuern die Größe von Nachrichten, die der Benutzer senden und empfangen kann. Klicken Sie auf **Details anzeigen**, zum Anzeigen und ändern die maximale Größe für gesendete und empfangene Nachrichten.

**NOTE**

Diese Einstellungen können in Exchange Online nicht geändert werden.

- **Gesendete Nachrichten:** zum Angeben der maximal zulässigen Größe für diesen Benutzer gesendeten Nachrichten aktivieren Sie das Kontrollkästchen **maximale Nachrichtengröße (KB)**, und geben Sie einen Wert in das Feld ein. Die Nachrichtengröße muss zwischen 0 und 2.097.151 KB sein. Wenn der Benutzer eine Nachricht größer als die angegebene Größe sendet, wird die Nachricht mit einer beschreibende Fehlermeldung an den Benutzer zurückgegeben werden soll.
- **Empfangene Nachrichten:** um eine maximale Größe für Nachrichten, die von diesem Benutzer angeben, aktivieren Sie das Kontrollkästchen **maximale Nachrichtengröße (KB)**, und geben Sie einen Wert in das Feld ein. Die Nachrichtengröße muss zwischen 0 und 2.097.151 KB sein. Wenn der Benutzer eine Nachricht größer als die angegebene Größe empfängt, wird die Nachricht mit einer beschreibende Fehlermeldung an den Absender zurückgegeben werden soll.

- **Nachricht Delivery Restrictions:** Diese Einstellungen steuern Sie, wer e-Mail-Nachrichten an diesen Benutzer senden kann. Klicken Sie auf **Details anzeigen**, um anzeigen und ändern diese Beschränkungen.

- **Nachrichten annehmen von:** Verwenden Sie diesen Abschnitt, um anzugeben, wer Nachrichten an diesen Benutzer senden kann.
- **Alle Absender:** Wählen Sie diese Option, um anzugeben, dass der Benutzer Nachrichten von allen Absendern annehmen kann. Dazu gehören sowohl Absender in Ihrer Exchange-Organisation und externe Absender. Diese Option ist standardmäßig aktiviert. Diese Option umfasst externe Benutzer nur, wenn Sie das Kontrollkästchen **erforderlich, dass die Authentifizierung aller Absender anfordern** deaktivieren. Wenn Sie dieses Kontrollkästchen aktivieren, werden Nachrichten von externen Benutzern abgelehnt.
- **Nur Absender in der folgenden Liste:** Wählen Sie diese Option, um anzugeben, dass der Benutzer Nachrichten nur von einer bestimmten Gruppe von Absendern in Ihrer Exchange-Organisation akzeptieren kann. Klicken Sie auf **Hinzufügen**  die Seite **Wählen Sie Empfänger** angezeigt werden, die eine Liste aller Empfänger in Ihrer Exchange-Organisation angezeigt wird. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen** .

- **Erfordern, dass alle Absender authentifiziert werden:** Wählen Sie diese Option aus, um zu verhindern, dass anonyme Benutzer Nachrichten an die Benutzer senden können.
- **Nachrichten ablehnen von:** Verwenden Sie diesen Abschnitt zu hindern, Nachrichten an diesen Benutzer zu senden.
- **Kein Absender:** Wählen Sie diese Option, um anzugeben, dass das Postfach ablehnen von Nachrichten von beliebigen Absendern in der Exchange-Organisation wird nicht aus. Diese Option ist standardmäßig aktiviert.
- **Absender in der folgenden Liste:** Wählen Sie diese Option, um anzugeben, dass das Postfach ablehnen von Nachrichten von einer bestimmten Gruppe von Absendern in Ihrer Exchange-Organisation wird. Klicken Sie auf **Hinzufügen** [ ] die Seite **Wählen Sie Empfänger** angezeigt werden, die eine Liste aller Empfänger in Ihrer Exchange-Organisation angezeigt wird. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen** [ ].

#### **Mitglied von**

Im Abschnitt **Mitglied von** können Sie eine Liste der Verteiler- oder Sicherheitsgruppen anzeigen, denen dieser Benutzer angehört. Informationen zur Mitgliedschaft können auf dieser Seite nicht geändert werden. Beachten Sie, dass der Benutzer möglicherweise den Kriterien für mindestens eine dynamische Verteilergruppe in Ihrer Organisation entspricht. Dynamische Verteilergruppen werden auf dieser Seite jedoch nicht angezeigt, da ihre Mitgliedschaft zum Zeitpunkt ihrer Verwendung stets neu berechnet wird.

#### **E-Mail-Info**

Verwenden Sie den Abschnitt **E-Mail-Info**, um eine E-Mail-Info hinzuzufügen, mit der Benutzer auf potenzielle Probleme beim Senden einer Nachricht an diesen Empfänger hingewiesen werden. Eine E-Mail-Info ist Text, der in der Infoleiste angezeigt wird, wenn dieser Empfänger dem Feld "An", "Cc" oder "Bcc" einer neuen E-Mail hinzugefügt wird.

#### **NOTE**

Eine E-Mail-Info kann HTML-Tags enthalten, Skripts sind jedoch nicht zulässig. Die Länge einer benutzerdefinierten E-Mail-Info darf 175 angezeigte Zeichen nicht überschreiten. HTML-Tags werden bei diesem Zeichenlimit nicht mitgezählt.

#### **Stellvertretung für Postfächer**

Verwenden Sie den Abschnitt **Stellvertretung für Postfächer**, um es anderen Benutzern (einer Stellvertretung) zu ermöglichen, sich im Namen eines Benutzers am Benutzerpostfach anzumelden oder Nachrichten zu senden. Sie können die folgenden Berechtigungen zuweisen:

- **Senden als:** mit dieser Berechtigung können Benutzer, die nicht der Postfachbesitzer das Postfach zum Senden von Nachrichten verwenden. Nachdem diese Berechtigung Stellvertreter zugewiesen ist, wird jede Nachricht, die eine Stellvertretung aus diesem Postfach gesendet angezeigt, als wäre es von der Postfachbesitzer gesendet wurde. Mit dieser Berechtigung kann jedoch keine Stellvertretung das Postfach des Benutzers anmelden.
- **Senden im Auftrag von:** mit dieser Berechtigung können auch eine Stellvertretung dieses Postfach zum Senden von Nachrichten verwenden. Jedoch, nachdem diese Berechtigung eine Stellvertretung zugeordnet ist die **aus:** Adresse in jeder Nachricht, die von der Stellvertretung gesendet gibt an, dass die Nachricht vom Delegaten im Namen der Postfachbesitzer gesendet wurde.
- **Vollzugriff:** Diese Berechtigung ermöglicht es einer Stellvertretung, melden Sie sich beim Postfach des Benutzers und der Inhalt des Postfachs angezeigt. Jedoch, nachdem diese Berechtigung Stellvertreter zugewiesen ist, kann nicht die Stellvertretung Nachrichten aus dem Postfach senden. Damit eine

Stellvertretung senden von e-Mails aus dem Postfach des Benutzers kann, müssen Sie dennoch der Stellvertretung senden als "oder" Senden im Auftrag Berechtigung zuweisen.

Klicken Sie auf **Hinzufügen**, um Stellvertretungen Berechtigungen zuzuweisen, [ ] wählen Sie die entsprechende Berechtigung zum Anzeigen einer Seite, die eine Liste aller Empfänger in Ihrer Exchange-Organisation anzeigt, die die Berechtigung zugewiesen werden können. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen** [ ].

### Verwenden von Exchange Online PowerShell so ändern Sie die Eigenschaften von Benutzerpostfächern

Verwenden Sie die Cmdlets **Get-Mailbox** und **Set-Mailbox**, anzeigen und Ändern der Eigenschaften für Benutzerpostfächer. Ein Vorteil von Exchange Online PowerShell ist die Möglichkeit zum Ändern der Eigenschaften für mehrere Postfächer. Informationen dazu, welche Parameter Postfacheigenschaften entsprechen finden Sie unter den folgenden Themen:

- [Get-Mailbox](#)
- [Set-Mailbox](#)

Es folgen einige Beispiele der Verwendung von Exchange Online PowerShell zum Ändern von Eigenschaften des Benutzerpostfachs.

In diesem Beispiel wird gezeigt, wie die E-Mails für Pat Coleman an das Postfach von Sunil Koduri (sunilk@contoso.com) weitergeleitet werden können.

```
Set-Mailbox -Identity patc -DeliverToMailboxAndForward $true -ForwardingAddress sunilk@contoso.com
```

In diesem Beispiel wird der Befehl **Get-Mailbox** verwendet, um alle Benutzerpostfächer in der Organisation zu finden, und dann wird mit dem Befehl **Set-Mailbox** der Empfängergrenzwert auf 500 zulässige Empfänger in den Zeilen "An:", "Cc:" und "Bcc:" einer E-Mail-Nachricht festgelegt.

```
Get-Mailbox -ResultSize unlimited -Filter {((RecipientTypeDetails -eq 'UserMailbox'))} | Set-Mailbox -RecipientLimits 500
```

In diesem Beispiel wird mithilfe des Befehls **Get-Mailbox** nach allen Postfächern in der Organisationseinheit "Marketing" gesucht. Anschließend werden diese Postfächer mit dem Befehl **Set-Mailbox** konfiguriert. Die Grenzwerte für benutzerdefinierte Warnungen, Sendeverbote sowie Sende- und Empfangsverbote werden entsprechend auf 200 MB, 250 MB und 280 MB festgelegt. Die Standardgrenzwerte der Postfachdatenbank werden ignoriert. Mit diesem Befehl können Sie für eine bestimmte Gruppe von Postfächern höhere oder niedrigere Grenzwerte als für andere Postfächer in der Organisation festlegen.

```
Get-Mailbox -OrganizationalUnit "Marketing" | Set-Mailbox -IssueWarningQuota 209715200 -ProhibitSendQuota 262144000 -ProhibitSendReceiveQuota 293601280 -UseDatabaseQuotaDefaults $false
```

In diesem Beispiel werden mit dem Cmdlet **Get-Mailbox** alle Benutzer in der Kundendienstabteilung gesucht. Anschließend wird mit dem Cmdlet **Set-Mailbox** die maximale Nachrichtengröße für das Senden von Nachrichten auf 2 MB festgelegt.

```
Get-Mailbox -Filter "Department -eq 'Customer Service'" | Set-Mailbox -MaxSendSize 2097152
```

In diesem Beispiel wird QuickInfo-Übersetzung auf Französisch und Chinesisch eingestellt.

```
Set-Mailbox john@contoso.com -MailTipTranslations ("FR: C'est la langue française", "CHT: 這是漢語語言")
```

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie folgendermaßen vor, um zu überprüfen, ob die Eigenschaften eines Benutzerpostfachs erfolgreich geändert wurden:

- In der Exchange-Verwaltungskonsole, wählen Sie das Postfach aus, und klicken Sie dann auf **Bearbeiten** [ ] anzeigen, die Eigenschaft oder Funktion, die Sie geändert haben. Je nach der Eigenschaft, die Sie geändert haben, kann es im Bereich Details für das ausgewählte Postfach angezeigt werden.
- Verwenden Sie das Cmdlet **Get-Mailbox** in Exchange Online PowerShell um die Änderungen zu überprüfen. Ein Vorteil von Exchange Online PowerShell ist, dass Sie mehrere Eigenschaften für mehrere Postfächer anzeigen können. Führen Sie im Beispiel oben, in dem die Empfängerzahl geändert wurde den folgenden Befehl zum Überprüfen des neuen Werts.

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | Format-List Name,RecipientLimits
```

Führen Sie diesen Befehl für das vorherige Beispiel aus, in dem die Nachrichtengrenzwerte geändert wurden.

```
Get-Mailbox -OrganizationalUnit "Marketing" | Format-List Name,IssueWarningQuota,ProhibitSendQuota,ProhibitSendReceiveQuota,UseDatabaseQuotaDefaults
```

## Massenbearbeitung von Benutzerpostfächern

Sie können mithilfe der Exchange-Verwaltungskonsole die Eigenschaften mehrerer Benutzerpostfächer ändern. Wenn Sie in der Exchange-Verwaltungskonsole mindestens zwei Benutzerpostfächer aus der Postfachliste auswählen, werden die Eigenschaften im Detailbereich angezeigt, die per Massenbearbeitung geändert werden können. Wenn Sie eine dieser Eigenschaften ändern, wird die Änderungen auf alle ausgewählten Postfächer angewendet.

Es folgt eine Liste der Eigenschaften und Funktionen von Benutzerpostfächern, für die eine Massenbearbeitung möglich ist. Beachten Sie, dass nicht alle Eigenschaften in jedem Bereich geändert werden können.

- **Kontaktinformationen:** Ändern Sie freigegebene Eigenschaften wie Straße, PLZ und Ort.
- **Organisation:** Ändern Sie freigegebene Eigenschaften wie Abteilungsname, Firmenname und den Manager, die an die ausgewählten Benutzer Berichten.
- **Benutzerdefinierte Attribute:** ändern oder Hinzufügen von Werten für benutzerdefinierte Attribute 1 – 15.
- **Postfachkontingent:** Ändern Sie die Kontingentwerte Postfach und die Aufbewahrungszeit für gelöschte Objekte. Dies ist nicht verfügbar in Exchange Online.
- **E-Mail-Konnektivität:** Aktivieren oder Deaktivieren von Outlook Web App, POP3, IMAP, MAPI und Exchange ActiveSync.
- **Archiv:** Aktivieren oder deaktivieren Sie das Archivpostfach.
- **Aufbewahrungsrichtlinie, rollenzuweisungsrichtlinie, und Freigaberichtlinie:** Aktualisieren Sie die Einstellungen für jede dieser Postfachfunktionen.

- **Verschieben von Postfächern in eine andere Datenbank:** die ausgewählten Postfächer in eine andere Datenbank verschieben.
- **Berechtigungen der Stellvertretung:** Zuweisen von Berechtigungen zu Benutzern oder Gruppen, die sie zum Öffnen oder Senden von Nachrichten aus anderen Postfächern zulassen. Sie können weisen Sie vollständig, senden als und Senden im Auftrag von Berechtigungen auf Benutzer oder Gruppen. Checken Sie [Berechtigungen verwalten für Empfänger](#) für weitere Details.

#### NOTE

Die geschätzte Zeit bis zum Abschließen dieser Aufgabe sind 2 Minuten, aber dies kann länger dauern, wenn Sie mehrere Eigenschaften oder Funktionen ändern.

### Massenbearbeitung von Benutzerpostfächern mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Wählen Sie in der Liste der Postfächer mindestens zwei Postfächer aus.

#### TIP

Sie können mehrere benachbarte Postfächer auswählen, indem Sie bei gedrückter UMSCHALTTASTE auf das erste und anschließend auf das letzte zu bearbeitende Postfach klicken. Sie können auch mehrere nicht benachbarte Postfächer auswählen, indem Sie bei gedrückter STRG-TASTE auf die gewünschten Postfächer klicken.

3. Wählen Sie im Detailbereich unter **Massenbearbeitung** die Postfacheigenschaften oder -funktion aus, die Sie bearbeiten möchten.
4. Nehmen Sie die Änderungen auf der Eigenschaftenseite vor, und speichern Sie Ihre Änderungen.

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie folgendermaßen vor, um die erfolgreiche Massenbearbeitung von Benutzerpostfächern zu überprüfen:

- In der Exchange-Verwaltungskonsole, wählen Sie die einzelnen Postfächer, die Sie Massen bearbeitet, und klicken Sie dann auf **Bearbeiten** [ ] anzeigen, die Eigenschaft oder Funktion, die Sie geändert haben.
- Verwenden Sie das Cmdlet **Get-Mailbox** in Exchange Online PowerShell um die Änderungen zu überprüfen. Ein Vorteil von Exchange Online PowerShell ist, dass Sie mehrere Eigenschaften für mehrere Postfächer anzeigen können. Angenommen Sie, dass Sie die Bearbeitungsfunktion Massen in der Exchange-Verwaltungskonsole zum aktivieren das Archivpostfach und weisen Sie eine Aufbewahrungsrichtlinie für alle Benutzer in Ihrer Organisation verwendet. Um diese Änderungen zu überprüfen, könnten Sie den folgenden Befehl ausführen:

```
Get-Mailbox -ResultSize unlimited -Filter {{RecipientTypeDetails -eq 'UserMailbox')} | Format-List Name,ArchiveDatabase,RetentionPolicy
```

Weitere Informationen zu den verfügbaren Parametern für das Cmdlet **Get-Mailbox** finden Sie unter [Get-Mailbox](#).

# Hinzufügen oder Entfernen von E-Mail-Adressen für ein Postfach

18.12.2018 • 11 minutes to read

Sie können mehrere e-Mail-Adresse für dasselbe Postfach konfigurieren. Die zusätzlichen Adressen werden Proxyadressen bezeichnet. Eine Proxyadresse ermöglicht dem Benutzer die e-Mails erhalten, die an eine andere e-Mail-Adresse gesendet wird. Alle e-Mail-Nachricht an Weiterleitungsadresse des Benutzers gesendet wird, deren primäre e-Mail-Adresse, auch bekannt als die primäre SMTP-Adresse ist oder die Standard-Antwortadresse übermittelt.

## IMPORTANT

Wenn Sie Office 365 für Unternehmen verwenden, sollten Sie hinzufügen oder Entfernen von e-Mail-Adressen für Benutzerpostfächer in [einen anderen e-Mail-Alias für einen Benutzer hinzufügen](#)

Eine Aufstellung weiterer Aufgaben im Rahmen der Empfängerverwaltung finden Sie in der Tabelle „Empfängerdokumentation“ im Artikel [Recipients](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Die geschätzte Zeit zum Ausführen der einzelnen Verfahren beträgt 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie müssen finden Sie unter dem Abschnitt "Empfängerbereitstellungsberechtigungen" im Thema [Recipients Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

Anhand der Verfahren in diesem Thema wird das Hinzufügen und Entfernen von E-Mail-Adressen für ein Benutzerpostfach erläutert. Mithilfe ähnlicher Verfahren können Sie E-Mail-Adressen für andere Empfängertypen hinzufügen oder entfernen.

## Hinzufügen einer E-Mail-Adresse zu einem Benutzerpostfach

### Hinzufügen einer E-Mail-Adresse mithilfe der Exchange-Verwaltungskonsole

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
- In der Liste der Benutzerpostfächer, klicken Sie auf das Postfach, dem Sie eine e-Mail-Adresse hinzufügen möchten, und klicken Sie dann auf **Bearbeiten**.
- Klicken Sie auf der Eigenschaftenseite des Postfachs auf **E-Mail-Adresse**.

## NOTE

Auf der Seite **E-Mail-Adresse** wird die primäre SMTP-Adresse fett gedruckt in der Adressenliste und dem groß geschriebenen Wert **SMTP** in der Spalte **Typ** angezeigt.

- Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **SMTP**, um eine SMTP-e-Mail-Adresse für dieses Postfach hinzuzufügen.

#### NOTE

SMTP ist der Standard-E-Mail-Adresstyp. Sie können einem Postfach auch Exchange Unified Messaging (EUM)- oder benutzerdefinierte Adressen hinzufügen. Weitere Informationen finden Sie unter "Ändern der Eigenschaften von Benutzerpostfächern" im Thema [Manage user mailboxes](#).

5. Geben Sie die neue SMTP-Adresse in das Feld **E-Mail-Adresse** ein, und klicken Sie dann auf **OK**.

Die neue Adresse wird in der Liste der E-Mail-Adressen für das ausgewählte Postfach angezeigt.

6. Klicken Sie zum Speichern der Änderung auf **Speichern**.

#### Verwenden von Exchange Online PowerShell zum Hinzufügen einer e-Mail-Adresse

Die einem Postfach zugeordneten E-Mail-Adressen sind in der Eigenschaft *EmailAddresses* des Postfachs enthalten. Da mehrere E-Mail-Adressen enthalten sein können, ist die Eigenschaft *EmailAddresses* eine sog. mehrwertige Eigenschaft. Die folgenden Beispiele veranschaulichen verschiedene Möglichkeiten, eine mehrwertige Eigenschaft zu ändern.

Dieses Beispiel zeigt, wie eine SMTP-Adresse dem Postfach von Dan Jump hinzugefügt wird.

```
Set-Mailbox "Dan Jump" -EmailAddresses @{add="dan.jump@northamerica.contoso.com"}
```

Dieses Beispiel zeigt, wie mehrere SMTP-Adressen einem Postfach hinzugefügt werden.

```
Set-Mailbox "Dan Jump" -EmailAddresses @{add="dan.jump@northamerica.contoso.com", "danh@tailspintoys.com"}
```

Weitere Informationen zu dieser Methode zum Hinzufügen oder Entfernen von Werten bei mehrwertigen Eigenschaften finden Sie unter [Modifying Multivalued Properties](#).

Dieses Beispiel zeigt, wie Sie e-Mail-Adressen an ein Postfach hinzufügen, indem Sie alle Adressen, die dem Postfach zugeordnete. In diesem Beispiel wird die danh@tailspintoys.com die neue e-Mail-Adresse, die Sie hinzufügen möchten. Die anderen beiden e-Mail-Adressen werden vorhandene Adressen. Die Adresse mit der Groß-/Kleinschreibung beachtet Qualifizierer **SMTP** ist die primäre SMTP-Adresse. Sie müssen alle e-Mail-Adressen für das Postfach einschließen, wenn Sie diese Befehlssyntax verwenden. Wenn dies nicht der Fall, werden die Adressen im Befehl angegeben die vorhandenen Adressen überschrieben.

```
Set-Mailbox "Dan Jump" -EmailAddresses  
SMTP:dan.jump@contoso.com,dan.jump@northamerica.contoso.com,danh@tailspintoys.com
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailbox](#).

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um das erfolgreiche Hinzufügen einer E-Mail-Adresse zu einem Postfach zu überprüfen:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**, klicken Sie auf das Postfach, und klicken Sie dann auf **Bearbeiten**.
- Klicken Sie auf der Eigenschaftenseite des Postfachs auf **E-Mail-Adresse**.
- Prüfen Sie in der Liste der E-Mail-Adressen für das Postfach, ob die neue E-Mail-Adresse enthalten ist.

oder -

- Führen Sie den folgenden Befehl in Exchange Online PowerShell.

```
Get-Mailbox <identity> | Format-List EmailAddresses
```

- Stellen Sie sicher, dass die neue E-Mail-Adresse in den Ergebnissen enthalten ist.

## Entfernen einer E-Mail-Adresse aus einem Benutzerpostfach

### Entfernen einer E-Mail-Adresse mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Liste der Benutzerpostfächer, klicken Sie auf das Postfach, dem Sie eine e-Mail-Adresse aus entfernen möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **E-Mail-Adresse**.
4. In der Liste der e-Mail-Adressen, wählen Sie die Adresse, die Sie entfernen möchten, und klicken Sie dann auf **Entfernen**.
5. Klicken Sie zum Speichern der Änderung auf **Speichern**.

### Verwenden Sie Exchange Online PowerShell, um eine e-Mail-Adresse zu entfernen.

Dieses Beispiel zeigt, wie eine E-Mail-Adresse aus dem Postfach von Janet Schorr entfernt wird.

```
Set-Mailbox "Janet Schorr" -EmailAddresses @{remove="janets@corp.contoso.com"}
```

Dieses Beispiel zeigt, wie mehrere Adressen aus einem Postfach entfernt werden.

```
Set-Mailbox "Janet Schorr" -EmailAddresses @{remove="janet.schorr@corp.contoso.com","janets@tailspintoys.com"}
```

Weitere Informationen zu dieser Methode zum Hinzufügen oder Entfernen von Werten bei mehrwertigen Eigenschaften finden Sie unter [Modifying Multivalued Properties](#).

Sie können eine E-Mail-Adresse auch entfernen, indem Sie sie im Befehl zum Festlegen von E-Mail-Adressen für ein Postfach weglassen. Angenommen, das Postfach von Janet Schorr hat drei E-Mail-Adressen: janets@contoso.com (die primäre SMTP-Adresse), janets@corp.contoso.com und janets@tailspintoys.com. Um die Adresse janets@corp.contoso.com zu entfernen, müssen Sie den folgenden Befehl ausführen.

```
Set-Mailbox "Janet Schorr" -EmailAddresses SMTP:janets@contoso.com,janets@tailspintoys.com
```

Da janets@corp.contoso.com im vorherigen Befehl weggelassen wurde, wird die Adresse aus dem Postfach entfernt.

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailbox](#).

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um das erfolgreiche Entfernen einer E-Mail-Adresse aus einem Postfach zu überprüfen:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**, klicken Sie auf das Postfach, und klicken Sie dann auf **Bearbeiten**.
- Klicken Sie auf der Eigenschaftenseite des Postfachs auf **E-Mail-Adresse**.

- Prüfen Sie in der Liste der E-Mail-Adressen für das Postfach, ob die E-Mail-Adresse fehlt.

oder -

- Führen Sie den folgenden Befehl in Exchange Online PowerShell.

```
Get-Mailbox <identity> | Format-List EmailAddresses
```

- Vergewissern Sie sich, dass die E-Mail-Adresse nicht in der Ausgabe aufgeführt ist.

## Verwenden von Exchange Online PowerShell, e-Mail-Adressen auf mehrere Postfächer hinzufügen

Sie können eine neue e-Mail-Adresse auf mehrere Postfächer gleichzeitig mithilfe von Exchange Online PowerShell und ein Komma getrennt, Wertetabelle (CSV) hinzufügen.

In diesem Beispiel werden Daten aus "C:\Users\Administrator\Desktop\AddEmailAddress.csv" importiert, die das folgende Format haben.

```
Mailbox,NewEmailAddress
Dan Jump,danj@northamerica.contoso.com
David Pelton,davidp@northamerica.contoso.com
Kim Akers,kima@northamerica.contoso.com
Janet Schorr,janets@northamerica.contoso.com
Jeffrey Zeng,jeffreyz@northamerica.contoso.com
Spencer Low,spencerl@northamerica.contoso.com
Toni Poe,tonip@northamerica.contoso.com
...
...
```

Führen Sie den folgenden Befehl aus, um mithilfe der Daten in der CSV-Datei die E-Mail-Adressen jedem in der CSV-Datei angegebenen Postfach hinzuzufügen.

```
Import-Csv "C:\Users\Administrator\Desktop\AddEmailAddress.csv" | ForEach {Set-Mailbox $_.Mailbox -EmailAddresses @{$add=$_.NewEmailAddress}}
```

### NOTE

Die Spaltennamen in der ersten Zeile der CSV-Datei ( `Mailbox,NewEmailAddress` ) sind willkürlich. Was Sie für Spaltennamen verwenden, stellen Sie sicher, dass Sie die gleichen Spaltennamen in Exchange Online PowerShell-Befehl verwenden.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um das erfolgreiche Hinzufügen einer E-Mail-Adresse zu mehreren Postfächern zu überprüfen:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**, klicken Sie auf ein Postfach, das Sie die Adresse hinzugefügt haben, und klicken Sie dann auf **Bearbeiten**.
- Klicken Sie auf der Eigenschaftenseite des Postfachs auf **E-Mail-Adresse**.
- Prüfen Sie in der Liste der E-Mail-Adressen für das Postfach, ob die neue E-Mail-Adresse enthalten ist.

oder -

- Führen Sie den folgenden Befehl in Exchange Online PowerShell, verwenden die gleiche CSV-Datei, die Sie zum Hinzufügen der neuen e-Mail-Adresse verwendet.

```
Import-Csv "C:\Users\Administrator\Desktop\AddEmailAddress.csv" | ForEach {Get-Mailbox $_.Mailbox | Format-List Name,EmailAddresses}
```

- Stellen Sie sicher, dass die neue E-Mail-Adresse in den Ergebnissen für jedes Postfach enthalten ist.

**TIP**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Ändern des Aufbewahrungszeitraums für gelöschte Elemente für ein Exchange Online-Postfach

18.12.2018 • 6 minutes to read

Wenn Sie haben ein Objekt in Microsoft Outlook oder Outlook im Web (vormals Outlook Web App) *dauerhaft* gelöscht, das Element wird in einen Ordner verschoben ( **Wiederherstellbare Elemente > Löschgänge** ) und 14 Tagen standardmäßig dort abgelegt. Sie können ändern, wie lange Elemente werden beibehalten, bis auf ein Maximum von 30 Tagen.

## NOTE

Sie müssen Exchange Online PowerShell verwenden, um die Änderung vorzunehmen. Leider möglich derzeit dies direkt in der Outlook oder Outlook im Web nicht.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 3 Minuten.
- Wenn Sie für ein Postfach **In-Place Hold and Litigation Hold** aktivieren möchten, damit dieser Grenzwert für die Aufbewahrung ignoriert wird, ist für das Postfach eine Exchange Online (Plan 2)-Benutzerlizenz erforderlich.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berechtigungen für die Empfängerbereitstellung" im Thema [Mailbox Permissions](#).
- Sie können nur Exchange Online PowerShell verwenden, um dieses Verfahren ausführen. So verwenden Sie Windows PowerShell für die Verbindung zu Exchange Online finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern des Aufbewahrungszeitraums für gelöschte Elemente

In den folgenden Beispielen wird die Aufbewahrungsduer auf 30 Tage erhöht, d. h. die maximale Aufbewahrungsduer für Exchange Online-Postfächer. Sie können den Aufbewahrungszeitraum beliebig bis zu diesem Grenzwert festlegen.

**Beispiel 1:** für das Postfach festlegen Emily Maier des gelöschten Elemente 30 Tage lang aufbewahrt werden sollen. Führen Sie in Exchange Online PowerShell den folgenden Befehl ein.

```
Set-Mailbox -Identity "Emily Maier" -RetainDeletedItemsFor 30
```

**Beispiel 2:** Legen Sie alle Benutzerpostfächer in der Organisation für die gelöschten Elemente 30 Tage lang aufbewahrt werden sollen. Führen Sie in Exchange Online PowerShell den folgenden Befehl ein.

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | Set-Mailbox -RetainDeletedItemsFor 30
```

Benötigen Sie weitere Informationen zur Verwendung dieser Befehle? Finden Sie unter Exchange Online PowerShell-Hilfethema [Set-Mailbox](#).

#### TIP

Sie möchten gelöschte Elemente länger als 30 Tage aufzubewahren? Platzieren Sie hierfür das Postfach in einem In-Situ-Speicher, oder aktivieren das Beweissicherungsverfahren. Dies funktioniert, da gelöschte Elemente beibehalten und Aufbewahrungseinstellungen für gelöschte Elemente ignoriert werden, wenn ein Postfach der Aufbewahrungspflicht unterliegt. Informationen dazu finden Sie unter [In-Place Hold and Litigation Hold](#).

## Überprüfen der Wertänderung

Führen Sie zum Überprüfen dieser Wertänderung für ein Postfach den folgenden Befehl aus:

```
Get-Mailbox <Name> | Format-List RetainDeletedItemsFor
```

Oder führen Sie zum Überprüfen dieser Wertänderung für alle Postfächer den folgenden Befehl aus:

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | Format-List Name,RetainDeletedItemsFor
```

## Weitere Informationen zu gelöschten Elementen und zur Aufbewahrungsdauer

Wenn ein Benutzer ein Postfachelement (z. B. eine E-Mail-Nachricht, einen Kontakt, einen Kalendertermin oder eine Aufgabe) in Microsoft Outlook und Outlook Web App dauerhaft löscht, wird das Element in den Ordner **Wiederherstellbare Elemente** und in einen Unterordner mit dem Namen **Löschvorgänge** verschoben.

Ein Postfachelement wird gelöscht und in den Ordner **Wiederherstellbare Elemente** verschoben, wenn ein Benutzer eine der folgenden Aktionen durchführt:

- Löschen eines Elements aus dem Ordner „Gelöschte Elemente“
- Leeren des Ordners „Gelöschte Elemente“
- Dauerhaftes Löschen eines Elements durch Auswählen des Elements und Drücken von **UMSCHALT+ENTF**

Wie lange gelöschte Elemente aufbewahrt werden in der **Löschvorgänge** Ordner hängt von der Aufbewahrungszeitraum für gelöschte Elemente, die für das Postfach festgelegt wird. Exchange Online-Postfach behält gelöschte Elemente für 14 Tage standardmäßig. Verwenden Sie Exchange Online PowerShell, wie oben gezeigt, zum Ändern dieser Einstellung den Zeitraum bis maximal 30 Tage zu erhöhen.

Benutzer können wiederherstellen oder löschen, Gelöschte Objekte vor Ablauf die Aufbewahrungszeit für ein gelöschtes Element. Dazu verwenden sie das Feature **Gelöschte Elemente wiederherstellen** in Outlook oder Outlook im Web. Für [Outlook](#) oder [Outlook Web App](#), finden Sie unter den folgenden Themen.

Weitere Hilfe:

- Wenn ein Benutzer ein gelöschtes Element endgültig löscht, können Sie es vor Ablauf der Aufbewahrungszeit für gelöschte Objekte wiederherstellen. Weitere Informationen finden Sie unter [Recover deleted messages in a user's mailbox](#).
- Weitere Informationen zur Aufbewahrung von gelöschten Elementen, zum Ordner „Wiederherstellbare Elemente“, In-Situ-Speicher und Beweissicherungsverfahren finden Sie unter [Understanding Recoverable Items](#).

# Konfigurieren der E-Mail-Weiterleitung für ein Postfach

18.12.2018 • 5 minutes to read

E-Mail-Weiterleitung ermöglicht Ihnen das Einrichten eines Postfachs auf forward-e-Mail-Nachrichten mit dem Postfach eines anderen Benutzers Postfach in oder außerhalb Ihrer Organisation gesendet.

## IMPORTANT

Wenn Sie Office 365 für Unternehmen verwenden, sollten Sie e-Mail-Weiterleitung in Konfigurieren der [Office 365 Administrationscenter: Konfigurieren der e-Mail-Weiterleitung in Office 365](#)

Wenn Ihre Organisation einen lokalen Exchange- oder hybride Exchange-Umgebung verwendet wird, sollten Sie die lokalen Exchange-Verwaltungskonsole (EAC) zu erstellen und Verwalten von freigegebenen Postfächern verwenden.

## Verwenden Sie die Exchange-Verwaltungskonsole zum Konfigurieren von e-Mail-Weiterleitung

Sie können die Exchange-Verwaltungskonsole (EAC) Einrichten von e-Mail-Weiterleitung an einen einzelnen internen Empfänger, einen externen Empfänger (mit e-Mail-Kontakt) oder mehrere Empfänger (mit einer Verteilergruppe) verwenden.

Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter „Berechtigungen für die Empfängerbereitstellung“ im Thema [Empfängerberechtigungen](#).

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Liste der Benutzerpostfächer, klicken Sie auf oder tippen Sie auf das Postfach, das Sie e-Mail-Weiterleitung, konfigurieren möchten und klicken oder tippen Sie auf **Bearbeiten**.
3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.
4. Wählen Sie unter **E-Mail-Fluss Details anzeigen** aus, um die Einstellung für die Weiterleitung von E-Mail-Nachrichten anzuzeigen oder zu ändern.

Auf dieser Seite können Sie die maximale Anzahl von Empfängern festlegen, denen der Benutzer eine Nachricht senden kann. Für lokale Exchange-Organisationen ist die Empfängerzahl unbegrenzt. Der Grenzwert ist für Exchange Online-Organisationen 500 Empfänger.

5. Aktivieren Sie das Kontrollkästchen **Weiterleitung aktivieren**, und klicken Sie dann auf **Durchsuchen**.
6. Wählen Sie auf der Seite **Empfänger wählen** einen Benutzer aus, an den die E-Mail weitergeleitet werden soll. Aktivieren Sie das Kontrollkästchen **Nachricht an Weiterleitungsadresse und Postfach übermitteln**, wenn der Empfänger und die E-Mail-Adresse für die Weiterleitung Kopien der gesendeten E-Mails erhalten sollen. Klicken oder tippen Sie auf **OK** und anschließend auf **Speichern**.

Wie gehen Sie vor, wenn Sie E-Mails an eine E-Mail-Adresse außerhalb Ihrer Organisation weiterleiten möchten? Oder E-Mail-Nachrichten an mehrere Empfänger weiterleiten? Dies ist ebenfalls möglich.

- **Externen Adressen:** Erstellen Sie einen e-Mail-Kontakt, und wählen Sie in den Schritten des e-Mail-

Kontakts auf der Seite **Empfänger auswählen**. Möchten Sie wissen, wie Sie e-Mail-Kontakt erstellen? Verwalten von e-Mail-KontakteAuschecken.

- **Mehrere Empfänger:** Erstellen einer Verteilergruppe, Empfänger hinzugefügt, und wählen Sie dann in den Schritten des e-Mail-Kontakts auf der Seite **Empfänger auswählen**. Möchten Sie wissen, wie Sie e-Mail-Kontakt erstellen? Checken Sie [Erstellen und Verwalten von Verteilergruppen](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie erfolgreich e-Mail-Weiterleitung konfiguriert haben, führen Sie eine der folgenden Aktionen aus:

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Liste der Benutzerpostfächer, klicken Sie auf, oder tippen Sie auf das Postfach, das Sie für die e-Mail-Weiterleitung konfiguriert haben, und klicken Sie dann auf **Bearbeiten** 
3. Klicken oder tippen Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.
4. Klicken oder tippen Sie unter **Nachrichtenfluss** auf **Details anzeigen**, um die E-Mail-Weiterleitungseinstellungen anzuzeigen.

## Weitere Informationen

Dieses Thema ist für Administratoren bestimmt. Wenn Sie eigene E-Mail-Nachrichten an einen anderen Empfänger weiterleiten möchten, lesen Sie die folgenden Themen:

- [Weiterleiten von E-Mails an ein anderes E-Mail-Konto](#)
- [Verwalten von E-Mails mithilfe von Regeln](#)

Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Konfigurieren von Nachrichtenzustellungseinschränkungen für ein Postfach

18.12.2018 • 10 minutes to read

Sie können die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell verwenden, platziert Einschränkungen auf gibt an, ob Nachrichten an einzelne Empfänger übermittelt werden. Nachricht Übermittlung Einschränkungen eignen sich steuern, wer Nachrichten an Benutzer in Ihrer Organisation senden können. Beispielsweise können Sie ein Postfach annehmen oder ablehnen von Nachrichten, die von bestimmten Benutzern gesendet oder Empfangen von Nachrichten nur von Benutzern in Ihrer Exchange-Organisation zu konfigurieren.

## IMPORTANT

Nachricht Übermittlung Einschränkungen wirken sich nicht auf Postfachberechtigungen auf. Ein Benutzer mit Vollzugriff-Berechtigungen für ein Postfach weiterhin werden können zum Aktualisieren des Inhalts in diesem Postfach wie durch Kopieren von Nachrichten in das Postfach, auch wenn der Benutzer beschränkt wurde.

Die in diesem Thema behandelten Nachrichtenübermittlungseinschränkungen gelten für alle Empfängertypen. Weitere Informationen zu den verschiedenen Empfängertypen finden Sie unter [Recipients](#).

Zusätzliche Verwaltungsaufgaben im Zusammenhang mit Empfängern finden Sie in den folgenden Themen:

- [Verwalten von Benutzerpostfächern](#)
- [Erstellen und Verwalten von Verteilergruppen](#)
- [Verwalten dynamischer Verteilergruppen](#)
- [Verwalten von E-Mail-Benutzern](#)
- [Verwalten von E-Mail-Kontakten](#)

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie müssen finden Sie unter dem Abschnitt "Empfängerbereitstellungsberechtigungen" im Thema [Recipients Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

Verwenden der Exchange-Verwaltungskonsole zum Konfigurieren von

# Einschränkungen für die Nachrichtenzustellung

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Liste der Benutzerpostfächer, klicken Sie auf das Postfach, das Sie Nachricht Übermittlung Einschränkungen für konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**
3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.
4. Klicken Sie unter **Einschränkungen für die Nachrichtenzustellung** auf **Details anzeigen**, um die folgenden Zustellungseinschränkungen anzuzeigen und zu ändern:
  - **Nachrichten annehmen von:** Verwenden Sie diesen Abschnitt, um anzugeben, wer Nachrichten an diesen Benutzer senden kann.
  - **Alle Absender:** Diese Option gibt an, dass der Benutzer Nachrichten von allen Absendern annehmen kann. Dazu gehören sowohl Absender in Ihrer Exchange-Organisation und externe Absender. Dies ist die Standardoption. Sie umfasst externe Benutzer nur, wenn Sie das Kontrollkästchen **erforderlich, dass die Authentifizierung aller Absender anfordern** deaktivieren. Wenn Sie dieses Kontrollkästchen aktivieren, werden Nachrichten von externen Benutzern abgelehnt.
  - **Nur Absender in der folgenden Liste:** Diese Option gibt an, dass der Benutzer Nachrichten nur von einer bestimmten Gruppe von Absendern in Ihrer Exchange-Organisation akzeptieren kann. Klicken Sie auf **Hinzufügen**  zum Anzeigen einer Liste aller Empfänger in Ihrer Exchange-Organisation. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen** .
  - **Erfordern, dass alle Absender authentifiziert werden:** Diese Option wird verhindert, dass anonyme Benutzer Nachrichten an die Benutzer senden können. Dazu gehören externe Benutzer, die sich außerhalb Ihrer Exchange-Organisation befinden.
  - **Nachrichten ablehnen von:** Verwenden Sie diesen Abschnitt zu hindern, Nachrichten an diesen Benutzer zu senden.
  - **Kein Absender:** Diese Option gibt an, dass das Postfach ablehnen von Nachrichten von beliebigen Absendern in der Exchange-Organisation wird nicht. Dies ist die Standardoption.
  - **Absender in der folgenden Liste:** Diese Option gibt an, dass das Postfach ablehnen von Nachrichten von einer bestimmten Gruppe von Absendern in Ihrer Exchange-Organisation wird. Klicken Sie auf **Hinzufügen**  zum Anzeigen einer Liste aller Empfänger in Ihrer Exchange-Organisation. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen** .
5. Klicken Sie auf **OK**, um die Seite **Einschränkungen für die Nachrichtenzustellung** zu schließen, und dann auf **Speichern**, um die Änderungen zu speichern.

## Verwenden von Exchange Online PowerShell Nachricht Übermittlung Einschränkungen konfigurieren

In den folgenden Beispielen gezeigt, wie Exchange Online PowerShell verwenden, um die Nachricht Übermittlung Einschränkungen für ein Postfach zu konfigurieren. Verwenden Sie das entsprechende **Set** - Cmdlet für andere Empfängertypen mit denselben Parametern.

In diesem Beispiel wird das Postfach von Robin Wood so konfiguriert, dass nur Nachrichten der Benutzer Lori Penor, Jens Phillips und von Mitgliedern der Verteilergruppe "Legal Team 1" akzeptiert werden.

```
Set-Mailbox -Identity "Robin Wood" -AcceptMessagesOnlyFrom "Lori Penor","Jeff Phillips" -  
AcceptMessagesOnlyFromDLMembers "Legal Team 1"
```

#### NOTE

Wenn Sie ein Postfach so konfigurieren möchten, dass nur Nachrichten einzelner Absender angenommen werden, müssen Sie den Parameter *AcceptMessagesOnlyFrom* verwenden. Wenn Sie ein Postfach so konfigurieren möchten, dass nur Nachrichten von Absendern angenommen werden, die Mitglied einer bestimmten Verteilergruppe sind, verwenden Sie den Parameter *AcceptMessagesOnlyFromDLMembers*.

In diesem Beispiel wird der Benutzer David Pelton der Liste der Benutzer hinzugefügt, deren Nachrichten vom Postfach von Robin Wood akzeptiert werden.

```
Set-Mailbox -Identity "Robin Wood" -AcceptMessagesOnlyFrom @{add="David Pelton"}
```

In diesem Beispiel wird das Postfach von Robin Wood so konfiguriert, dass nur authentifizierte Absender zugelassen werden. Dies bedeutet, dass das Postfach nur Nachrichten akzeptiert, die von anderen Benutzern in Ihrer Exchange-Organisation gesendet wurden.

```
Set-Mailbox -Identity "Robin Wood" -RequireSenderAuthenticationEnabled $true
```

In diesem Beispiel wird das Postfach von Robin Wood so konfiguriert, dass Nachrichten der Benutzer Joe Healy, Terry Adams und von Mitgliedern der Verteilergruppe "Legal Team 2" zurückgewiesen werden.

```
Set-Mailbox -Identity "Robin Wood" -RejectMessagesFrom "Joe Healy","Terry Adams" -RejectMessagesFromDLMembers  
"Legal Team 2"
```

In diesem Beispiel wird das Postfach von Robin Wood so konfiguriert, dass auch Nachrichten von Mitgliedern der Gruppe "Legal Team 3" zurückgewiesen werden.

```
Set-Mailbox -Identity "Robin Wood" -RejectMessagesFromDLMembers @{add="Legal Team 3"}
```

#### NOTE

Wenn Sie ein Postfach so konfigurieren möchten, dass nur Nachrichten einzelner Absender zurückgewiesen werden, müssen Sie den Parameter *RejectMessagesFrom* verwenden. Wenn Sie ein Postfach so konfigurieren möchten, dass nur Nachrichten von Absendern zurückgewiesen werden, die Mitglied einer bestimmten Verteilergruppe sind, verwenden Sie den Parameter *RejectMessagesFromDLMembers*.

In den folgenden Themen finden Sie detaillierte Informationen zu Syntax und Parametern im Zusammenhang mit der Konfiguration von Zustellungseinschränkungen für verschiedene Empfängertypen:

- [Set-DistributionGroup](#)
- [Set-DynamicDistributionGroup](#)
- [Set-Mailbox](#)
- [Set-MailContact](#)
- [Set-MailUser](#)

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um die erfolgreiche Konfiguration von Einschränkungen für die Nachrichtenzustellung für ein Benutzerpostfach zu überprüfen:

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Liste der Benutzerpostfächer, klicken Sie auf das Postfach, dem Sie die Nachricht Übermittlung Einschränkungen für überprüfen möchten, und klicken Sie dann auf **Bearbeiten** .
3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.
4. Klicken Sie unter **Einschränkungen für die Nachrichtenzustellung** auf **Details anzeigen**, um die Einschränkungen für die Nachrichtenzustellung für das Postfach zu überprüfen.

oder -

Führen Sie den folgenden Befehl in Exchange Online PowerShell.

```
Get-Mailbox <identity> | Format-List  
AcceptMessagesOnlyFrom,AcceptMessagesOnlyFromDLMembers,RejectMessagesFrom,RejectMessagesFromDLMembers,Requires  
enderAuthenticationEnabled
```

# Konvertieren eines Postfachs

18.12.2018 • 3 minutes to read

Konvertieren eines Postfachs in einen anderen Typ des Postfachs ist sehr ähnlich wie in Exchange 2010. Sie müssen das Cmdlet Set-Mailbox in Exchange Online PowerShell weiterhin verwenden, für die Konvertierung.

Sie können die folgenden Postfächer von einem Typ in einen anderen konvertieren:

- Benutzerpostfach in Ressourcenpostfach (Raum/Arbeitsgerät)
- Freigegebenes Postfach in Benutzerpostfach
- Freigegebenes Postfach in Ressourcenpostfach
- Ressourcenpostfach in Benutzerpostfach
- Ressourcenpostfach in freigegebenes Postfach

Wenn Ihre Organisation eine Exchange-Hybridumgebung verwendet, müssen Sie Ihre Postfächer mithilfe der lokalen Exchange-Verwaltungstools verwalten. Um ein Postfach in einer Hybridumgebung zu konvertieren, müssen Sie das Postfach möglicherweise zurück auf den lokalen Exchange-Computer verschieben, den Postfachtyp konvertieren und das Postfach dann zurück nach Office 365 verschieben.

## IMPORTANT

Wenn Sie ein Benutzerpostfach auf ein freigegebenes Postfach konvertieren, sollten Sie entweder alle mobilen Geräte aus dem Postfach vor der Konvertierung entfernen, oder Sie sollten mobilen Zugriff auf das Postfach nach der Konvertierung blockieren. Dies liegt daran, sobald das Postfach in einem freigegebenen Postfach konvertiert wird, Funktionen für mobile Geräte nicht ordnungsgemäß ausgeführt werden. Weitere Informationen zum Blockieren des Zugriffs finden Sie unter [einem früheren Mitarbeiter von Office 365 zu entfernen](#).

## Verwenden Sie Exchange Online PowerShell, um ein Postfach zu konvertieren.

Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.

Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berechtigungen für die Empfängerbereitstellung" im Thema [Mailbox Permissions](#).

In diesem Beispiel wird das freigegebene Postfach „MarketingDept1“ in ein Benutzerpostfach konvertiert.

```
Set-Mailbox MarketingDept1 -Type Regular
```

Für den Parameter *Type* können folgende Werte verwendet werden:

- Regular
- Room
- Equipment
- Shared

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailbox](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie das Postfach erfolgreich konvertiert haben, führen Sie den folgenden Befehl in Exchange Online PowerShell:

```
Get-Mailbox -Identity MarketingDept1 | Format-List RecipientTypeDetails
```

Der Wert für "*RecipientTypeDetails*" sein sollte `UserMailbox`.

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-Mailbox](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Aktivieren oder Deaktivieren von Exchange ActiveSync für ein Postfach

18.12.2018 • 4 minutes to read

Sie können die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell verwenden, aktivieren oder Deaktivieren von Microsoft Exchange ActiveSync für ein Benutzerpostfach. Exchange ActiveSync ist ein Clientprotokoll, mit denen Benutzer ein mobiles Gerät mit ihrem Exchange-Postfach synchronisieren kann. Exchange ActiveSync ist standardmäßig aktiviert, wenn ein Benutzerpostfach erstellt wird. Weitere Informationen finden Sie unter [Exchange ActiveSync](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Exchange ActiveSync-Einstellungen" im Thema [Clients and Mobile Devices Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Aktivieren oder Deaktivieren von Exchange ActiveSync

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Liste der Benutzerpostfächer, klicken Sie auf das Postfach, das Sie aktivieren oder Deaktivieren von Exchange ActiveSync für möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.
4. Führen Sie unter **Mobilgeräte** einen der folgenden Schritte aus:
  - Klicken Sie zum Deaktivieren von Exchange ActiveSync auf **Exchange ActiveSync deaktivieren**. Eine Warnung gefragt, wenn Sie sicher sind, dass Sie Exchange ActiveSync deaktivieren möchten. Klicken Sie auf **Ja**.
  - Klicken Sie zum Aktivieren von Exchange ActiveSync auf **Exchange ActiveSync aktivieren**.
5. Klicken Sie auf **Speichern**, um die Änderung zu speichern.

#### NOTE

Sie können aktivieren und Deaktivieren von Exchange ActiveSync für mehrere Benutzerpostfächer mithilfe der Exchange-Verwaltungskonsole Bulk Edit-Funktion. Weitere Informationen hierzu finden Sie im Abschnitt "Massenbearbeitung von Benutzerpostfächern" in [Verwalten von Benutzerpostfächern](#).

## Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren von Exchange ActiveSync

In diesem Beispiel wird für das Postfach von Yan Li Exchange ActiveSync deaktiviert.

```
Set-CASMailbox -Identity "Yan Li" -ActiveSyncEnabled $false
```

In diesem Beispiel wird für das Postfach von Elly Nkya Exchange ActiveSync aktiviert.

```
Set-CASMailbox -Identity Ellyn@contoso.com -ActiveSyncEnabled $true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-CASMailbox](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um zu überprüfen, dass Sie erfolgreich aktiviert oder Exchange ActiveSync für ein Benutzerpostfach deaktiviert haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**, klicken Sie auf das Postfach, und klicken Sie dann auf **Bearbeiten**.
- Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.
- Überprüfen Sie, ob Exchange ActiveSync aktiviert oder deaktiviert ist, klicken Sie unter **Mobile Geräte**.

Oder

- Führen Sie den folgenden Befehl in Exchange Online PowerShell.

```
Get-CASMailbox <identity>
```

Wenn Exchange ActiveSync aktiviert ist, ist der Wert für die Eigenschaft *ActiveSyncEnabled* `True`. Wenn Exchange ActiveSync deaktiviert ist, ist der Wert `False`.

# Aktivieren oder Deaktivieren von MAPI für ein Postfach

18.12.2018 • 4 minutes to read

Sie können die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell verwenden, aktivieren oder Deaktivieren von MAPI für ein Benutzerpostfach. Wenn MAPI aktiviert ist, kann dem Postfach eines Benutzers von Outlook oder andere MAPI-e-Mail-Clients zugegriffen werden. Wenn MAPI deaktiviert ist, kann es von Outlook oder andere MAPI-Clients zugegriffen werden. Jedoch weiterhin das Postfach zum Empfangen von e-Mail-Nachrichten und, unter der Annahme, dass das Postfach für die Unterstützung des Zugriffs durch diese Clients aktiviert ist, kann ein Benutzer auf das Postfach zum Senden und Empfangen von e-Mail mit Outlook Web App, ein POP-e-Mail-Client oder einen IMAP-Client zugreifen.

## NOTE

Unterstützung für Outlook Web App sowie MAPI-, POP3- und IMAP4-E-Mail-Clients ist standardmäßig aktiviert, wenn ein Benutzerpostfach erstellt wird.

Informationen zu weiteren Verwaltungsaufgaben in Bezug die Verwaltung des E-Mail-Clientzugriffs auf ein Postfach finden Sie in den folgenden Themen:

- [Aktivieren oder Deaktivieren von Outlook Web App für ein Postfach](#)
- [Enable or Disable IMAP4 Access for a User](#)
- [Aktivieren oder Deaktivieren des POP3-Zugriffs für einen Benutzer](#)

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Benutzereinstellungen Clientzugriff" im Thema [Clients and Mobile Devices Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Shell zum Aktivieren oder Deaktivieren von MAPI

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Liste der Benutzerpostfächer, klicken Sie auf das Postfach, das Sie aktivieren oder Deaktivieren von MAPI möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.

4. Führen Sie unter **E-Mail-Konnektivität** einen der folgenden Schritte aus.

- Klicken Sie zum Deaktivieren von MAPI unter **MAPI: Aktiviert** auf **Deaktivieren**.

Es wird eine Warnung angezeigt, in der Sie gefragt werden, ob Sie MAPI wirklich deaktivieren möchten.

Klicken Sie auf **Ja**.

- Klicken Sie zum Aktivieren von MAPI unter **MAPI: Deaktiviert** auf **Aktivieren**.

5. Klicken Sie auf **Speichern**, um die Änderung zu speichern.

## Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren von MAPI

In diesem Beispiel wird MAPI für das Postfach von Ken Sanchez deaktiviert.

```
Set-CASMailbox -Identity "Ken Sanchez" -MAPIEnabled $false
```

In diesem Beispiel wird MAPI für das Postfach von Esther Valle aktiviert.

```
Set-CASMailbox -Identity "Esther Valle" -MAPIEnabled $true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-CASMailbox](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um die erfolgreiche Aktivierung bzw. Deaktivierung von MAPI für ein Benutzerpostfach zu überprüfen:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**, klicken Sie auf das Postfach, und klicken Sie dann auf **Bearbeiten**.
- Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.
- Überprüfen Sie unter **E-Mail-Konnektivität**, ob MAPI aktiviert oder deaktiviert ist.

oder -

- Führen Sie den folgenden Befehl in Exchange Online PowerShell.

```
Get-CASMailbox <identity>
```

Wenn MAPI aktiviert ist, ist der Wert für die Eigenschaft *MapiEnabled* `True`. Wenn MAPI deaktiviert ist, ist der Wert `False`.

# Aktivieren oder Deaktivieren von Outlook Web App für ein Postfach

18.12.2018 • 5 minutes to read

Sie können die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell verwenden, aktivieren oder Deaktivieren von Outlook Web App für ein Benutzerpostfach. Wenn Outlook Web App aktiviert ist, kann ein Benutzer Outlook Web App verwenden, senden und Empfangen von e-Mail. Wenn Outlook Web App deaktiviert ist, wird das Postfach zum Empfangen von e-Mail-Nachrichten fortgesetzt, und ein Benutzer zugreifen kann, um das Senden und Empfangen von e-Mail mithilfe von MAPI-Client wie beispielsweise Microsoft Outlook oder mit einem POP- oder IMAP-e-Mail-Client vorausgesetzt, dass das Postfach aktiviert ist, zur Unterstützung von Access durch diese Clients.

## NOTE

Unterstützung für Outlook Web App sowie MAPI-, POP3- und IMAP4-E-Mail-Clients ist standardmäßig aktiviert, wenn ein Benutzerpostfach erstellt wird.

Informationen zu weiteren Verwaltungsaufgaben in Bezug die Verwaltung des E-Mail-Clientzugriffs auf ein Postfach finden Sie in den folgenden Themen:

- [Aktivieren oder Deaktivieren von MAPI für ein Postfach](#)
- [Enable or Disable IMAP4 Access for a User](#)
- [Aktivieren oder Deaktivieren des POP3-Zugriffs für einen Benutzer](#)

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Benutzereinstellungen Clientzugriff" im Thema [Clients and Mobile Devices Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren oder Deaktivieren von Outlook Web App mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Liste der Benutzerpostfächer, klicken Sie auf das Postfach, das Sie aktivieren oder Deaktivieren von Outlook Web App für möchten, und klicken Sie dann auf **Bearbeiten**

3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.

4. Führen Sie unter **E-Mail-Konnektivität** eine der folgenden Aktionen aus:

- So deaktivieren Sie Outlook Web App unter **Outlook Web App: aktiviert**, klicken Sie auf **Deaktivieren**.

Eine Warnung gefragt, wenn Sie sicher sind, dass Sie Outlook Web App klicken Sie auf **Ja** deaktivieren möchten.

- So aktivieren Sie unter Outlook Web App **Outlook Web App: deaktivierte**, klicken Sie auf **Aktivieren**.

5. Klicken Sie auf **Speichern**, um die Änderung zu speichern.

#### NOTE

Sie können aktivieren und Deaktivieren von Outlook Web App für mehrere Benutzerpostfächer mithilfe der Exchange-Verwaltungskonsole Bulk Edit-Funktion. Weitere Informationen hierzu finden Sie im Abschnitt "Massenbearbeitung von Benutzerpostfächern" in [Verwalten von Benutzerpostfächern](#).

## Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren von Outlook Web App

In diesem Beispiel wird für das Postfach von Yan Li Outlook Web App deaktiviert.

```
Set-CASMailbox -Identity "Yan Li" -OWAEnabled $false
```

In diesem Beispiel wird für das Postfach von Ellyn Nkya Outlook Web App aktiviert.

```
Set-CASMailbox -Identity Ellyn@contoso.com -OWAEnabled $true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-CASMailbox](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um zu überprüfen, dass Sie erfolgreich aktiviert oder Outlook Web App für ein Benutzerpostfach deaktiviert haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**, klicken Sie auf das Postfach, und klicken Sie dann auf **Bearbeiten**
- Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.
- Klicken Sie unter **E-Mail-Konnektivität** überprüfen Sie, ob Outlook Web App aktiviert oder deaktiviert ist.

Oder

- Führen Sie den folgenden Befehl in Exchange Online PowerShell.

```
Get-CASMailbox <identity>
```

Wenn Outlook Web App aktiviert ist, ist der Wert für die Eigenschaft **OWAEnabled**  **True**. Wenn Outlook Web App deaktiviert ist, ist der Wert  **False**.

# Automatisches Speichern von gesendeten Elementen im Postfach des Stellvertreters

18.12.2018 • 10 minutes to read

Postfächer in Office 365 können eingerichtet werden, damit eine Person (beispielsweise wenn ein executive Assistent) Zugriff auf das Postfach einer anderen Person (beispielsweise ein Manager) und als diese e-Mail senden kann. Diese Personen werden häufig die Stellvertretung und Stellvertreter, jeweils bezeichnet. Wir müssen sie "Assistent" und "Manager" der Einfachheit halber anzurufen. Wenn ein Assistent Zugriff auf das Postfach des Managers gewährt wird, wird sie delegierten Zugriff aufgerufen.

Personen, die häufig eingerichtet Zugriffsrechte und Senden von Berechtigungen, wenn ein Assistent einen Manager-Kalender verwalten ermöglichen, zu senden und Antworten auf Besprechungsanfragen werden müssen. Wenn ein Assistent sendet e-Mail-Nachrichten im Auftrag von oder als, ein Manager wird die gesendete Nachricht wird standardmäßig im Ordner für seinen Vorgesetzten gesendete Objekte gespeichert. In diesem Artikel können Sie dieses Verhalten ändern, sodass die gesendete Nachricht in der Assistent und des Managers gesendete Objekte Ordner gespeichert ist.

Betrachten wir nun ein kurzes Beispiel, wie dies in der Praxis funktionieren würde:

- Mary ist die globale Vertriebsleiter. Er verfügt über eine sehr beschäftigt Zeitplan und Rob, dessen executive-Assistent zur Verwaltung von ihrem Kalender.
- Um Hilfe zu Mary Rob wurde der Zugriff auf Mary Postfach und zum Senden von Nachrichten in ihrem Auftrag gewährt delegiert. Dadurch können ihm finden Sie unter Neuigkeiten in ihrem Kalender. Planen, annehmen und Ablehnen von Besprechungsanfragen; und auf Nachrichten antworten.
- Nachrichten, die im Namen Mary Rob sendet, werden in den Ordner Gesendete Objekte gespeichert. Mary möchte eine Kopie, damit Rob manuell Nachrichten kopiert, die er in ihrem Auftrag von seinem Ordner Gesendete Objekte in ihrem Ordner Gesendete Elemente gesendet wird.
- Von Rob Young Wunder befindet sich eine bessere Möglichkeit, Gesendete Objekte behandeln, damit er seine IT-Helpdesk gefragt werden. Er lernen, dass Mary Postfach eingerichtet werden kann, um Nachrichten gespeichert werden sollen, die er in ihrem Auftrag in seinem gesendete Objekte und ihre gesendete Elemente automatisch sendet. Dies ist genau das, was er möchte, dass sodass er den Help Desk bittet eingerichtet.

## Senden als... Senden im Auftrag von... welcher möchten sie bedeuten und dem soll ich auswählen?

Wenn Sie eine Person als Stellvertretung für einen Manager Postfach eingerichtet, können Sie auswählen, ob sie "als" den Manager senden oder "im Auftrag von senden". Der Unterschied ist Subtiler, aber in einigen Organisationen wichtig sein kann:

- **Senden als** Wenn ein Benutzer die Berechtigung "Senden als" für ein Postfach hat, anzeigen Nachrichten, die sie aus dem Postfach senden nur die Namen der Postfachbesitzer From: Feld der Nachricht. Im obigen Beispiel, wenn Rob Berechtigungen "Senden als" für Mary Postfach verfügt Nachrichten von ihrem Postfach er sendet zeigt **aus: Mary** an Empfänger.
- **Senden im Auftrag von** Wenn ein Benutzer die Berechtigung "Senden im Auftrag von" für ein Postfach hat, zeigt gesendete Nachrichten aus den Besitzer Postfach an, dass die Nachricht von einer Person im Namen der Postfachbesitzer gesendet wurde. Im obigen Beispiel, wenn Rob Berechtigungen "Senden im

Auftrag von" Mary Postfach hat Nachrichten von ihrem Postfach er sendet zeigt **aus: Rob im Namen Mary** an Empfänger.

Die Send-Berechtigungen, die ein Benutzer auf einen anderen Benutzer Postfach hat sind wichtig, wenn denken wie gesendet, dass Elemente behandelt werden soll. Dies liegt daran, für die einzelnen Ebenen der Berechtigungen, können Sie entscheiden, ob die Nachrichten im Ordner Gesendete Objekte der Assistent von nur oder in der Assistent und des Managers gesendete Objekte Ordner gespeichert werden soll. Office 365 wird standardmäßig zum Speichern von gesendeten Elementen für Nachrichten, die mit "Senden als" und "Senden im Auftrag von"-Berechtigungen in der Assistent gesendete Objekte nur gesendet. Sie können dieses Standardverhalten wie nachstehend beschrieben ändern.

#### TIP

Manager möglicherweise mehrere Vertreter mit verschiedenen Berechtigungsstufen. Im obigen Beispiel konnte Rob zum Senden von Nachrichten im Namen Mary, möglicherweise er eine andere Mitarbeiter haben, die als Mary senden dürfen. Wenn dies der Fall, Mary des war IT-Abteilung konnte führen Sie die Schritte zum "Senden als" und "Senden im Auftrag von" Berechtigungen.

## Wie richte ich ein Postfach zum Speichern von Nachrichten "als" einen Manager nach Sendens durch einen Assistenten ein?

Wenn Sie folgendermaßen eine beliebige **als gesendete** Nachrichten den Manager, deren Postfach Sie konfigurieren tun, wird des Managers gesendete Objekte Ordner gespeichert werden. Befolgen Sie die folgenden Schritte aus, um dies einzurichten. Sie müssen Windows PowerShell verwenden, um die Schritte auszuführen. Wenn Sie es vor nicht verwendet haben, wechseln Sie zum [Verwenden von PowerShell mit Exchange Online](#) Anweisungen auf wie in Verbindung zu bleiben. Es ist ein hervorragendes Video zu!

1. Öffnen Sie Windows PowerShell, und verbinden Sie über die Anweisungen unter [Verwenden von PowerShell mit Exchange Online](#) mit Exchange Online PowerShell.
2. Rufen Sie die e-Mail-Adresse des Managers.
3. Führen Sie den folgenden Befehl in die PowerShell-Fenster.

```
Set-Mailbox <manager's email address> -MessageCopyForSentAsEnabled $true
```

<span data-ttu-id="d0c88-143">Beispielsweise ist Mary e-Mail-Adresse mary@contoso.com, IT-Abteilung würde führen Sie den Befehl `Set-Mailbox mary@contoso.com -MessageCopyForSentAsEnabled \$true` .</span><span class="sxs-lookup"><span data-stu-id="d0c88-143">For example, if Mary's email address is mary@contoso.com, her IT department would run the command `Set-Mailbox mary@contoso.com -MessageCopyForSentAsEnabled \$true` .</span></span>

Das wars! Der Manager erhalten jetzt automatisch eine Kopie der, wenn in ihrem Ordner Gesendete Objekte ein Assistent gesendeten Nachrichten.

#### TIP

Sie können dies deaktivieren, indem die obigen Schritte durchlaufen, und Ersetzen **\$true** mit **\$false** in den Befehl **[Set-Mailbox]**. Klicken sie zum Beispiel für Mary deaktivieren, Ausführen den Befehl

```
Set-Mailbox mary@contoso.com -MessageCopyForSentAsEnabled $false
```

## Wie richte ich ein Postfach ein "Gesendete Nachrichten im Auftrag von"

# einen Manager beim Sendens durch einen Assistenten speichern?

Wenn Sie diese Schritte, die alle Nachrichten **im Auftrag von gesendet** tun den Manager, deren Postfach Sie konfigurieren, wird auf den Ordner für den Manager gesendete Objekte gespeichert. Befolgen Sie die folgenden Schritte aus, um dies einzurichten. Sie müssen Windows PowerShell verwenden, um die Schritte auszuführen.

Wenn Sie es vor nicht verwendet haben, wechseln Sie zum [Verwenden von PowerShell mit Exchange Online](#) Anweisungen auf wie in Verbindung zu bleiben. Es ist ein hervorragendes Video zu!

1. Öffnen Sie Windows PowerShell, und verbinden Sie über die Anweisungen unter [Verwenden von PowerShell mit Exchange Online](#) mit Exchange Online PowerShell.
2. Rufen Sie die e-Mail-Adresse des Managers.
3. Führen Sie den folgenden Befehl in die PowerShell-Fenster.

```
Set-Mailbox <manager's email address> -MessageCopyForSendOnBehalfEnabled $true
```

<span data-ttu-id="d0c88-156">Beispielsweise ist Mary e-Mail-Adresse mary@contoso.com, IT-Abteilung würde führen Sie den Befehl `Set-Mailbox mary@contoso.com -MessageCopyForSendOnBehalfEnabled \$true`.</span><span class="sxs-lookup"><span data-stu-id="d0c88-156">For example, if Mary's email address is mary@contoso.com, her IT department would run the command `Set-Mailbox mary@contoso.com -MessageCopyForSendOnBehalfEnabled \$true`.</span></span>

Das wars! Der Manager erhalten jetzt automatisch eine Kopie der, wenn in ihrem Ordner Gesendete Objekte ein Assistent gesendeten Nachrichten.

## TIP

Sie können dies deaktivieren, indem die obigen Schritte durchlaufen, und Ersetzen **\$true** mit **\$false** in den Befehl **[Set-Mailbox]**. Klicken sie zum Beispiel für Mary deaktivieren, Ausführen den Befehl

```
Set-Mailbox mary@contoso.com -MessageCopyForSendOnBehalfEnabled $false .
```

# Benachrichtigungen über unwichtige Elemente in Outlook

18.12.2018 • 6 minutes to read

„Unwichtige Elemente“ ist eine Funktion in Office 365. Sie wurde entwickelt, um Benutzer dabei zu unterstützen, sich auf die wichtigsten Nachrichten in ihren Posteingängen zu konzentrieren, indem Nachrichten mit niedrigerer Priorität in den neuen Ordner „Unwichtige Elemente“ verschoben werden.

## Benachrichtigungen über unwichtige Elemente

„Unwichtige Elemente“ wird durch Benutzer in ihren jeweiligen O365- **Einstellungsoptionen** aktiviert. Dieser Artikel enthält Informationen für O365-Administratoren über Benachrichtigungen aus „Unwichtige Elemente“ für Endbenutzer.

Diese Benachrichtigungen sind ein wesentlicher Bestandteil der Clutterfunktion, sie können daher durch Administratoren nicht ausgesetzt werden. Clutter sind eine Benutzerauswahl. Sie ähneln jemandem, der die Unterhaltungsansicht verwendet, und die Benachrichtigungen helfen dem Benutzer, den Status von Clutter über alle Clients hinweg zu verstehen. Zurzeit steht keine zentrale Berichterstellung zur Verfügung. Informationen über das Ändern des Brandings der Benachrichtigungen finden Sie unter [Ändern des Brandings von Benachrichtigungen über unwichtige Elemente](#).

### NOTE

Informationen dazu, wie Endbenutzer Clutter aktivieren und verwenden können, finden Sie unter [Verwenden der Funktion „Clutter“ zum Sortieren von Nachrichten mit niedriger Priorität in Outlook](#).

### Einladung zur Verwendung von Clutter

Bevor Benutzer „Unwichtige Elemente“ verwenden, erhalten Sie eine Einladung für „Unwichtige Elemente“ in ihrem Posteingang. Durch die Einladung wird der Benutzer über die verfügbare Funktion informiert. Sie zeigt zudem die Vorteile der Verwendung von „Unwichtige Elemente“ auf.

„Unwichtige Elemente“ wird immer im Hintergrund ausgeführt, während Exchange das Postfach eines Benutzers durchsucht und versucht, sich in Bezug auf das Bestimmen von Nachrichten mit niedriger Priorität selbst zu schulen. Die Einladung, die ein Benutzer erhält, enthält einen Link zum Aktivieren von „Unwichtige Elemente“. Der Benutzer ermöglicht „Unwichtige Elemente“ somit, Nachrichten mit niedriger Priorität automatisch aus seinem Posteingang in einen dedizierten Ordner zu verschieben.

Zum Bestimmen, ob ein Benutzer eine Einladung zum Aktivieren von „Unwichtige Elemente“ erhält, stehen verschiedene Kriterien zur Verfügung, einschließlich:

- Hat Exchange nach genug Informationen im Postfach eines Benutzers gesucht, um die Parameter für „Unwichtige Elemente“ zu bestimmen?
- Ausreichende E-Mails: Empfängt der Benutzer mindestens drei als unwichtige Elemente eingestufte Nachrichten und mindestens drei nicht als unwichtige Elemente eingestufte Nachrichten?
- Wasserzeichen aktuell: Entspricht der Schulungsstatus dem aktuellen Status des Benutzers?
- Unterstützte Klassifikationsversion: Wird die Version, für die eine Schulung absolviert wurde, noch unterstützt?

- Erkennungsrate bei wirklich als unwichtige Elemente einzustufenden Nachrichten: Werden mindestens 85 % aller wirklich als unwichtige Elemente einzustufenden Nachrichten auch als solche klassifiziert?
- Fälschlicherweise gefilterte Nachrichten: Sind weniger als 20 % aller als unwichtige Elemente eingestuften Nachrichten tatsächlich Nachrichten, die nicht so eingestuft hätten werden sollen?

Ein Beispiel der Einladungsbenachrichtigung lautet wie folgt:

# Räumen Sie Ihr Postfach auf.

Die Option "Unwichtige Elemente" ist für Ihr Postfach bereits aktiviert. In der letzten Woche haben Sie 638 Elemente erhalten, die Sie möglicherweise ignorieren.

Wenn diese Meldung in Zukunft nicht mehr angezeigt werden soll, [klicken Sie auf "Hier", um die Option "Unwichtige Elemente" zu aktivieren.](#)

Mit dieser Option werden diese Elemente im Ordner "Unwichtige Elemente" platziert und Sie können sich auf Ihre wichtigsten Aussagen konzentrieren. Wenn falsche Elemente verschoben werden, können Sie Nachrichten verschieben und Unterhaltungen zurück in den Posteingang (und umgekehrt) verschieben. Weitere Informationen finden Sie [hier](#).

Freuen Sie sich über ein aufgeräumtes Postfach.

Diese Systembenachrichtigung ist keine E-Mail und Sie können nicht auf diese antworten.

Zum Zeitpunkt der Verwendung der Einladung wird ein neuer Ordner mit dem Namen **Unwichtige Elemente** erstellt und zu den Favoriten der Benutzer hinzugefügt. Dieselbe Einladungsnachricht wird als erste Nachricht im Ordner **Unwichtige Elemente** angezeigt.

## Löschen

Damit der Benutzer versteht, dass die neue Funktion aktiviert ist, sendet „Unwichtige Elemente“ eine weitere Benachrichtigung an dessen Posteingang. Darin wird beschrieben, wie „Unwichtige Elemente“ funktioniert und wie „Unwichtige Elemente“ korrigiert werden muss, wenn es eine Nachricht fälschlicherweise in den Ordner **Unwichtige Elemente** verschiebt. „Unwichtige Elemente“ ist eine Selbstlernfunktion. Nachdem der Benutzer durch das Verschieben von Nachrichten mit niedriger Priorität in den Ordner **Unwichtige Elemente** der Funktion „Unwichtige Elemente“ Informationen bereitgestellt hat, kann „Unwichtige Elemente“ demnach ähnliche Nachrichten bestimmen und sie automatisch verschieben.

Diese Benachrichtigung enthält jedoch auch einen Link zum Deaktivieren von „Unwichtige Elemente“, wenn der Benutzer der Ansicht ist, „Unwichtige Elemente“ ist für ihn ungeeignet. In neueren Clients stehen spezifischer Steuerungen zum Steuern von „Unwichtige Elemente“ zur Verfügung, diese stehen jedoch in älteren Clients nicht zur Verfügung.

**Von:** Das Office 365-Team  
**Gesendet:** Montag, 10. November 2014 6:42:00  
**An:**  
**Betreff:** Testen Sie Ihren neuen aufgeräumten Posteingang.

## Testen Sie Ihren neuen aufgeräumten Posteingang.

Da Sie die Option „Unwichtige Elemente“ aktiviert haben, wird Ihr Posteingang geordnet. Wenn Sie ein Element ignorieren, wird es in den Ordner „Unwichtige Elemente“ verschoben.

Manchmal kann es ggf. dazu kommen, dass falsche Elemente verschoben werden. Wenn Sie Outlook Web App verwenden, können Sie mit der rechten Maustaste klicken und die Option „Markierung als unwichtiges Element aufheben“ wählen. Bei allen anderen E-Mail-Programmen können Sie solche Unterhaltungen und Nachrichten aus dem Ordner „Unwichtige Elemente“ in den Ordner „Posteingang“ verschieben.

Datenschutz ist für uns sehr wichtig. Wir entfernen deshalb persönlich identifizierbare Informationen aus den Daten, die wir zur Verbesserung dieses Features verwenden.

Sollten Sie feststellen, dass Sie diese Option nicht nutzen möchten, können Sie sie jederzeit deaktivieren.

Wenn Sie das Verschieben von Nachrichten aus Ihrem Posteingang in den Ordner „Unwichtige Elemente“ beenden möchten, können Sie diese Option [deaktivieren](#). Diese Systembenachrichtigung ist keine E-Mail und Sie können nicht auf diese antworten.

### Harter Einsatz

Während der ersten drei Wochen der Verwendung von „Unwichtige Elemente“, wird die folgende Benachrichtigung regelmäßig aus zwei Gründen gesendet. Zunächst wird der Benutzer daran erinnert, den Ordner **Unwichtige Elemente** zu prüfen, um sicherzustellen, dass „Unwichtige Elemente“ die Nachrichten richtig filtert. Zudem stellt diese Benachrichtigung eine Möglichkeit für den Benutzer bereit, Feedback hinsichtlich „Unwichtige Elemente“ abzugeben. Zusätzlich stehen Links zur Verfügung, die weitere Informationen über die Funktion bereitstellen und mit denen „Unwichtige Elemente“ deaktiviert werden kann.

**Von:** Das Office 365-Team  
**Gesendet:** Montag, 17. November 2014 2:12:00  
**An:**  
**Betreff:** Shhh, unwichtige Elemente werden derzeit verschoben.

## Shhh, unwichtige Elemente werden derzeit verschoben.

Seit einiger Zeit nutzen Sie nun die Option „Unwichtige Elemente“. Sie können eine schnelle Überprüfung des Ordners durchführen und alle Nachrichten, die fälschlicherweise als „Unwichtige Elemente“ identifiziert wurden, zurück in den Ordner „Posteingang“ verschieben. Dadurch verbessern Sie die Funktionsweise dieses Features für das nächste Mal.

In einiger Zeit werden wir noch mal prüfen, wie gut das Feature funktioniert.

Haben Sie noch etwas Zeit übrig? Teilen Sie uns Ihre Meinung über dieses Feature mit.

[Feedback senden](#)

[Weitere Informationen](#)

Wenn Sie das Verschieben von Nachrichten aus Ihrem Posteingang in den Ordner „Unwichtige Elemente“ beenden möchten, können Sie diese Option [deaktivieren](#). Diese Systembenachrichtigung ist keine E-Mail und Sie können nicht auf diese antworten.

# Ändern des Brandings von Benachrichtigungen über unwichtige Elemente

18.12.2018 • 3 minutes to read

Die Funktion „Unwichtige Elemente“ verwendet Posteingangsbenachrichtigungen, um Benutzer einzuladen und um Statusmeldungen zu senden. Das standardmäßige für diese Benachrichtigungen verwendete Branding ist Outlook. Sie können das Branding jedoch für Ihre Organisation ändern.

## Ändern des Brandings von Benachrichtigungen über unwichtige Elemente

In diesem Artikel wird beschrieben, wie das Branding von Benachrichtigungen über unwichtige Elemente geändert wird, damit es mit Ihrer Schule, Ihrem Unternehmen oder Ihrer Organisation übereinstimmt.

### NOTE

Weitere Informationen über Typen von Benachrichtigungen über unwichtige Elemente, die Endbenutzer in Ihrer Organisation empfangen, finden Sie unter [Benachrichtigungen über unwichtige Elemente in Outlook](#).

Zunächst müssen Sie sich bei Office 365 mit Ihrem Arbeits- oder Schulkonto anmelden.

1. Wechseln Sie nach der Anmeldung bei Office 365 zu Office 365 Admin Center.
2. Erweitern Sie **Benutzer**, indem Sie mit der Maus darauf klicken, und wählen Sie **Aktive Benutzer** aus.
3. Wählen Sie das Hinzufügen eines Benutzers das Pluszeichen [ +] aus. Das Dialogfeld **Ein neues Benutzerkonto erstellen** wird geöffnet.
4. Geben Sie im Dialogfeld **erstellen ein neues Benutzerkonto** einen **Anzeigenamen** und einen **Benutzernamen** ein. Der Anzeigename wird in das Feld Absender für alle Unübersichtlichkeit Senden von Benachrichtigungen für Ihre Benutzer angezeigt. Office 365 generiert ein neues temporäres Kennwort für das neue Benutzerkonto ein. Klicken Sie auf **Erstellen**, um das Konto erstellt haben.
5. Wechseln Sie zu „Exchange Admin Center“.
6. Klicken Sie auf **Empfänger** und dann auf **Postfächer**.
7. Wählen Sie den soeben von Ihnen erstellten Benutzer aus, und klicken Sie dann auf das Stiftsymbol, um das Konto analog zur Darstellung im folgenden Beispiel zu bearbeiten.

## Exchange admin center

dashboard

### recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

unified messaging

mailboxes groups resources contacts shared migration



**Edit**  
DISPLAY NAME

MAILBOX TYPE

EMAIL ADDRESS

**Adatum IT**

**User**

**branding@adatum.com**

Administrator

User

admin@adatum.com

- Klicken Sie im Dialogfeld für das Benutzerkonto auf **E-Mail-Adresse** und dann auf das Pluszeichen [ +], um dem neuen Benutzerkonto eine E-Mail-Adresse hinzuzufügen.

Adatum IT

Help

general

mailbox usage

contact information

organization

#### ► email address

mailbox features

member of

MailTip

mailbox delegation

Each email address type has one default reply address. The default reply address is displayed in bold. To change the default reply address, select the email address that you want to set as the default, and then double-click to edit it.

Email address:



TYPE	EMAIL ADDRESS
<b>SMTP</b>	<b>branding@adatum.com</b>

You can add, change, or delete an email address associated with the user. The user's primary email address is displayed in bold type, but they'll receive email sent to any address in this list.

save

cancel

- Wählen Sie im Dialogfeld **Neue E-Mail-Adresse** SMTP als den E-Mail-Adressentyp aus. Geben Sie im Feld **E-Mail-Adresse** anschließend Folgendes ein: **7a694ec2-b7c9-41eb-b562-08fd2b277ae0@[Ihre Standarddomäne]**. [Ihre Standarddomäne] ist hierbei die von Ihrer Organisation verwendete Domäne. Bei den meisten Organisationen wäre dies **[Ihr Domänenname].onmicrosoft.com**.

Klicken Sie auf **OK**, nachdem Sie alle Änderungen vorgenommen haben.

new email address

Email address type:

- SMTP
- EUM
- enter a custom address type

The address can be EX, X.500, X.400, MSMail, CcMail, Lotus Notes, NovellGroupWise, EUM Proxy address, and free text. [Learn more](#)

\*Email address:

@NewEmailAddress\_AddressString

 Make this the reply address

ok

cancel

10. Klicken Sie im Dialogfeld für das Benutzerkonto auf **Speichern**, um die neue E-Mail-Adresse mit dem Benutzerkonto zu verknüpfen. Alle an Ihre Benutzer in Ihrer Organisation gesendeten Benachrichtigungen über unwichtige Elemente gehen nun auf dieses Konto zurück.

## Ändern Sie das branding der Übersichtlichkeit Benachrichtigungen von PowerShell

Sie können auch ein neues freigegebenes Postfach als der branding-Postfach über PowerShell erstellen. Gehen Sie folgendermaßen vor.

1. [Verbindung mit Exchange Online mit Remote-PowerShell](#).

2. Geben Sie die folgenden Befehle ein:

```
New-Mailbox -Shared -Name branding@contoso.com -DisplayName "Branding Clutter Mailbox" -Alias branding
Set-Mailbox "IT Admin" -EmailAddresses SMTP: branding@contoso
```

# Aktivieren oder Deaktivieren der Wiederherstellung einzelner Elemente für ein Postfach

18.12.2018 • 6 minutes to read

Exchange Online PowerShell können Sie aktivieren oder Deaktivieren der Wiederherstellung einzelner Elemente für ein Postfach. Wiederherstellung einzelner Elemente ist in Exchange Online standardmäßig aktiviert, wenn ein neues Postfach erstellt wird. Wiederherstellung einzelner Elemente ist in Exchange Server deaktiviert, wenn ein Postfach erstellt wird. Wiederherstellung einzelner Elemente aktiviert ist, werden Nachrichten, die endgültig gelöscht werden (gelöscht), durch den Benutzer im Ordner "wiederherstellbare Elemente" des Postfachs beibehalten, bis die Aufbewahrungszeit für gelöschte abläuft. Dies ermöglicht es einem Administrator, die vom Benutzer gelöscht wird, vor Ablauf die Aufbewahrungszeit für gelöschte Nachrichten wiederherstellen. Auch wenn eine Nachricht von einem Benutzer oder Prozess geändert wird, werden Kopien des ursprünglichen Elements auch beibehalten, wenn Wiederherstellung einzelner Elemente aktiviert ist.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Aufbewahrung und die rechtliche Aufbewahrungspflicht" im Thema [Mailbox Permissions](#).
- Die Wiederherstellung einzelner Elemente lässt sich nicht über das Exchange-Verwaltungskonsole (EAC) aktivieren oder deaktivieren.
- In Exchange Online ist die Aufbewahrungszeit für gelöschte standardmäßig auf 14 Tage festgelegt. Sie können diese Einstellung auf ein Maximum von 30 Tagen ändern. Weitere Informationen hierzu finden Sie unter [ändern wie lange dauerhaft gelöscht Elemente für ein Exchange Online-Postfach aufbewahrt werden](#).
- In Exchange verwendet Server, das Postfach die Einstellungen für die Aufbewahrung gelöschter Elemente der Postfachdatenbank, standardmäßig. Die Aufbewahrungszeit für eine Postfachdatenbank auf 14 Tage festgelegt ist, aber Sie können die Standardeinstellung außer Kraft setzen, durch das Konfigurieren dieser Einstellung für eine einzelne pro Postfach. Weitere Informationen hierzu finden Sie unter [Configure Aufbewahrungszeit und Kontingente für wiederherstellbare Elemente gelöscht](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um die Wiederherstellung einzelner Elemente aktivieren

In diesem Beispiel wird die Wiederherstellung einzelner Elemente für das Postfach von April Summers aktiviert.

```
Set-Mailbox -Identity "April Summers" -SingleItemRecoveryEnabled $true
```

In diesem Beispiel wird die Wiederherstellung einzelner Elemente für das Postfach von Pilar Pinilla aktiviert und die Aufbewahrungsfrist für gelöschte Elemente auf 30 Tage festgelegt.

```
Set-Mailbox -Identity "Pilar Pinilla" -SingleItemRecoveryEnabled $true -RetainDeletedItemsFor 30
```

In diesem Beispiel wird die Wiederherstellung einzelner Elemente für alle Benutzerpostfächer in der Organisation aktiviert.

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | Set-Mailbox -  
SingleItemRecoveryEnabled $true
```

In diesem Beispiel wird die Wiederherstellung einzelner Elemente für alle Benutzerpostfächer in der Organisation aktiviert, und die Aufbewahrungsfrist für gelöschte Elemente wird auf 30 Tage festgelegt.

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | Set-Mailbox -  
SingleItemRecoveryEnabled $true -RetainDeletedItemsFor 30
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailbox](#).

## Verwenden Sie Exchange Online PowerShell, um die Wiederherstellung einzelner Elemente deaktivieren

Sie müssen möglicherweise Wiederherstellung einzelner Elemente für das Postfach eines Benutzers zu deaktivieren. Bevor Sie endgültig löschen von Inhalt aus einem Postfach **Search-Mailbox-DeleteContent** verwenden können, müssen Sie beispielsweise Wiederherstellung einzelner Elemente deaktivieren. Weitere Informationen finden Sie unter [Suchen und Nachrichten löschen](#).

In diesem Beispiel wird die Wiederherstellung einzelner Elemente für das Postfach von Ayla Kol deaktiviert.

```
Set-Mailbox -Identity "Ayla Kol" -SingleItemRecoveryEnabled $false
```

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie zur Überprüfung der Aktivierung der Wiederherstellung einzelner Elemente und zur Anzeige des Werts für die Länge der Aufbewahrungsfrist (in Tagen) folgenden Befehl aus.

```
Get-Mailbox <Name> | Format-List SingleItemRecoveryEnabled,RetainDeletedItemsFor
```

Sie können denselben Befehl verwenden, um sicherzustellen, dass die Wiederherstellung einzelner Elemente für ein Postfach deaktiviert ist.

## Weitere Informationen

- Weitere Informationen zum Wiederherstellung einzelner Elemente finden Sie unter [Ordner „wiederherstellbare Elemente“](#). Zum Wiederherstellen von Nachrichten durch den Benutzer gelöscht wird, vor Ablauf die Aufbewahrungszeit für gelöschte, finden Sie unter [Wiederherstellen gelöschter Nachrichten im Postfach des Benutzers](#).
- Wenn ein Postfach in einem In-Situ-Speicher oder Beweissicherungsverfahren platziert wird, werden Nachrichten im Ordner „Wiederherstellbare Elemente“ beibehalten, bis die Aufbewahrungsdauer abläuft. Wenn die Aufbewahrungsdauer unbegrenzt ist, werden die Elemente beibehalten, bis der Haltebereich entfernt oder die Aufbewahrungsdauer geändert wird.

# Wiederherstellen von gelöschten Nachrichten im Postfach eines Benutzers

18.12.2018 • 15 minutes to read

(Dieses Thema ist für Exchange-Administratoren gedacht.)

Administratoren können Suchen nach und Wiederherstellen von gelöschten e-Mail-Nachrichten im Postfach des Benutzers. Dazu gehören Elemente, die (gelöscht) von einer Person (mithilfe des gelöschte Elemente wiederherstellen-Features in Outlook oder Outlook Web App) oder durch ein automatisierter Prozess, gelöschte Elemente endgültig gelöscht werden, wie die Aufbewahrungsrichtlinie auf Benutzerpostfächer zugewiesen. In den folgenden Situationen können nicht von einem Benutzer die gelöschten Elemente wiederhergestellt werden. Aber Administratoren können die gelöschten Nachrichten wiederherstellen, wenn die Aufbewahrungszeit für das Element abgelaufen ist.

## NOTE

Sie können dieses Verfahren nicht nur zum Suchen und Wiederherstellen gelöschter Elemente verwenden (die aus dem Ordner "Wiederherstellbare Elemente\Löschen" verschoben werden, wenn die Wiederherstellung einzelner Elemente oder die Aufbewahrung für eventuelle Rechtsstreitigkeiten aktiviert ist), sondern auch zum Suchen nach Elementen in anderen Ordnern des Postfachs sowie zum Löschen von Elementen aus dem Quellpostfach (auch bekannt als Suchen und Vernichten).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 15-30 Minuten.
- Für die Verfahren in diesem Thema sind bestimmte Berechtigungen erforderlich. Informationen zu den Berechtigungen finden Sie in den einzelnen Verfahren.
- Vor dem Löschen des Elements, den Sie wiederherstellen möchten, muss Wiederherstellung einzelner Elemente für ein Postfach aktiviert sein. Wiederherstellung einzelner Elemente ist in Exchange Online standardmäßig aktiviert, wenn ein neues Postfach erstellt wird. Wiederherstellung einzelner Elemente ist in Exchange Server deaktiviert, wenn ein Postfach erstellt wird. Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren der Wiederherstellung einzelner Elemente für ein Postfach](#).
- Zum Suchen und Wiederherstellen von Elementen benötigen Sie die folgenden Informationen:
  - **Quellpostfach:** Dies ist das Postfach, das durchsucht wird.
  - **Zielpostfach:** Hierbei handelt es sich um das discoverypostfach, in denen Nachrichten wiederhergestellt werden. Exchange-Setup erstellt eine standarddiscoverypostfach. In Exchange Online ist ein discoverypostfach auch in der Standardeinstellung erstellt. Falls erforderlich, können Sie zusätzliche discoverypostfächer erstellen. Weitere Informationen hierzu finden Sie unter [Erstellen eines discoverypostfachs](#).

## NOTE

Wenn Sie das Cmdlet **Search-Mailbox** verwenden, können Sie auch ein Zielpostfach angeben, bei dem es sich nicht um ein Discoverypostfach handelt. Sie können jedoch nicht dasselbe Postfach als Quell- und als Zielpostfach angeben.

- **Suchkriterien:** Kriterien Absender oder Empfänger oder Schlüsselwörter (Wörter oder Ausdrücke) in der Nachricht enthalten.
- In diesem Thema konzentriert sich auf die von PowerShell zum Wiederherstellen von gelöschter Objekten im Postfach des Benutzers. Sie können auch das GUI-basierten Compliance-eDiscovery-Tool suchen und gelöschte Elemente in eine PST-Datei exportieren. Der Benutzer wird in PST-Datei verwenden, um die gelöschte Nachrichten mit ihrem Postfach wiederherzustellen. Weitere Informationen finden Sie unter [Wiederherstellen gelöschter Elemente im Postfach eines Benutzers - Admin-Hilfe](#).

## (Optional) Schritt 1: Herstellen einer Verbindung mit Exchange Online mithilfe der Remote-PowerShell

Sie müssen nur diesen Schritt ausführen, wenn Sie eine Exchange Online oder Office 365-Organisation haben. Wenn Sie Exchange Server-Organisation haben, wechseln Sie mit dem nächsten Schritt fort, und führen Sie den Befehl im Exchange Online PowerShell.

1. Öffnen Sie auf Ihrem lokalen Computer Windows PowerShell, und führen Sie dann den folgenden Befehl aus.

```
$UserCredential = Get-Credential
```

<span data-ttu-id="3a490-136">Klicken Sie im Dialogfeld \*\*Windows PowerShell anmelden\*\* Geben Sie Benutzername und Kennwort für Office 365 globaler Administrator-Konto ein, und klicken Sie dann auf \*\*OK\*\*.</span><span class="sxs-lookup"><span data-stu-id="3a490-136">In the \*\*Windows PowerShell Credential Request\*\* dialog box, type username and password for an Office 365 global admin account, and then click \*\*OK\*\*.</span></span>

2. Führen Sie den folgenden Befehl aus.

```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection
```

3. Führen Sie den folgenden Befehl aus.

```
Import-PSSession $Session
```

4. Um zu prüfen, ob Sie mit Ihrer Exchange Online-Organisation verbunden sind, führen Sie den folgenden Befehl aus, um eine Liste aller Postfächer in Ihrer Organisation abzurufen.

```
Get-Mailbox
```

Weitere Informationen oder Hinweise bei Problemen mit der Verbindung zu Ihrer Exchange Online-Organisation finden Sie unter [Herstellen einer Verbindung mit Exchange Online mithilfe der Remote-PowerShell](#).

## Schritt 2: Suchen und Wiederherstellen fehlender Elemente

Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Compliance-eDiscovery" im Thema [Messaging Policy and Compliance Permissions](#).

#### **NOTE**

Compliance-eDiscovery können in der Exchange-Verwaltungskonsole (EAC) Sie nach fehlenden Elementen suchen. Bei der Exchange-Verwaltungskonsole zu verwenden, können nicht Sie jedoch für die Suche in den Ordner wiederherstellbare Elemente einschränken. Nachrichten, die die Suchkriterien entsprechen werden zurückgegeben, auch wenn diese nicht gelöscht werden. Nachdem sie in der angegebenen discoverypostfach wiederhergestellt haben, müssen Sie überprüfen Sie die Ergebnisse der Suche und unnötige Nachrichten vor dem Wiederherstellen der verbleibenden Nachrichten an das Postfach des Benutzers oder Exportieren in eine PST-Datei zu entfernen. > Weitere Informationen zur Verwendung der Exchange-Verwaltungskonsole zum Ausführen einer Compliance-eDiscovery-Suche finden Sie unter [erstellen eine Compliance - eDiscovery-Suche](#).

Der erste Schritt im Wiederherstellungsprozess besteht in der Suche nach Nachrichten im Quellpostfach. Durchsuchen Sie mithilfe einer der folgenden Methoden ein Benutzerpostfach, und kopieren Sie Nachrichten in ein Discoverypostfach.

In diesem Beispiel wird das Postfach von April Stewart nach Nachrichten durchsucht, die folgende Kriterien erfüllen:

- Absender: Ken Kwok
- Schlüsselwort: Seattle

```
Search-Mailbox "April Stewart" -SearchQuery "from:'Ken Kwok' AND seattle" -TargetMailbox "Discovery Search Mailbox" -TargetFolder "April Stewart Recovery" -LogLevel Full
```

#### **NOTE**

Wenn Sie das Cmdlet Search-Mailbox verwenden, können Sie den Suchbereich mithilfe des Parameters SearchQuery definieren, um eine mit Keyword Query Language (KQL) formatierte Abfrage anzugeben. Sie können auch die Option SearchDumpsterOnly angeben, um nur Elemente im Ordner Wiederherstellbare Elemente zu suchen.

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Search-Mailbox](#).

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Um zu prüfen, ob Sie die Nachricht erfolgreich durchsucht haben, die Sie wiederherstellen möchten, melden Sie sich am Discoverypostfach an, das Sie als Zielpostfach ausgewählt haben, und überprüfen Sie die Suchergebnisse.

## Schritt 3: Wiederherstellen wiederhergestellter Elemente

Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Compliance-eDiscovery" im Thema [Messaging Policy and Compliance Permissions](#).

#### **NOTE**

Die Exchange-Verwaltungskonsole kann nicht zum Zurückspeichern wiederherstellter Elemente verwendet werden.

Nach Nachrichten in ein discoverypostfach wiederhergestellt wurden, können Sie das Postfach des Benutzers wiederherstellen mit dem Cmdlet **Search-Mailbox**. In Exchange Server, auch die Cmdlets **New-MailboxExportRequest** und **New-MailboxImportRequest** können Sie die Nachrichten zu exportieren oder importieren Sie die Nachrichten aus einer PST-Datei.

#### **Verwenden von Exchange Online PowerShell zum Wiederherstellen von Nachrichten**

In diesem Beispiel werden Nachrichten im Postfach von April Stewart wiederhergestellt und aus dem Discoverysuchpostfach gelöscht.

```
Search-Mailbox "Discovery Search Mailbox" -SearchQuery "from:'Ken Kwok' AND seattle" -TargetMailbox "April Stewart" -TargetFolder "Recovered Messages" -LogLevel Full -DeleteContent
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Search-Mailbox](#).

### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Um zu prüfen, ob Sie Nachrichten erfolgreich im Postfach des Benutzers wiederhergestellt haben, lassen Sie den Benutzer Nachrichten im Zielordner überprüfen, den Sie im obigen Befehl angegeben haben.

### **(Exchange Server) Verwenden von Exchange Online PowerShell exportieren und Importieren von Nachrichten aus einer PST-Datei**

In Exchange können Server, Sie exportieren Inhalt aus einem Postfach in eine PST-Datei und Import den Inhalt einer PST-Datei an ein Postfach Datei. Weitere Informationen zum Postfach Import / Export finden Sie unter [Understanding Mailbox importieren und Exportieren von Anfragen](#). Das Ausführen dieser Aufgabe in Exchange Online ist nicht möglich.

In diesem Beispiel werden die folgenden Einstellungen zum Exportieren von Nachrichten aus dem Ordner "April Stewart Recovery" im Discoverysuchpostfach in eine PST-Datei exportiert:

- **Mailbox:** Discoverysuchpostfach
- **Des Quellordners:** April Stewart Recovery
- **ContentFilter:** April Reisepläne
- **Pfad der PST-Datei** \\MY SERVER\\HelpDeskPst\\AprilStewartRecovery.pst

```
New-MailboxExportRequest -Mailbox "Discovery Search Mailbox" -SourceRootFolder "April Stewart Recovery" -ContentFilter {Subject -eq "April travel plans"} -FilePath \\MY SERVER\\HelpDeskPst\\AprilStewartRecovery.pst
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-MailboxExportRequest](#).

In diesem Beispiel werden die folgenden Einstellungen zum Importieren von Nachrichten aus einer PST-Datei in den Ordner "Recovered By Helpdesk" im Postfach von April Stewart verwendet:

- **Mailbox:** April Stewart
- **Zielordner:** vom Helpdesk wiederhergestellt
- **Pfad der PST-Datei** \\MY SERVER\\HelpDeskPst\\AprilStewartRecovery.pst

```
New-MailboxImportRequest -Mailbox "April Stewart" -TargetRootFolder "Recovered By Helpdesk" -FilePath \\MY SERVER\\HelpDeskPst\\AprilStewartRecovery.pst
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-MailboxImportRequest](#).

### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Um zu prüfen, ob Sie Nachrichten erfolgreich in eine PST-Datei exportiert haben, öffnen Sie die PST-Datei in Outlook, und überprüfen Sie ihren Inhalt. Um zu prüfen, ob Sie Nachrichten erfolgreich aus der PST-Datei importiert haben, lassen Sie den Benutzer den Inhalt des Zielordners überprüfen, den Sie im obigen Befehl angegeben haben.

## Weitere Informationen

- Die Möglichkeit zum Wiederherstellen gelöschter Objekte ist durch die Wiederherstellung einzelner Elemente, aktiviert die ermöglicht es Administratoren, eine Nachricht wiederherzustellen, die von einem Benutzer oder durch Aufbewahrungsrichtlinie gelöscht wird, solange die Aufbewahrungszeit für gelöschte Elemente für dieses Element abgelaufen ist. Weitere Informationen zum Wiederherstellen einzelner Elemente finden Sie unter [Recoverable Items Folder](#).
- Exchange Online-Postfachs ist für gelöschte Elemente 14 Tage lang aufbewahrt werden standardmäßig konfiguriert. Sie können diese Einstellung auf ein Maximum von 30 Tagen ändern. In Exchange Server ist eine Postfachdatenbank konfiguriert 14 Tagen gelöschte Elemente aufbewahrt werden standardmäßig. Sie können die Einstellungen für die Aufbewahrung gelöschter Elemente für ein Postfach oder Postfachdatenbank konfigurieren. Weitere Informationen finden Sie unter:
  - Ändern des Aufbewahrungszeitraums für gelöschte Elemente für ein Exchange Online-Postfach
  - Konfigurieren der Aufbewahrungszeit für gelöschte Elemente und Kontingente für wiederherstellbare Elemente
- Wie bereits erklärt können Sie auch das Compliance-eDiscovery-Tool suchen und gelöschte Elemente in eine PST-Datei exportieren. Der Benutzer wird in PST-Datei verwenden, um die gelöschte Nachrichten mit ihrem Postfach wiederherzustellen. Weitere Informationen finden Sie unter [Wiederherstellen gelöschter Elemente im Postfach eines Benutzers - Admin-Hilfe](#).
- Benutzer können ein gelöschtes Element wiederherstellen, wenn es nicht gelöscht wurde und wenn die Aufbewahrungsdauer für das gelöschte Element nicht abgelaufen ist. Sollte ein Benutzer gelöschte Elemente aus dem Ordner "Wiederherstellbare Elemente" wiederherstellen müssen, verweisen Sie ihn auf die folgenden Themen:
  - [Wiederherstellen gelöschter Elemente in Outlook 2010](#)
  - [Wiederherstellen gelöschter Elemente in Outlook 2013](#)
  - [Wiederherstellen gelöschter Elemente oder E-Mails in Outlook Online](#)
- In diesem Thema wird das Verwenden Sie das Cmdlet **Search-Mailbox** zum Suchen nach und Wiederherstellen von fehlenden Elementen veranschaulicht. Wenn Sie dieses Cmdlet verwenden, können Sie nur ein Postfach gleichzeitig zu suchen. Wenn Sie mehrere Postfächer gleichzeitig suchen möchten, können Sie [Compliance - eDiscovery](#) in der Exchange-Verwaltungskonsole (EAC) oder das Cmdlet "[New-MailboxSearch](#)" in Windows PowerShell verwenden.
- Zusätzlich zur Verwendung dieser Prozedur zum Suchen und Wiederherstellen gelöschter Elemente können Sie auch eine ähnliche Prozedur verwenden, um nach Elementen in Benutzerpostfächern zu suchen und um diese dann aus dem Quellpostfach zu löschen. Weitere Informationen finden Sie unter [Suchen und Löschen von Nachrichten](#).

# Verwenden von Exchange Online PowerShell zum Anzeigen von Informationen zu Office 365-Postfächern

18.12.2018 • 6 minutes to read

Administratoren erfahren, wie Sie Exchange Online PowerShell zum Anzeigen von Informationen über Postfächer in ihrer Office 365-Organisation verwenden können.

Um Ihnen ein Gefühl davon vermitteln zu können, welche Möglichkeiten Ihnen mit PowerShell und Office 365 zur Verfügung stehen, werfen wir einen Blick auf die Benutzerpostfächer in Exchange Online PowerShell.

## Bevor Sie beginnen:

Informationen zum Herstellen einer Verbindung mit Exchange Online mit PowerShell finden Sie unter [Herstellen einer Verbindung mit Exchange Online mithilfe der Remote-PowerShell](#).

## Anzeigen von Postfachinformationen mit Exchange Online PowerShell

Sie können Informationen zu einem einzelnen Benutzerfach leicht abrufen. Hier ist beispielsweise ein Befehl, mit dem Informationen zum Postfach von Ken Myer zurückgegeben werden können:

```
Get-Mailbox -Identity "Ken Myer"
```

Dieser Befehl gibt etwas zurück, was Folgendem ähnelt:

Name	Alias	ServerName	ProhibitSendQuota
---	---	-----	-----
kenmyer	kenmyer	bn1pr02mb038	49.5 GB (53,150,220,288 bytes)

Sie können den Alias und die Größe des Postfachkontingents von Ken sehen. Aber ein Exchange Online-Postfach ist viel umfangreicher als nur diese vier Eigenschaften, die vom **Get-Mailbox** -Cmdlet zurückgegeben werden.

Hier ist ein Beispielbefehl, der alle Informationen für ein bestimmtes Postfach anzeigt:

```
Get-Mailbox -Identity "Ken Myer" | Format-List
```

Der Befehl weist Exchange Online PowerShell an, alle verfügbaren Eigenschaften für das Postfach in einer Liste zurückzugeben. Es gibt ungefähr 200 unterschiedliche Eigenschaften und Eigenschaftswerte. Sie können auch die **Format-List** - und **Format-Table** -Cmdlets verwenden, um nur bestimmte Eigenschaftswerte zurückzugeben. Mit dem folgenden Befehl können Sie z. B. auch aufbewahrungsbezogene Eigenschaften für Ken Myer anzeigen:

```
Get-Mailbox -Identity "Ken Myer" | Format-List DisplayName, LitigationHoldEnabled, LitigationHoldDate,  
LitigationHoldOwner, LitigationHoldDuration
```

Sie können auch Platzhalterzeichen verwenden, bei der Arbeit mit dem Cmdlet **Format-List**. Alle der Aufbewahrung für eventuelle Rechtsstreitigkeiten beispielsweise Eigenschaften beginnen mit einem Buchstaben von `lit`. Sie können die gleiche Informationen abrufen, mit dem folgenden Befehl:

```
Get-Mailbox -Identity "Ken Myer" | Format-List DisplayName, Lit*
```

Dieser Befehl gibt **Get-Mailbox**, um den Wert von Ken **DisplayName**-Eigenschaft und die Werte der Eigenschaften abzurufen, deren Namen, die mit einem Buchstaben beginnen **lit**. Es folgt ein Beispiel für ähnliche erhalten:

```
DisplayName : Ken Myer
LitigationHoldEnabled : False
LitigationHoldDate :
LitigationHoldOwner :
LitigationHoldDuration : Unlimited
```

Sie können Informationen über mehrere Postfächer durch Auslassen des Parameters *Identity* zurückzugeben. In diesem Beispiel wird die **DisplayName** und **LitigationHoldEnabled** Eigenschaften für alle Postfächer zurückgegeben:

```
Get-Mailbox -ResultSize unlimited | Format-Table -Auto DisplayName, LitigationHoldEnabled
```

In vielen Fällen möchten Sie nur eine Teilmenge Ihrer Postfächer betrachten. Gehen wir beispielsweise davon aus, Sie sollen eine Liste von allen Postfächern erstellen, denen ein Beweissicherungsverfahren zugewiesen wurde. Sie können das **Where-Object**-Cmdlet in Verbindung mit dem **Get-Mailbox**-Cmdlet verwenden. Das **Where-Object**-Cmdlet benötigt einen Filterausdruck, um Exchange Online PowerShell anzulegen, an welcher Gruppe von Postfächern Sie interessiert sind.

Verwenden Sie die Syntax in ihrer einfachsten Form Filter Ausdrücke

```
{<PropertyName> -<ComparisonOperator> <PropertyValue>} .
```

Hier sind die am häufigsten verwendeten Vergleichsoperatoren:

- **eq** (gleich; unterscheidet nicht zwischen Groß- und Kleinschreibung)
- **ne** (ungleich; unterscheidet nicht zwischen Groß- und Kleinschreibung)
- **gt** (größer als)
- **lt** (kleiner als)

Eine vollständige Liste der Vergleichsoperatoren finden Sie unter [Where-Object](#).

Werte für **<PropertyValue>** hängen die-Eigenschaft, und die Werte wie Zeichenfolgen, Zahlen, boolesche Werte werden kann (**\$True** oder **\$False**), oder keinen Wert (**\$Null**). Textwerte mit Leerzeichen ist der Wert in Anführungszeichen erforderlich. Numerische Werte, boolesche Werte und **\$Null** den Wert in Anführungszeichen ist nicht erforderlich.

Wechseln Sie wieder zu unserem Beispiel aller halten Sie die Postfächer, die eine Aufbewahrung für eventuelle zugewiesen wurden, der Filter-Ausdruck ist **{LitigationHoldEnabled -eq \$True}**:

- Ist der Name der Eigenschaft **LitigationHoldEnabled**.
- Ist der Vergleichsoperator **eq**.
- Ist der Wert der Eigenschaft wir suchen nach **\$True**.

Wenn Sie den Filterausdruck haben, können Sie den **Where-Object**-Teil des Befehls mit der folgenden Syntax erstellen:

```
Get-Mailbox -ResultSize unlimited | Where-Object {$_.<Filter Phrase>}
```

Hier ist der Befehl für unser Beispiel:

```
Get-Mailbox -ResultSize unlimited | Where-Object {$_.LitigationHoldEnabled -eq $True}
```

Gehen wir davon aus, Sie möchten sicherstellen, dass bei allen Benutzern die Junk-E-Mail-Regel aktiviert ist. Hier finden Sie einen schnellen Befehl zum Ermitteln, bei welchen Benutzern die Regel nicht aktiviert ist:

```
Get-Mailbox -ResultSize unlimited | Get-MailboxJunkEmailConfiguration | Where-Object {$_.Enabled -eq $False}
```

Dies ist nur ein Beispiel. Wenn Sie eine Reihe von Postfächern basierend auf einer Einstellung anzeigen möchten und in Office 365 Admin Center nicht nach dieser Einstellung filtern können, gehen Sie folgendermaßen vor:

1. Hier finden Sie die Mailbox-Eigenschaft, die die Einstellung entspricht, mithilfe des Befehls interessiert sind

`Get-Mailbox -Identity "<MailboxIdentity>" | Select-Object *` zum Auflisten aller Eigenschaften eines Postfachs an. `<MailboxIdentity>` ist eine beliebige eindeutige ID für das Postfach (Name, e-Mail-Adresse, Alias, usw.).

2. Erstellen Sie Ihre Office 365 PowerShell-Befehl wie folgt:

```
Get-Mailbox -ResultSize unlimited | Where-Object {$_.<PropertyName> -<ComparisonOperator> <PropertyValue>}
```

# Erstellen und Verwalten von Verteilergruppen

18.12.2018 • 31 minutes to read

Verwenden Sie die Exchange-Verwaltungskonsole (EAC) oder Exchange Online PowerShell zum Erstellen einer neuen Verteilergruppe in Ihrer Exchange Online-Organisation oder für eine vorhandene Gruppe e-Mail aktivieren.

Es gibt zwei Arten von Gruppen, die zum Verteilen von Nachrichten verwendet werden können:

- E-Mail-aktivierte universelle Verteilergruppen (werden auch als Verteilergruppen bezeichnet) können ausschließlich zum Verteilen von Nachrichten verwendet werden.
- E-Mail-aktivierte universelle Sicherheitsgruppen (auch als Sicherheitsgruppen bezeichnet) können zum Verteilen von Nachrichten als auch über das Erteilen von Zugriffsberechtigungen auf Ressourcen verwendet werden. Weitere Informationen finden Sie unter [Verwalten von e-Mail-aktivierten Sicherheitsgruppen](#).

Es ist wichtig, beachten Sie die Terminologie Unterschiede zwischen Active Directory und Exchange Online. In Active Directory bezieht sich eine Verteilergruppe auf keiner Gruppe, die einen Sicherheitskontext nicht, ob sie e-Mail-aktivierten oder nicht. Im Gegensatz dazu werden in Exchange alle e-Mail-aktivierten Gruppen als Verteilergruppen bezeichnet, ob sie einen Sicherheitskontext besitzen.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 bis 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Verteilergruppen" im Thema [Empfängerberechtigungen](#).
- Wenn Ihre Organisation eine gruppenbenennungsrichtlinie konfiguriert hat, wird es nur für Gruppen von Benutzern erstellte angewendet. Wenn Sie oder andere Administratoren der Exchange-Verwaltungskonsole Erstellen von Verteilergruppen mithilfe, die gruppenbenennungsrichtlinie wird ignoriert, und ist nicht auf den Namen der Gruppe angewendet. Bei Verwendung von Exchange Online PowerShell erstellen, oder benennen Sie eine Verteilergruppe ist jedoch die Richtlinie angewendet, es sei denn, Sie den *IgnoreNamingPolicy* -Parameter verwenden, um die gruppenbenennungsrichtlinie außer Kraft setzen. Weitere Informationen finden Sie unter:
  - [Erstellen einer Benennungsrichtlinie für Verteilergruppen](#)
  - [Außerkraftsetzen der Benennungsrichtlinie für Verteilergruppen](#)

## Erstellen einer Verteilergruppe

### Erstellen einer Verteilergruppe mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**.
2. Klicken Sie auf **neu**  > **Verteilergruppe**.

 **New!** Try Office 365 Groups, the next generation of distribution lists.  
Groups give teams tools to collaborate using email, shared files, a calendar, and more. [Learn more about Office 365 Groups](#).

3. Wenn Sie ein Office 365 für Unternehmen Plan oder ein Exchange Online-Plan haben, können Sie nun

eine Office 365-Gruppe statt einer Verteilergruppe erstellen. Office 365 Gruppen müssen die Funktionen einer Verteilergruppe und vieles mehr. Mit Office 365-Gruppen können Sie e-Mail an eine Gruppe senden, allgemeinen Kalender freigeben, eine Bibliothek zum Speichern von und arbeiten auf Gruppendateien und Ordner haben. Klicken Sie auf **neu** > **Office 365-Gruppe** zum Einstieg in die und checken Sie [Gruppen für Office 365 - Admin-Hilfe](#).

Wenn Sie vorhandene Verteilergruppen, die Sie zu Office 365 Gruppen migrieren möchten verfügen, checken Sie das [Migrieren von Verteilerlisten zu Office 365 Gruppen - Admin-Hilfe](#).

Wenn Sie weiterhin eine Verteilergruppe erstellen möchten, klicken oder tippen Sie auf den Assistenten für **Neue Verteilergruppe**.

4. Füllen Sie auf der Seite **Neue Verteilergruppe** die folgenden Felder aus:

- \*\*\* Anzeigenamen\*\*: Geben Sie den Anzeigenamen in diesem Feld können. Dieser Name erscheint im Adressbuch Ihrer Organisation, in der: Linie, wenn e-Mail an diese Gruppe, und klicken Sie in der Liste der Gruppen in der Exchange-Verwaltungskonsole gesendet wird. Der Anzeigename ist erforderlich und sollte benutzerfreundlichen sein, damit Personen erkannt wird. Es muss eindeutig auch in der Gesamtstruktur sein.
- \*\*\* Alias\*\*: in diesem Feld können Sie den Namen des Alias für die Gruppe eingeben. Der Alias darf 64 Zeichen nicht überschreiten und muss in der Gesamtstruktur eindeutig sein. Wenn ein Benutzer den Alias zu macht: Zeile einer e-Mail-Nachricht, es in der Gruppe Anzeigenamen aufgelöst wird.
- **Organisationseinheit** (Sie sehen nur diese Option in Exchange Server lokal) Sie können eine Organisationseinheit (OU) als die Standardstärke auswählen (Dies ist der Empfängerbereich). Wenn der Empfängerbereich auf die Gesamtstruktur festgelegt ist, wird der Standardwert in den Container Users in Active Directory-Domäne festgelegt, die den Computer enthält, auf dem der Exchange-Verwaltungskonsole ausgeführt wird. Wenn der Empfängerbereich auf eine bestimmte Domäne festgelegt ist, ist der Container "Users" in dieser Domäne standardmäßig aktiviert. Wenn der Empfängerbereich auf eine bestimmte Organisationseinheit festgelegt ist, ist dieser Organisationseinheit standardmäßig aktiviert.

Um eine andere Organisationseinheit auszuwählen, klicken Sie auf **Durchsuchen**. In diesem Dialogfeld werden alle Organisationseinheiten der Gesamtstruktur angezeigt, die sich in einem bestimmten Bereich befinden. Wählen Sie die gewünschte Organisationseinheit aus, und klicken Sie dann auf **OK**.

- \*\*\* Besitzer\*\*: die Person, die eine Gruppe erstellt wird standardmäßig der Besitzer. Alle Gruppen müssen Sie mindestens einen Besitzer haben. Sie können Besitzer hinzufügen, indem Sie auf **Hinzufügen**.
- **Member**: Verwenden Sie diesen Abschnitt zum Hinzufügen von Mitgliedern und um anzugeben, ob die Genehmigung ist erforderlich, damit Benutzern beitreten oder diese verlassen der Gruppe.

Besitzer von Gruppen müssen nicht Mitglied der Gruppe sein. Verwenden Sie die Option **Gruppenbesitzer als Mitglieder hinzufügen**, um die Besitzer als Mitglieder hinzuzufügen bzw. zu entfernen.

Klicken Sie auf **Hinzufügen**, um Mitglieder der Gruppe hinzuzufügen. Wenn Sie das Hinzufügen von Mitgliedern abgeschlossen haben, klicken Sie auf **OK**, um zur Seite **neue Verteilergruppe** zurückzukehren.

Geben Sie unter **Wählen Sie aus, ob für den Beitritt zur Gruppe eine Besitzergenehmigung erforderlich ist** an, ob eine Genehmigung erforderlich ist, damit Benutzer der Gruppe beitreten können. Wählen Sie eine der folgenden Einstellungen aus:

- **Open: jeder kann diese Gruppe ohne Genehmigung durch die Gruppenbesitzer beitreten**: Dies

ist die Standardeinstellung.

- **Geschlossen:** Mitglieder können nur von den Gruppenbesitzern hinzugefügt werden. Alle Beitrittsanforderungen werden automatisch zurückgewiesen
- **Besitzergenehmigung:** alle Anfragen manuell genehmigt oder abgelehnt werden durch die Gruppenbesitzer: Wenn Sie diese Option auswählen, die Besitzer der Gruppe oder der Besitzer erhält eine e-Mail-Nachricht anfordern der Genehmigung für die Gruppe.

Geben Sie unter **Wählen Sie aus, ob die Gruppe zum Verlassen geöffnet ist** an, ob eine Genehmigung erforderlich ist, wenn Benutzer die Gruppe verlassen möchten. Wählen Sie eine der folgenden Einstellungen aus:

- **Open:** jeder kann diese Gruppe ohne Genehmigung durch die Gruppenbesitzer verlassen: Dies ist die Standardeinstellung.
- **Geschlossen:** Mitglieder können nur durch die Gruppenbesitzer entfernt werden. Alle Anfragen zu belassen, werden automatisch abgelehnt

5. Wenn Sie fertig sind, klicken Sie auf **Speichern**, um die Verteilergruppe erstellen.

#### NOTE

Standardmäßig ist für neue Verteilergruppen die Authentifizierung aller Absender erforderlich. Auf diese Weise wird verhindert, dass externe Absender Nachrichten an Verteilergruppen senden können. Um eine Verteilergruppe für das Annehmen von Nachrichten von allen Absendern zu konfigurieren, müssen Sie die Einstellungen für die Einschränkungen der Nachrichtenübermittlung für die betreffende Verteilergruppe ändern.

### Verwenden von Exchange Online PowerShell zum Erstellen einer Verteilergruppe

In diesem Beispiel wird eine Verteilergruppe mit dem Alias **itadmin** und dem Namen **IT Administrators** erstellt. Die Verteilergruppe wird in der Standardorganisationseinheit erstellt, und jeder kann ohne Genehmigung der Gruppenbesitzer dieser Gruppe beitreten.

```
New-DistributionGroup -Name "IT Administrators" -Alias itadmin -MemberJoinRestriction open
```

Weitere Informationen zur Verwendung von Exchange Online PowerShell zum Erstellen von Verteilergruppen finden Sie unter [New-DistributionGroup](#).

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um die erfolgreiche Erstellung einer Verteilergruppe zu überprüfen:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**. Die neue Verteilergruppe wird in der Gruppenliste angezeigt. Unter **Gruppentyp** lautet der Typ **Verteilergruppe**.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl zum Anzeigen von Informationen zur neuen Verteilergruppe ein.

```
Get-DistributionGroup <Name> | Format-List Name,RecipientTypeDetails,PrimarySmtpAddress
```

#### NOTE

Sie können erstellen oder e-Mail-nur universelle Verteilergruppen zu aktivieren. Um eine lokale Domäne oder eine globale Gruppe in eine universelle Gruppe konvertieren möchten, können Sie das Cmdlet [Set-Group](#) von Exchange Online PowerShell verwenden. Sie müssen möglicherweise e-Mail-aktivierte Gruppen, die von früheren Versionen von Exchange migriert wurden, die nicht universelle Gruppen sind. Der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell können Sie diese Gruppen verwalten

## Ändern von Verteilergruppeneigenschaften

### Ändern von Verteilergruppeneigenschaften mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**.
2. Klicken Sie in der Liste der Gruppen, klicken Sie auf die Verteilergruppe, die Sie anzeigen oder ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Eigenschaftenseite für die Gruppe auf einen der folgenden Abschnitte, um Eigenschaften anzuzeigen oder zu ändern.

#### Allgemein

Verwenden Sie diesen Abschnitt, um grundlegende Informationen zur Gruppe anzuzeigen oder zu ändern.

- \*\* \* Anzeigenamen\*\*: dieser Name erscheint im Adressbuch in der: Linie, wenn e-Mail an diese Gruppe, und klicken Sie in der Liste Gruppen gesendet wird. Der Anzeigename ist erforderlich und sollte benutzerfreundlichen sein, damit Personen erkannt wird. Es muss auch in Ihrer Domäne eindeutig sein.

Wenn Sie eine Gruppenbenennungsrichtlinie implementiert haben, muss der Anzeigename dem von der Richtlinie definierten Namensformat entsprechen.

- \*\*\* Alias\*\*: Dies ist der Teil der e-Mail-Adresse, die auf der linken Seite des angezeigt wird die am (@) Symbol. Wenn Sie den Alias ändern, die primäre SMTP-Adresse für die Gruppe wird auch geändert werden, und den neuen Alias enthalten. Darüber hinaus wird mit dem vorherigen Alias die e-Mail-Adresse als Proxyadresse für die Gruppe beibehalten.
- **Beschreibung:** in diesem Feld können Sie die Gruppe beschreiben, damit die Benutzer wissen, was der Zweck der Gruppe ist. Diese Beschreibung wird im Adressbuch und in der Exchange-Verwaltungskonsole im Detailfenster angezeigt.
- **Diese Gruppe aus Adresslisten ausgeblendet:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie nicht, dass Benutzer diese Gruppe im Adressbuch anzeigen möchten. Zum Senden von e-Mails an diese Gruppe hat ein Absender in der die Gruppe Alias oder die e-Mail-Adresse eingeben: oder Cc: Zeilen.

#### TIP

Blenden Sie ggf. Sicherheitsgruppen aus, da sie normalerweise zum Zuweisen von Berechtigungen zu Gruppenmitgliedern und nicht zum Senden von E-Mails verwendet werden.

- **Organisationseinheit:** Dieses schreibgeschützte Feld zeigt die Organisationseinheit (OU), die die Verteilergruppe enthält. Sie müssen Active Directory-Benutzer und-Computer verwenden, um die Gruppe in eine andere Organisationseinheit verschieben.

#### Besitz

Verwenden Sie diesen Abschnitt, um Gruppenbesitzer zuzuweisen. Der Gruppenbesitzer kann der Gruppe Mitglieder hinzufügen, Beitrags- oder Austrittsanfragen genehmigen oder ablehnen sowie an die Gruppe

gesendete Nachrichten genehmigen oder ablehnen. Standardmäßig ist die Person, die eine Gruppe erstellt, deren Besitzer. Jede Gruppe muss mindestens einen Besitzer aufweisen.

Sie können Besitzer hinzufügen, indem Sie auf **Hinzufügen**  . Sie können einen Besitzer entfernen, indem Sie den Besitzer auswählen und dann auf **Entfernen**

#### **Mitgliedschaft**

Verwenden Sie diesen Abschnitt hinzufügen oder Entfernen von Mitgliedern aus. Gruppenbesitzer müssen keine Mitglieder der Gruppe sein. Klicken Sie unter **Mitglieder** können Sie Mitglieder hinzufügen, indem Sie auf **Hinzufügen**  . Sie können ein Element entfernen, indem Sie einen Benutzer in der Mitgliederliste auswählen und dann auf **Entfernen**

#### **Genehmigung der Mitgliedschaft**

In diesem Abschnitt können Sie angeben, ob eine Genehmigung erforderlich ist, damit Benutzer der Gruppe betreten bzw. diese verlassen können.

- **Wählen Sie, ob besitzergenehmigung erforderlich ist, um der Gruppe**

"Leistungsprotokollbenutzer": Wählen Sie eine der folgenden Einstellungen:

- **Offen: Jeder Benutzer kann dieser Gruppe ohne Genehmigung durch die Gruppenbesitzer beitreten**
- **Geschlossen: Mitglieder können nur von den Gruppenbesitzern hinzugefügt werden. Alle Beitragsanforderungen werden automatisch zurückgewiesen**
- **Besitzergenehmigung: alle Anfragen genehmigt oder abgelehnt werden durch die Gruppenbesitzer:** Wenn Sie diese Option auswählen, die Besitzer der Gruppe oder Besitzer empfangen eine e-Mail anfordern der Genehmigung für die Gruppe "Leistungsprotokollbenutzer".
- **Wählen Sie, ob die Gruppe zum verlassen geöffnet ist:** Wählen Sie eine der folgenden Einstellungen:
  - **Offen: Jeder kann diese Gruppe lassen ohne Genehmigung durch die Gruppenbesitzer**
  - **Geschlossen: Mitglieder können nur durch die Gruppenbesitzer entfernt werden. Alle Anfragen zu belassen, werden automatisch abgelehnt**

#### **Zustellungsverwaltung**

In diesem Abschnitt können Sie verwalten, von wem E-Mails an diese Gruppe gesendet werden können.

- **Nur Absender innerhalb meiner Organisation:** Wählen Sie diese Option, um nur Absender in Ihrer Organisation Nachrichten an die Gruppe senden können. Dies bedeutet, dass wenn eine Person außerhalb Ihrer Organisation an diese Gruppe eine e-Mail-Nachricht sendet, werden sie abgelehnt, wird. Dies ist die Standardeinstellung.
- **Absender innerhalb und außerhalb meiner Organisation:** Wählen Sie diese Option, damit alle Benutzer Nachrichten an die Gruppe senden können.

Sie können weiter einschränken, wer Nachrichten an die Gruppe durch Zulassen der nur bestimmte Absender zum Senden von Nachrichten an diese Gruppe senden können. Klicken Sie auf **Hinzufügen**  und wählen Sie dann einen oder mehrere Empfänger aus. Wenn Sie diese Liste Absender hinzufügen, werden sie die einzigen Benutzer, die e-Mail-Nachrichten an die Gruppe senden können. E-Mails, die von jeder Person nicht in der Liste gesendet wird zurückgewiesen.

Wenn eine Person oder eine Gruppe aus der Liste entfernen möchten, wählen sie in der Liste aus, und klicken Sie dann auf **Entfernen**

## **IMPORTANT**

Wenn Sie die Gruppe so konfiguriert haben, dass nur Absender in der Organisation Nachrichten an die Gruppe senden dürfen, werden von E-Mail-Kontakten gesendete E-Mails abgelehnt, auch wenn sie dieser Liste hinzugefügt werden.

### **Nachrichtenbestätigung**

In diesem Abschnitt können Sie Optionen zum Moderieren der Gruppe festlegen. Moderatoren genehmigen Nachrichten, die an die Gruppe gesendet werden, oder weisen sie zurück, bevor diese die Gruppenmitglieder erreichen.

- **An diese Gruppe gesendete Nachrichten von einem Moderator genehmigt werden müssen:** dieses Kontrollkästchen ist nicht standardmäßig aktiviert. Wenn Sie dieses Kontrollkästchen aktivieren, werden von den gruppenmoderatoren vor der Zustellung eingehende Nachrichten überprüft. Gruppenmoderatoren können genehmigen oder ablehnen eingehender Nachrichten.
- **Gruppenmoderatoren:** Klicken Sie auf **Hinzufügen**, um gruppenmoderatoren hinzuzufügen, [ ] . Um einen Moderator zu entfernen, wählen Sie aus der Moderator, und klicken Sie dann auf **Entfernen** [ ]. Wenn Sie "An diese Gruppe gesendete Nachrichten sind vom Moderator genehmigt werden" ausgewählt und Sie keinen Moderator auswählen haben, werden Nachrichten an die Gruppe zur Genehmigung an die Gruppenbesitzer gesendet.
- **Absender, die nachrichtengenehmigung erfordern keinen:** Hinzufügen von Personen oder Gruppen, die für diese Gruppe Moderation umgangen werden können, klicken Sie auf **Add** [ ]. Um eine Person oder eine Gruppe zu entfernen, wählen Sie das Element aus, und klicken Sie dann auf **Entfernen** [ ].
- **Wählen Sie für die Moderation Benachrichtigungen:** Verwenden Sie diesen Abschnitt, um festzulegen, wie Benutzer über nachrichtengenehmigungen benachrichtigt werden.
  - **Wenn Ihre Nachrichten genehmigt werden nicht alle Absender benachrichtigen:** Dies ist die Standardeinstellung. Benachrichtigen Sie alle Absender, innerhalb und außerhalb Ihrer Organisation, wenn ihre Nachricht nicht genehmigt wird.
  - **Absender benachrichtigen, in Ihrer Organisation, wenn ihre Nachrichten genehmigt werden nicht:** Wenn Sie diese Option auswählen, nur Personen oder Gruppen in Ihrer Organisation werden benachrichtigt, wenn eine Nachricht, die sie an die Gruppe gesendet nicht von einem Moderator genehmigt wird.
  - **Nicht benachrichtigt, wenn eine Nachricht nicht genehmigt wird:** Wenn Sie diese Option auswählen, werden nicht an den Absender einer Nachricht, deren Nachrichten nicht von den gruppenmoderatoren genehmigt, Benachrichtigungen gesendet.

### **E-Mail-Optionen**

In diesem Abschnitt können Sie die E-Mail-Adressen anzeigen und ändern, die der Gruppe zugeordnet sind. Dazu gehören die primären SMTP-Adressen der Gruppe sowie alle zugeordneten Proxyadressen. Die primäre SMTP-Adresse (auch als Antwortadresse bezeichnet) wird fettgedruckt in der Adressliste angezeigt. Der Wert **SMTP** in der Spalte **Typ** wird dabei in Großbuchstaben angegeben.

- **Hinzufügen:** Klicken Sie auf **Add** [ ] So fügen Sie eine neue e-Mail-Adresse für dieses Postfach hinzu. Wählen Sie eine der folgenden Adresstypen:
  - **SMTP:** Dies ist die Adresse. Klicken Sie auf diese Schaltfläche, und geben Sie dann die neue SMTP-Adresse in der \*\* \* E-Mail-Adresse\*\* Feld.

#### **NOTE**

Damit die neue Adresse die primäre SMTP-Adresse der Gruppe wird, aktivieren Sie das Kontrollkästchen **Diese Adresse als Antwortadresse verwenden.**

- **Benutzerdefinierte Adresstyp:** Klicken Sie auf diese Schaltfläche, und geben Sie einen der unterstützten nicht-SMTP-e-Mail-Adressotypen in der \*\*\* E-Mail-Adresse\*\* Feld.

#### **NOTE**

Mit Ausnahme von X.400-Adressen überprüft Exchange benutzerdefinierte Adressen nicht auf ordnungsgemäße Formatierung. Sie müssen sicherstellen, dass die von Ihnen angegebene benutzerdefinierte Adresse die Formatanforderungen für den jeweiligen Adressotyp erfüllt.

- **Bearbeiten:** um eine der Gruppe zugeordnete e-Mail-Adresse zu ändern, wählen Sie sie in der Liste aus, und klicken Sie dann auf **Bearbeiten** .

#### **NOTE**

Damit eine vorhandene Adresse die primäre SMTP-Adresse der Gruppe wird, aktivieren Sie das Kontrollkästchen **Diese Adresse als Antwortadresse verwenden.**

- **Entfernen:** um eine e-Mail-Adresse der Gruppe zugeordnete zu löschen, wählen Sie sie in der Liste aus, und klicken Sie dann auf **Entfernen** .
- **E-Mail-Adressen basierend auf der e-Mail-Adressrichtlinie angewendet an diesen Empfänger automatisch aktualisieren:** Aktivieren Sie dieses Kontrollkästchen, um dem Empfänger der e-Mail-Adressen automatisch aktualisierte basierend auf Änderungen an e-Mail-Adressrichtlinien in Ihrer Organisation. Dieses Feld ist standardmäßig aktiviert.

#### **E-Mail-Info**

Verwenden Sie diesen Abschnitt, um eine E-Mail-Info hinzuzufügen, in der Benutzer vor möglichen Problemen gewarnt werden, wenn sie eine Nachricht an diese Gruppe senden. Eine E-Mail-Info ist Text, der in der Infoleiste angezeigt wird, wenn diese Gruppe der Zeile "An", "Cc" oder "Bcc" einer neuen E-Mail hinzugefügt wird. Sie könnten z. B. großen Gruppen eine E-Mail-Info hinzufügen, um potenzielle Absender zu warnen, dass ihre Nachricht an viele Personen gesendet wird.

#### **NOTE**

Eine E-Mail-Info kann HTML-Tags enthalten, Skripts sind jedoch nicht zulässig. Die Länge einer benutzerdefinierten E-Mail-Info darf 175 angezeigte Zeichen nicht überschreiten. HTML-Tags werden bei diesem Zeichenlimit nicht mitgezählt.

#### **Gruppendelegierung**

In diesem Abschnitt können Sie einem Benutzer (der als Stellvertretung bezeichnet wird) Berechtigungen zuweisen, sodass der Benutzer Nachrichten als die Gruppe oder im Namen der Gruppe senden kann. Sie können die folgenden Berechtigungen zuweisen:

- **Senden als:** Diese Berechtigung ermöglicht es der Stellvertretung zum Senden von Nachrichten als Gruppe. Nachdem diese Berechtigung zugewiesen wurde, verfügt die Stellvertretung über die Option zum Hinzufügen der Gruppe in die Zeile **aus**, um anzugeben, dass die Nachricht von der Gruppe gesendet wurde.

- **Senden im Auftrag von:** mit dieser Berechtigung können auch eine Stellvertretung, Nachrichten im Namen der Gruppe zu senden. Nachdem diese Berechtigung zugewiesen wurde, verfügt die Stellvertretung über die Option zum Hinzufügen der Gruppe in **der Zeile**. Die Nachricht wird angezeigt, die von der Gruppe gesendet werden, und es wird angenommen, dass sie durch den Delegaten im Namen der Gruppe gesendet wurde.

Wenn Sie einer Stellvertretung eine Berechtigung zuweisen möchten, klicken Sie unter der entsprechenden Berechtigung auf **Hinzufügen**, um die Seite **Empfänger auswählen** anzuzeigen, auf der eine Liste mit allen Empfängern in der Exchange-Organisation angezeigt wird, denen die Berechtigung zugewiesen werden kann. Wählen Sie die gewünschten Empfänger aus, fügen Sie diese der Liste hinzu, und klicken Sie dann auf **OK**. Sie können auch nach einem bestimmten Empfänger suchen, indem Sie seinen Namen in das Suchfeld eingeben und dann auf **Suchen** klicken.

#### **Verwenden von Exchange Online PowerShell Verteilergruppeneigenschaften ändern**

Verwenden Sie die Cmdlets **Get-DistributionGroup** und **Set-DistributionGroup**, anzeigen und Ändern der Eigenschaften für Verteilergruppen. Vorteile der Verwendung von Exchange Online PowerShell sind die Möglichkeit zum Ändern der Eigenschaften, die in der Exchange-Verwaltungskonsole nicht verfügbar sind und Sie die Eigenschaften für mehrere Gruppen ändern. Informationen darüber, welche Parameter Verteilergruppeneigenschaften entsprechen, finden Sie unter den folgenden Themen:

- [Get-DistributionGroup](#)
- [Set-DistributionGroup](#)

Hier sind einige Beispiele für die Verwendung von Exchange Online PowerShell Verteilergruppeneigenschaften ändern.

In diesem Beispiel wird die primäre SMTP-Adresse (wird auch als Antwortadresse bezeichnet) für die Verteilergruppe "Seattle Employees" von "employees@contoso.com" in "sea.employees@contoso.com" geändert. Zudem wird die vorherige Adresse als Proxyadresse beibehalten.

```
Set-DistributionGroup "Seattle Employees" -EmailAddresses
SMTP:sea.employees@contoso.com,smtp:employees@contoso.com
```

In diesem Beispiel wird die maximale Größe von Nachrichten, die an alle Verteilergruppen in der Organisation gesendet werden können, auf 10 Megabytes (MB) beschränkt.

```
Get-DistributionGroup -ResultSize unlimited -Filter {(RecipientTypeDetails -eq
'MailUniversalDistributionGroup')} | Set-DistributionGroup -MaxReceiveSize 10MB
```

In diesem Beispiel wird die Moderation für die Verteilergruppe "Customer Support" aktiviert und der Moderator auf "Amy" festgelegt. Zusätzlich werden für diese modierte Verteilergruppe Absender, die Mail aus der Organisation senden, darüber benachrichtigt, wenn ihre Nachrichten nicht genehmigt werden.

```
Set-DistributionGroup -Identity "Customer Support" -ModeratedBy "Amy" -ModerationEnabled $true -
SendModerationNotifications 'Internal'
```

In diesem Beispiel wird die durch einen Benutzer erstellte Verteilergruppe "Dog Lovers" so geändert, dass der Gruppenleiter Benutzeranforderungen zum Gruppenbeitritt genehmigen muss. Zusätzlich wird durch Verwendung des Parameters *BypassSecurityGroupManagerCheck* der Gruppenleiter nicht über Änderungen benachrichtigt, die an den Einstellungen der Verteilergruppe vorgenommen wurden.

```
Set-DistributionGroup -Identity "Dog Lovers" -MemberJoinRestriction 'ApprovalRequired' -  
BypassSecurityGroupManagerCheck
```

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie die folgenden Schritte aus, um die erfolgreiche Änderung von Verteilergruppeneigenschaften zu überprüfen:

- In der Exchange-Verwaltungskonsole, wählen Sie die Gruppe, und klicken Sie dann auf **Bearbeiten** [ ] anzeigen, die Eigenschaft oder Funktion, die Sie geändert haben. Je nach der Eigenschaft, die Sie geändert haben, kann es im Bereich Details für die ausgewählte Gruppe angezeigt werden.
- Verwenden Sie das Cmdlet **Get-DistributionGroup** in Exchange Online PowerShell um die Änderungen zu überprüfen. Ein Vorteil von Exchange Online PowerShell ist, dass Sie mehrere Eigenschaften für mehrere Gruppen anzeigen können. Führen Sie im Beispiel oben, in dem die Empfängerzahl geändert wurde den folgenden Befehl zum Überprüfen des neuen Werts.

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | Format-List  
Name,RecipientLimits
```

Führen Sie diesen Befehl für das vorherige Beispiel aus, in dem die Nachrichtengrenzwerte geändert wurden.

```
Get-Mailbox -OrganizationalUnit "Marketing" | Format-List  
Name,IssueWarningQuota,ProhibitSendQuota,ProhibitSendReceiveQuota,UseDatabaseQuotaDefaults
```

# Erstellen einer Benennungsrichtlinie für Verteilergruppen

18.12.2018 • 8 minutes to read

Eine Benennungsrichtlinie für Gruppen ermöglicht das Standardisieren und Verwalten der Namen von Verteilergruppen, die von Benutzern in der Organisation erstellt werden. Sie können festlegen, dass dem Namen der Verteilergruppe bei der Erstellung ein bestimmtes Präfix und Suffix hinzugefügt werden muss, und Sie können die Verwendung bestimmter Wörter unterbinden. Dadurch können Sie die Verwendung ungeeigneter Wörter in Gruppennamen verringern.

Eine Gruppenbenennungsrichtlinie:

- Erzwingt eine konsistente Benennungsstrategie für Gruppen, die von Benutzern erstellt werden.
- Identifiziert Verteilergruppen im freigegebenen Adressbuch.
- Schlägt die Funktion oder Mitgliedschaft der Gruppe vor.
- Bestimmt den Typ der Benutzer, die wahrscheinlich Mitglieder der Gruppe sind.
- Kennzeichnet die geografische Region, in der die Gruppe verwendet wird.
- Verhindert die Verwendung von ungeeigneten Wörtern in Gruppennamen.

Wie funktioniert ein Benennungsrichtlinie Gruppe? Wenn ein Benutzer eine Gruppe erstellt wird, geben sie einen Namen im Feld Anzeigename den Namen an. Nachdem die Gruppe erstellt wird, wendet Microsoft Exchange gruppenbenennungsrichtlinie durch Hinzufügen einer Präfix oder Suffix, das Sie in die gruppenbenennungsrichtlinie definiert haben. Der vollständige Name wird angezeigt, in die Verteilerliste Gruppen in der Exchange-Verwaltungskonsole (EAC) und im freigegebenen Adressbuch an; Cc; und aus: Felder in der e-Mail-Nachrichten. Wenn ein Benutzer versucht, ein Wort zu verwenden, die Sie blockiert haben, erhalten sie eine Fehlermeldung, wenn sie versuchen, speichern Sie die neue Gruppe und aufgefordert werden, die gesperrte Word zu entfernen, und speichern die Gruppe erneut.

Es folgen einige Beispiele zu einer Gruppenbenennungsrichtlinie. In jedem Beispiel ist <**Gruppename**> ein beschreibender Name, der von der Person eingegeben wird, die die Gruppe erstellt. Exchange fügt dem Anzeigennamen die in der Richtlinie definierten Präfixe und Suffixe hinzu, wenn die Gruppe erstellt wird.

- Textzeichenfolgen (mit Unterstrichen), die für ein einzelnes Präfix (DG) und ein Suffix (Benutzer) verwendet werden:

DG\_<Gruppennamen ein>Users

- Mehrere Präfixe (DG und Contoso) und ein Suffix (Benutzer) mit Textzeichenfolgen:

DG\_Contoso\_<Gruppennamen ein>Users

- Ein als Präfix verwendetes Attribut (Department):

Department\_<Gruppename>

Angenommen, von Ihrer Schule wird für Fakultätsmitglieder das Department-Attribut verwendet. Im Anschluss finden Sie ein Beispiel für einen Gruppennamen, der von einem Fakultätsmitglied aus der Psychologieabteilung erstellt wurde:

In diesem Beispiel wird der Unterstrich () *in einem zweiten Präfix als einzige Textzeichenfolge angegeben, um den Abteilungsnamen vom Gruppennamen zu trennen.*

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Verteilergruppen" im Thema [Recipients Permissions](#).
- Die maximale Länge für einen Gruppennamen beträgt 64 Zeichen. Dies beinhaltet die kombinierte Anzahl von Zeichen im Präfix, im vom Benutzer angegebenen Gruppennamen und im Suffix.
- Die Gruppenbenennungsrichtlinie wird nur auf Gruppen angewendet, die von Benutzern erstellt werden. Wenn Sie oder andere Administratoren mithilfe der Exchange-Verwaltungskonsole Verteilergruppen erstellen, wird die Gruppenbenennungsrichtlinie ignoriert und nicht auf den Gruppennamen angewendet.
- Gruppennamen werden ohne Leerzeichen erstellt. Es empfiehlt sich, zwischen Textzeichenfolgen, Attributen und dem Gruppennamen einen Unterstrich () *oder einen anderen Platzhalter zu verwenden.*
- Mit Windows PowerShell können Sie die Gruppenbenennungsrichtlinie außer Kraft setzen, wenn Sie eine Verteilergruppe erstellen oder bearbeiten. Weitere Informationen finden Sie unter [Außerkraftsetzen der Benennungsrichtlinie für Verteilergruppen](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen einer Gruppenbenennungsrichtlinie mithilfe der Exchange-Verwaltungskonsole

1. Wählen Sie in der Exchange-Verwaltungskonsole **Gruppen** > **Weitere**  > **gruppenbenennungsrichtlinie konfigurieren**.
2. Konfigurieren Sie unter **Gruppenbenennungsrichtlinie** das Präfix, indem Sie im Pulldownmenü entweder **Attribut** oder **Text** auswählen.
  - **Attribut:** Wählen Sie das Attribut aus, und klicken Sie dann auf **OK**.
  - **Text:** Geben Sie die Zeichenfolge ein, und klicken Sie auf **OK**.Beachten Sie, dass die eingegebene Textzeichenfolge bzw. das ausgewählte Attribut als Link dargestellt wird. Klicken Sie auf den Link, um die Textzeichenfolge oder das Attribut zu ändern.
3. Klicken Sie auf **Hinzufügen**, um weitere Präfixe hinzuzufügen.
4. Wählen Sie für das Suffix im Pulldownmenü entweder **Attribut** oder **Text** aus, und konfigurieren Sie das Suffix.
5. Klicken Sie auf **Hinzufügen**, um weitere Suffixe hinzuzufügen.

Nach dem Hinzufügen eines Präfix oder Suffix wird eine Vorschau der Gruppenbenennungsrichtlinie

angezeigt.

6. Klicken Sie auf **Entfernen**, um ein Präfix oder Suffix aus der Richtlinie zu löschen, .
7. Klicken Sie auf **Blockierte Wörter**, um blockierter Wörter hinzuzufügen oder zu entfernen.
  - Um ein Wort zur Liste hinzuzufügen, geben Sie das Wort blockieren, und klicken Sie auf **Hinzufügen**, um .
  - Um ein Wort aus der Liste zu entfernen, wählen Sie es aus, und klicken Sie auf **Entfernen**.
  - Um ein vorhandenes blockiertes Wort zu bearbeiten, wählen Sie es aus, und klicken Sie auf **Bearbeiten**.
8. Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie wie folgt vor, um die erfolgreiche Erstellung einer Gruppenbenennungsrichtlinie zu überprüfen:

- Wählen Sie in der Exchange-Verwaltungskonsole **Gruppen** > **Mehr** > **Gruppenbenennungsrichtlinie konfigurieren**.

Die Gruppenbenennungsrichtlinie, die Sie definiert haben, wird auf der Seite **Gruppenbenennungsrichtlinie** unter **Vorschau der Richtlinie** angezeigt.

- Führen Sie in Windows PowerShell den folgenden Befehl aus, um die Gruppenbenennungsrichtlinie anzuzeigen.

```
Get-OrganizationConfig | Format-List DistributionGroupNamingPolicy
```

# Außerkraftsetzen der Benennungsrichtlinie für Verteilergruppen

18.12.2018 • 4 minutes to read

Die gruppenbenennungsrichtlinie für Verteilergruppen gilt nur für Gruppen von Benutzern erstellte. Wenn Sie oder andere Administratoren der Exchange-Verwaltungskonsole (EAC mithilfe) Verteilergruppen erstellen, die gruppenbenennungsrichtlinie wird ignoriert, und nicht auf den Namen der Gruppe angewendet.

Wenn Sie Exchange Online PowerShell erstellen, oder benennen Sie eine Verteilergruppe verwenden, wird jedoch die gruppenbenennungsrichtlinie angewendet, Gruppen von Administratoren erstellt wurden, es sei denn, Sie den *IgnoreNamingPolicy* -Parameter verwenden, um die gruppenbenennungsrichtlinie außer Kraft setzen.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Verteilergruppen" im Thema [Recipients Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Was möchten Sie tun?

### Verwenden Sie Exchange Online PowerShell überschreiben Sie die gruppenbenennungsrichtlinie, wenn Sie eine neue Gruppe erstellen

Führen Sie folgenden Befehl aus, um eine Gruppenbenennungsrichtlinie außer Kraft zu setzen.

```
New-DistributionGroup -Name <Group Name> -IgnoreNamingPolicy
```

Wenn die Gruppenbenennungsrichtlinie für die Organisation z. B. DG\_<Gruppenname>Users lautet, führen Sie den folgenden Befehl aus, um eine Gruppe mit dem Namen All Administrators zu erstellen.

```
New-DistributionGroup -Name "All Administrators" -IgnoreNamingPolicy
```

Wenn Microsoft Exchange diese Gruppe erstellt wird, wird alle Administratoren für den *Namen* und die *DisplayName* -Parameter verwendet.

### Verwenden Sie Exchange Online PowerShell überschreiben Sie die gruppenbenennungsrichtlinie, wenn Sie eine Gruppe umbenennen

Um die gruppenbenennungsrichtlinie, wenn Sie eine vorhandene Gruppe mit Exchange Online PowerShell umbenennen zu überschreiben, führen Sie den folgenden Befehl aus.

```
Set-DistributionGroup -Identity <Old Group Name> -Name <New Group Name> -DisplayName <New Group Name> -  
IgnoreNamingPolicy
```

Angenommen, beispielsweise eine gruppenbenennungsrichtlinie einem Abend erstellten und am nächsten Morgen Ihnen bewusst, dass Sie die Textzeichenfolge in das Präfix falsch geschrieben. Am nächsten Morgen sehen Sie, dass eine neue Gruppe mit dem falsch geschriebenen Präfix bereits erstellt worden ist. Sie können die gruppenbenennungsrichtlinie in der Exchange-Verwaltungskonsole beheben, aber Sie Exchange Online PowerShell verwenden, um die Gruppe mit dem falsch geschriebenen Namen umbenennen müssen. Führen Sie den folgenden Befehl aus.

```
Set-DistributionGroup -Identity "Government_Contracts_NWRegion" -Name "Government_ContractEstimates_NWRegion"  
-DisplayName "Government_ContractEstimates_NWRegion" -IgnoreNamingPolicy
```

#### IMPORTANT

Geben Sie beim Umbenennen einer Gruppe immer den Parameter *DisplayName* an. Andernfalls wird der alte Name weiter im freigegebenen Adressbuch und in den Feldern "An:", "Cc:" und "Von:" in E-Mails angezeigt.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie die folgenden Befehle aus, um zu überprüfen, ob eine Verteilergruppe, in der die Gruppenbenennungsrichtlinie ignoriert wird, erfolgreich erstellt oder umbenannt wurde.

```
Get-DistributionGroup <Name> | Format-List DisplayName
```

```
Get-OrganizationConfig | Format-List DistributionGroupNamingPolicy
```

Wenn sich das Format des Anzeigenamens für die Gruppe von dem Format unterscheidet, das durch die Gruppenbenennungsrichtlinie Ihrer Organisation erzwungen wird, war der Vorgang erfolgreich.

# Verwalten dynamischer Verteilergruppen

18.12.2018 • 31 minutes to read

Dynamische Verteilergruppen sind E-Mail-aktivierte Active Directory-Gruppenobjekte, die erstellt werden, um den Massenversand von E-Mail-Nachrichten und sonstigen Informationen innerhalb einer Microsoft Exchange-Organisation zu beschleunigen.

Im Gegensatz zu normalen Verteilergruppen mit einer festgelegten Anzahl an Mitgliedern wird die Mitgliederliste für dynamische Verteilergruppen basierend auf den von Ihnen festgelegten Filtern und Bedingungen jedes Mal berechnet, wenn eine Nachricht an die Gruppe übermittelt wird. Wenn eine E-Mail an eine dynamische Verteilergruppe gesendet wird, wird sie an alle Empfänger in der Organisation zugestellt, die mit den für die Gruppe festgelegten Kriterien übereinstimmen.

## IMPORTANT

Eine dynamische Verteilergruppe enthält alle Empfänger in Active Directory, deren Attributwerte dem jeweiligen Filter entsprechen. Werden die Eigenschaften eines Empfängers geändert, damit sie dem Filter entsprechen, kann dieser Empfänger ggf. versehentlich ein Gruppenmitglied werden und Nachrichten erhalten, die an die Gruppe gesendet werden. Ordnungsgemäße und konsistente Kontobereitstellungsverfahren verringern das Risiko solcher Vorkommnisse.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 bis 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter „Dynamische Verteilergruppen“ im Thema [Empfängerberechtigungen](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen einer dynamischen Verteilergruppe

### Erstellen einer dynamischen Verteilergruppe mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen > Neu > Dynamische Verteilergruppe**.
2. Füllen Sie auf der Seite **Neue dynamische Verteilergruppe** die folgenden Felder aus:
  - \*\*\* Anzeigename\*\*: Geben Sie den Anzeigennamen in diesem Feld können. Dieser Name erscheint im freigegebenen Adressbuch in der: Linie, wenn e-Mail an diese Gruppe, und klicken Sie in der Liste der Gruppen in der Exchange-Verwaltungskonsole gesendet wird. Der Anzeigename ist erforderlich und sollte benutzerfreundlichen sein, damit Personen erkannt wird. Es muss eindeutig auch in der Gesamtstruktur sein.

**NOTE**

Die Gruppenbenennungsrichtlinie wird auf dynamische Verteilergruppen nicht angewendet.

- \*\*\* Alias\*\*: in diesem Feld können Sie den Namen des Alias für die Gruppe eingeben. Der Alias darf 64 Zeichen nicht überschreiten und muss in der Gesamtstruktur eindeutig sein. Wenn ein Benutzer den Alias zu macht: Zeile einer e-Mail-Nachricht, es in der Gruppe Anzeigenamen aufgelöst wird.
- **Beschreibung:** in diesem Feld können Sie die Gruppe beschreiben, damit die Benutzer wissen, was der Zweck der Gruppe ist. Diese Beschreibung wird im freigegebenen Adressbuch.
- **Organisationseinheit:** Sie können eine Organisationseinheit (OU) als die Standardstärke (Dies ist der Empfängerbereich) auswählen. Wenn der Empfängerbereich auf die Gesamtstruktur festgelegt ist, wird der Standardwert in den Container Users in Active Directory-Domäne festgelegt, die den Computer enthält, auf dem der Exchange-Verwaltungskonsole ausgeführt wird. Wenn der Empfängerbereich auf eine bestimmte Domäne festgelegt ist, ist der Container "Users" in dieser Domäne standardmäßig aktiviert. Wenn der Empfängerbereich auf eine bestimmte Organisationseinheit festgelegt ist, ist dieser Organisationseinheit standardmäßig aktiviert.

Um eine andere Organisationseinheit auszuwählen, klicken Sie auf **Durchsuchen**. In diesem Dialogfeld werden alle Organisationseinheiten der Gesamtstruktur angezeigt, die sich in einem bestimmten Bereich befinden. Wählen Sie die gewünschte Organisationseinheit aus, und klicken Sie dann auf **OK**.

- **Besitzer:** ein Besitzers für eine dynamische Verteilergruppe ist optional. Sie können Besitzer hinzufügen, indem Sie auf **Durchsuchen**, und klicken Sie dann in der Liste Benutzer auswählen.
- 3. Im Abschnitt **Mitglieder** geben Sie die Empfängertypen für die Gruppe an und richten Regeln zum Festlegen der Mitgliedschaft ein. Wählen Sie eines der folgenden Felder aus:
  - **Alle Empfängertypen:** Wählen Sie diese Option zum Senden von Nachrichten, die für diese Gruppe sein, um alle Empfängertypen definierten Kriterien entsprechen.
  - **Die folgenden Empfängertypen:** Nachrichten, die die Kriterien für diese Gruppe an einen oder mehrere der folgenden Empfängertypen gesendet werden definiert:
  - **Benutzer mit Exchange-Postfächer:** Aktivieren Sie dieses Kontrollkästchen, wenn Benutzer enthalten, die Exchange-Postfächer werden soll. Benutzer, die Exchange-Postfächer sind die, die ein Benutzerkonto für die Domäne und ein Postfach in der Exchange-Organisation haben.
  - **Benutzer mit externen e-Mail-Adressen:** Aktivieren Sie dieses Kontrollkästchen, wenn Benutzer umfassen, die externe e-Mail-Adressen verfügen soll. Benutzer, die externe e-Mail-Konten haben haben in Active Directory-Domäne Benutzerkonten, jedoch außerhalb des Unternehmens e-Mail-Konten verwenden. Auf diese Weise können sie in der globalen Adressliste (GAL) enthalten und Verteilerlisten hinzugefügt werden.
  - **Ressourcenpostfächer:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie Exchange-Postfächer für Ressourcen einschließen möchten. Ressourcenpostfächer ermöglichen das Verwalten von Unternehmensressourcen über ein Postfach, wie einem Konferenzraum oder ein Unternehmen Fahrzeug.
  - **Kontakte mit externen e-Mail-Adressen:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie Kontakte hinzufügen, die externe e-Mail-Adressen verfügen möchten. Kontakte, die externe e-Mail-Adressen verfügen nicht über Domänenkonten Benutzer in Active Directory verfügen, aber die externe e-Mail-Adresse steht in der globalen Adressliste.
  - **E-Mail-aktivierte Gruppen:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie Sicherheitsgruppen oder Verteilergruppen, die e-Mail-aktivierte wurden einschließen möchten. E-Mail-aktivierte Gruppen ähneln

Verteilergruppen. E-Mail-Nachrichten, die an ein e-Mail-aktivierte Gruppenkonto gesendet werden, werden an mehrere Empfänger übermittelt werden.

4. Klicken Sie auf **Regel hinzufügen**, um die Kriterien für die Mitgliedschaft in dieser Gruppe zu definieren.
5. Wählen Sie eines der folgenden Empfängerattribute aus der Dropdownliste aus, und geben Sie einen Wert an. Wenn der Wert für das ausgewählte Attribut dem von Ihnen definierten Wert entspricht, erhält der Empfänger eine Nachricht, die an diese Gruppe gesendet wird.

ATTRIBUT	SENDEN SIE NACHRICHT AN EINEN EMPFÄNGER...
<b>Empfängercontainer</b>	Das Empfängerobjekt befindet sich in der angegebenen Domäne oder Organisationseinheit.
<b>Bundesland oder Kanton</b>	Der angegebene Wert entspricht der Eigenschaft Bundesland/Kanton des Empfängers.
<b>Company</b>	Der angegebene Wert entspricht der Eigenschaft Firma des Empfängers.
<b>Department</b>	Der angegebene Wert entspricht der Eigenschaft Abteilung des Empfängers.
<b>Benutzerdefiniertes AttributN</b> (wobei N für eine Zahl zwischen 1 und 15 steht)	Der angegebene Wert entspricht der Eigenschaft CustomAttributeN des Empfängers.

<span data-ttu-id="4e5f2-p118">\*\*Wichtig\*\*: die Werte, die Sie für das ausgewählte Attribut eingeben müssen exakt übereinstimmen, die in den Eigenschaften des Empfängers angezeigt werden. Beispielsweise wird Wenn Sie \*\*Washington\*\* für \*\*Bundesland/Kanton\*\*eingeben, aber der Wert für die Eigenschaft des Empfängers \*\*WA ist\*\*, die Bedingung werden nicht erfüllt. Darüber hinaus sind textbasierte Werte, die Sie angeben nicht Groß-/Kleinschreibung beachtet. Beispielsweise wenn Sie \*\*Contoso\*\* für das \*\*Unternehmen\*\* -Attribut angeben, werden Nachrichten an einen Empfänger gesendet werden, wenn dieser Wert \*\*"Contoso"\*\* ist.</span><span class="sxs-lookup"><span data-stu-id="4e5f2-p118">\*\*Important\*\*: The values that you enter for the selected attribute must exactly match those that appear in the recipient's properties. For example, if you enter \*\*Washington\*\* for \*\*State or province\*\*, but the value for the recipient's property is \*\*WA\*\*, the condition will not be met. Also, text-based values that you specify aren't case-sensitive. For example, if you specify \*\*Contoso\*\* for the \*\*Company\*\* attribute, messages will be sent to a recipient if this value is \*\*contoso\*\*.</span></span>

6. Geben Sie im Fenster **Wörter oder Ausdrücke angeben** den Wert im Textfeld ein. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **OK**.
7. Wenn Sie eine weitere Regel zum Definieren der Kriterien für die Mitgliedschaft hinzufügen möchten, klicken Sie unter der zuvor erstellten Regel auf **Regel hinzufügen**.

#### IMPORTANT

Wenn Sie mehrere Regeln zum Definieren der Mitgliedschaft hinzufügen, muss ein Empfänger die Kriterien aller Regeln erfüllen, um eine an die Gruppe gesendete Nachricht zu erhalten. Anders ausgedrückt: Jede Regel ist über den Booleschen Operator **UND** verbunden.

8. Klicken Sie nach Abschluss dieses Vorgangs auf **Speichern**, um die dynamische Verteilergruppe zu erstellen.

#### **NOTE**

Wenn Sie Regeln für andere als die in der Exchange-Verwaltungskonsole verfügbaren Attribute angeben möchten, müssen Sie Exchange Online PowerShell verwenden, um eine dynamische Verteilergruppe zu erstellen. Überwachungsfunktionen Sie benötigen, beachten Sie, dass die Filter und Bedingung Einstellungen für dynamische Verteilergruppen, die benutzerdefinierte Empfängerfiltern haben nur mithilfe von Exchange Online PowerShell verwaltet werden können. Ein Beispiel dafür, wie eine dynamische Verteilergruppe mit einer benutzerdefinierten Abfrage erstellen finden Sie unter dem nächsten Abschnitt zur Verwendung von Exchange Online PowerShell eine dynamische Verteilergruppe zu erstellen.

### **Verwenden Sie Exchange Online PowerShell, um eine dynamische Verteilergruppe zu erstellen.**

In diesem Beispiel wird die dynamische Verteilergruppe "Mailbox Users DDG" erstellt, die nur Postfachbenutzer enthält.

```
New-DynamicDistributionGroup -IncludedRecipients MailboxUsers -Name "Mailbox Users DDG" -OrganizationalUnit  
Users
```

In diesem Beispiel wird eine dynamische Verteilergruppe mit einem benutzerdefinierten Empfängerfilter erstellt. Die dynamische Verteilergruppe enthält alle Postfachbenutzer auf dem Server "Server1".

```
New-DynamicDistributionGroup -Name "Mailbox Users on Server1" -OrganizationalUnit Users -RecipientFilter  
{((RecipientTypeDetails -eq 'UserMailbox' -and ServerName -eq 'Server1'))}
```

In diesem Beispiel wird eine dynamische Verteilergruppe mit einem benutzerdefinierten Empfängerfilter erstellt. Die dynamische Verteilergruppe enthält alle Postfachbenutzer, deren Eigenschaft **CustomAttribute10** den Wert "FullTimeEmployee" aufweist.

```
New-DynamicDistributionGroup -Name "Full Time Employees" -RecipientFilter {((RecipientTypeDetails -eq  
'UserMailbox') -and (CustomAttribute10 -eq 'FullTimeEmployee'))}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-DynamicDistributionGroup](#).

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Führen Sie einen der folgenden Schritte aus, um die erfolgreiche Erstellung einer dynamischen Verteilergruppe zu überprüfen:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**. Die neue dynamische Verteilergruppe wird in der Gruppenliste angezeigt. Unter **Gruppentyp** lautet der Typ **Dynamische Verteilergruppe**.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um Informationen über die neue dynamische Verteilergruppe anzuzeigen.

```
Get-DynamicDistributionGroup | Format-List Name,RecipientTypeDetails,RecipientFilter,PrimarySmtpAddress
```

## **Ändern der Eigenschaften für dynamische Verteilergruppen**

#### **Ändern der Eigenschaften einer dynamischen Verteilergruppe mithilfe der Exchange-Verwaltungskonsole**

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**.
2. Klicken Sie in der Liste der Gruppen, klicken Sie auf die dynamische Verteilergruppe, die Sie anzeigen oder ändern möchten, und klicken Sie dann auf **Bearbeiten**.

3. Klicken Sie auf der Eigenschaftenseite für die Gruppe auf einen der folgenden Abschnitte, um Eigenschaften anzuzeigen oder zu ändern.

#### Allgemein

Verwenden Sie diesen Abschnitt, um grundlegende Informationen zur Gruppe anzuzeigen oder zu ändern.

- \*\*\* Anzeigename\*\*: dieser Name erscheint im Adressbuch in der Linie, wenn e-Mail an diese Gruppe, und klicken Sie in der Liste Gruppen gesendet wird. Der Anzeigename ist erforderlich und sollte benutzerfreundlichen sein, damit Personen erkannt wird. Es muss auch in Ihrer Domäne eindeutig sein.
- \*\*\* Alias\*\*: Dies ist der Teil der e-Mail-Adresse, die auf der linken Seite des angezeigt wird am (@) Symbol. Wenn Sie den Alias ändern, die primäre SMTP-Adresse für die Gruppe wird auch geändert werden, und den neuen Alias enthalten. Darüber hinaus wird mit dem vorherigen Alias die e-Mail-Adresse als Proxyadresse für die Gruppe beibehalten.
- **Beschreibung:** in diesem Feld können Sie die Gruppe beschreiben, damit die Benutzer wissen, was der Zweck der Gruppe ist. Diese Beschreibung wird im Adressbuch und in der Exchange-Verwaltungskonsole im Detailfenster angezeigt.
- **Diese Gruppe aus Adresslisten ausgeblendet:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie nicht, dass Benutzer diese Gruppe im Adressbuch angezeigt möchten. Zum Senden von e-Mails an diese Gruppe hat ein Absender in der die Gruppe Alias oder die e-Mail-Adresse eingeben: oder Cc: Zeilen.
- **Organisationseinheit:** Dieses schreibgeschützte Feld zeigt die Organisationseinheit (OU), die die dynamische Verteilergruppe enthält. Sie müssen Active Directory-Benutzer und -Computer verwenden, um die Gruppe in eine andere Organisationseinheit verschieben.

#### Besitz

Verwenden Sie diesen Abschnitt, um einen Gruppenbesitzer zuzuweisen. Eine dynamische Verteilergruppe kann nur einen Besitzer haben. Der Gruppenbesitzer wird auf der Registerkarte **Veraltet von** des Objekts in Active Directory-Benutzer und -Computer angezeigt.

Sie können Besitzer hinzufügen, indem Sie auf **Durchsuchen** klicken und den Besitzer aus der Liste auswählen. Klicken Sie zum Entfernen des Benutzers auf **Löschen**, und klicken Sie anschließend auf **Speichern**.

#### Mitgliedschaft

In diesem Abschnitt ändern Sie die Kriterien, die zum Festlegen der Gruppenmitgliedschaft verwendet werden. Sie können vorhandene Mitgliedschaftsregeln löschen oder ändern und neue Regeln hinzufügen. Verfahren hierzu finden Sie unter [Erstellen einer dynamischen Verteilergruppe mithilfe der Exchange-Verwaltungskonsole](#) in den Verfahren zum Konfigurieren der Mitgliedschaft, wenn Sie eine neue dynamische Verteilergruppe mithilfe der Exchange-Verwaltungskonsole erstellen.

#### Zustellungsverwaltung

In diesem Abschnitt können Sie verwalten, von wem E-Mails an diese Gruppe gesendet werden können.

- **Nur Absender innerhalb meiner Organisation:** Wählen Sie diese Option, um nur Absender in Ihrer Organisation Nachrichten an die Gruppe senden können. Dies bedeutet, dass wenn eine Person außerhalb Ihrer Organisation an diese Gruppe eine e-Mail-Nachricht sendet, zurückgewiesen wird. Dies ist die Standardeinstellung.
- **Absender innerhalb und außerhalb meiner Organisation:** Wählen Sie diese Option, damit alle Benutzer Nachrichten an die Gruppe senden können.

Sie können weiter einschränken, wer Nachrichten an die Gruppe durch Zulassen der nur bestimmte Absender zum Senden von Nachrichten an diese Gruppe senden können. Klicken Sie auf **Hinzufügen** und wählen Sie dann einen oder mehrere Empfänger aus. Wenn Sie diese Liste

Absender hinzufügen, werden sie die einzigen Benutzer, die e-Mail-Nachrichten an die Gruppe senden können. E-Mails, die von jeder Person nicht in der Liste gesendet wird zurückgewiesen.

Wenn eine Person oder eine Gruppe aus der Liste entfernen möchten, wählen sie in der Liste aus, und klicken Sie dann auf **Entfernen** [ ] .

#### **IMPORTANT**

Wenn Sie die Gruppe so konfiguriert haben, dass nur Absender innerhalb Ihrer Organisation Nachrichten an die Gruppe senden dürfen, werden von externen Kontakten gesendete E-Mails auch dann abgelehnt, wenn sie dieser Liste hinzugefügt werden.

#### **Nachrichtenbestätigung**

In diesem Abschnitt können Sie Optionen zum Moderieren der Gruppe festlegen. Moderatoren genehmigen Nachrichten, die an die Gruppe gesendet werden, oder weisen sie zurück, bevor diese die Gruppenmitglieder erreichen.

- **An diese Gruppe gesendete Nachrichten von einem Moderator genehmigt werden müssen:** dieses Kontrollkästchen ist nicht standardmäßig aktiviert. Wenn Sie dieses Kontrollkästchen aktivieren, werden von den gruppenmoderatoren vor der Zustellung eingehende Nachrichten überprüft. Gruppenmoderatoren können genehmigen oder ablehnen eingehender Nachrichten.
- **Gruppenmoderatoren:** Klicken Sie auf **Hinzufügen** , um gruppenmoderatoren hinzuzufügen, [ ]. Um einen Moderator zu entfernen, wählen Sie aus der Moderator, und klicken Sie dann auf **Entfernen** [ ]. Wenn Sie "An diese Gruppe gesendete Nachrichten sind vom Moderator genehmigt werden" ausgewählt und Sie keinen Moderator auswählen haben, werden Nachrichten an die Gruppe zur Genehmigung an die Gruppenbesitzer gesendet.
- **Absender, die nachrichtengenehmigung erfordern keinen:** Hinzufügen von Personen oder Gruppen, die für diese Gruppe Moderation umgangen werden können, klicken Sie auf **Add** [ ]. Um eine Person oder eine Gruppe zu entfernen, wählen Sie das Element aus, und klicken Sie dann auf **Entfernen** [ ].
- **Wählen Sie für die Moderation Benachrichtigungen:** Verwenden Sie diesen Abschnitt, um festzulegen, wie Benutzer über nachrichtengenehmigungen benachrichtigt werden.
  - **Wenn ihre Nachrichten genehmigt werden nicht alle Absender benachrichtigen:** Dies ist die Standardeinstellung. Benachrichtigen Sie alle Absender, innerhalb und außerhalb Ihrer Organisation, wenn Ihre Nachricht nicht genehmigt wird.
  - **Absender benachrichtigen, in Ihrer Organisation nur, wenn ihre Nachrichten genehmigt werden nicht:** Wenn Sie diese Option auswählen, nur Personen oder Gruppen in Ihrer Organisation werden benachrichtigt, wenn eine Nachricht, die sie an die Gruppe gesendet nicht von einem Moderator genehmigt wird.
  - **Nicht benachrichtigt, wenn eine Nachricht nicht genehmigt wird:** Wenn Sie diese Option auswählen, werden nicht an den Absender einer Nachricht, deren Nachrichten nicht von den gruppenmoderatoren genehmigt, Benachrichtigungen gesendet.

#### **E-Mail-Optionen**

In diesem Abschnitt können Sie die E-Mail-Adressen anzeigen und ändern, die der Gruppe zugeordnet sind. Dazu gehören die primären SMTP-Adressen der Gruppe sowie alle zugeordneten Proxyadressen. Die primäre SMTP-Adresse (auch als Antwortadresse bezeichnet) wird fettgedruckt in der Adressliste angezeigt. Der Wert **SMTP** in der Spalte **Typ** wird dabei in Großbuchstaben angegeben.

- **Hinzufügen:** Klicken Sie auf **Add**  So fügen Sie eine neue e-Mail-Adresse für dieses Postfach hinzu. Wählen Sie eine der folgenden Adresstypen:

- **SMTP:** Dies ist die Adresse. Klicken Sie auf diese Schaltfläche, und geben Sie dann die neue SMTP-Adresse in der \*\* \* E-Mail-Adresse\*\* Feld.

**NOTE**

Damit die neue Adresse die primäre SMTP-Adresse der Gruppe wird, aktivieren Sie das Kontrollkästchen **Diese Adresse als Antwortadresse verwenden.**

- **Benutzerdefinierte Adresstyp:** Klicken Sie auf diese Schaltfläche, und geben Sie einen der unterstützten nicht-SMTP-e-Mail-Adresstypen in der \*\* \* E-Mail-Adresse\*\* Feld.

**NOTE**

Mit Ausnahme von X.400-Adressen überprüft Exchange benutzerdefinierte Adressen nicht auf ordnungsgemäße Formatierung. Sie müssen sicherstellen, dass die von Ihnen angegebene benutzerdefinierte Adresse die Formatanforderungen für den jeweiligen Adresstyp erfüllt.

- **Bearbeiten:** um eine der Gruppe zugeordnete e-Mail-Adresse zu ändern, wählen Sie sie aus der Liste aus, und klicken Sie dann auf **Bearbeiten** .

**NOTE**

Damit eine vorhandene Adresse die primäre SMTP-Adresse der Gruppe wird, aktivieren Sie das Kontrollkästchen **Diese Adresse als Antwortadresse verwenden.**

- **Entfernen:** um eine e-Mail-Adresse der Gruppe zugeordnete zu löschen, wählen Sie sie aus der Liste aus, und klicken Sie dann auf **Entfernen** .

- **E-Mail-Adressen basierend auf der e-Mail-Adressrichtlinie angewendet an diesen Empfänger automatisch aktualisieren:** Aktivieren Sie dieses Kontrollkästchen, um dem Empfänger der e-Mail-Adressen automatisch aktualisierte basierend auf Änderungen an e-Mail-Adressrichtlinien in Ihrer Organisation. Dieses Feld ist standardmäßig aktiviert.

#### E-Mail-Info

Verwenden Sie diesen Abschnitt, um eine E-Mail-Info hinzuzufügen, in der Benutzer vor möglichen Problemen gewarnt werden, bevor sie eine Nachricht an diese Gruppe senden. Eine E-Mail-Info ist Text, der in der Infoleiste angezeigt wird, wenn diese Gruppe der Zeile "An", "Cc" oder "Bcc" einer neuen E-Mail hinzugefügt wird. Sie könnten z. B. großen Gruppen eine E-Mail-Info hinzufügen, um potenzielle Absender zu warnen, dass ihre Nachricht an viele Personen gesendet wird.

**NOTE**

Eine E-Mail-Info kann HTML-Tags enthalten, Skripts sind jedoch nicht zulässig. Die Länge einer benutzerdefinierten E-Mail-Info darf 175 angezeigte Zeichen nicht überschreiten. HTML-Tags werden bei diesem Zeichenlimit nicht mitgezählt.

#### Gruppendelegierung

In diesem Abschnitt können Sie einem Benutzer (der als Stellvertretung bezeichnet wird) Berechtigungen zuweisen, sodass der Benutzer Nachrichten als die Gruppe oder im Namen der Gruppe senden kann. Sie können die folgenden Berechtigungen zuweisen:

- **Senden als:** Diese Berechtigung ermöglicht es der Stellvertretung zum Senden von Nachrichten als Gruppe. Nachdem diese Berechtigung zugewiesen wurde, verfügt die Stellvertretung über die Option zum Hinzufügen der Gruppe in die Zeile **aus**, um anzugeben, dass die Nachricht von der Gruppe gesendet wurde.
- **Senden im Auftrag von:** mit dieser Berechtigung können auch eine Stellvertretung, Nachrichten im Namen der Gruppe zu senden. Nachdem diese Berechtigung zugewiesen wurde, verfügt die Stellvertretung über die Option zum Hinzufügen der Gruppe in der Zeile **von**. Die Nachricht wird angezeigt, die von der Gruppe gesendet werden, und es wird angenommen, dass sie durch den Delegaten im Namen der Gruppe gesendet wurde.

Wenn Sie einer Stellvertretung eine Berechtigung zuweisen möchten, klicken Sie unter der entsprechenden Berechtigung auf **Hinzufügen**, um die Seite **Empfänger auswählen** anzuzeigen, auf der eine Liste mit allen Empfängern in der Exchange-Organisation angezeigt wird, denen die Berechtigung zugewiesen werden kann. Wählen Sie die gewünschten Empfänger aus, fügen Sie diese der Liste hinzu, und klicken Sie dann auf **OK**. Sie können auch nach einem bestimmten Empfänger suchen, indem Sie seinen Namen in das Suchfeld eingeben und dann auf **Suchen** klicken.

#### **Verwenden von Exchange Online PowerShell Eigenschaften einer dynamischen Verteilergruppe ändern**

Verwenden Sie die Cmdlets **Get-DynamicDistributionGroup** und **Set-DynamicDistributionGroup**, um Eigenschaften für dynamische Verteilergruppen anzeigen und ändern. Vorteile der Verwendung von Exchange Online PowerShell sind die Möglichkeit zum Ändern der Eigenschaften, die in der Exchange-Verwaltungskonsole nicht mehr verfügbar und Ändern der Eigenschaften für mehrere Gruppen. Informationen dazu, welche Parameter Verteilergruppeneigenschaften entsprechen finden Sie unter den folgenden Themen:

- [Get-DynamicDistributionGroup](#)
- [Set-DynamicDistributionGroup](#)

Hier sind einige Beispiele für die Verwendung von Exchange Online PowerShell Eigenschaften einer dynamischen Verteilergruppe ändern.

In diesem Beispiel werden die folgenden Parameter für alle dynamischen Verteilergruppen in der Organisation geändert:

- Ausblenden aller dynamischen Verteilergruppen aus dem Adressbuch
- Festlegen der maximalen Nachrichtengröße, die an die Gruppe gesendet werden kann, auf 5 MB
- Aktivieren der Moderation
- Zuweisen des Administrators als Moderator der Gruppe

```
Get-DynamicDistributionGroup -ResultSize unlimited | Set-DynamicDistributionGroup -HiddenFromAddressListsEnabled $true -MaxReceiveSize 5MB -ModerationEnabled $true -ModeratedBy administrator
```

In diesem Beispiel wird die Proxy-SMTP-E-Mail-Adresse "Seattle.Employees@contoso.com" der Gruppe "Alle Mitarbeiter" hinzugefügt.

```
Set-DynamicDistributionGroup -Identity "All Employees" -EmailAddresses SMTP:All.Employees@contoso.com, smtp:Seattle.Employees@contoso.com
```

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Gehen Sie folgendermaßen vor, um zu überprüfen, ob die Eigenschaften einer dynamischen Verteilergruppe erfolgreich geändert wurden:

- In der Exchange-Verwaltungskonsole, wählen Sie die Gruppe, und klicken Sie dann auf **Bearbeiten**

anzeigen, die Eigenschaft oder Funktion, die Sie geändert haben. Je nach der Eigenschaft, die Sie geändert haben, kann es im Bereich Details für die ausgewählte Gruppe angezeigt werden.

- Verwenden Sie das Cmdlet **Get-DynamicDistributionGroup** in Exchange Online PowerShell um die Änderungen zu überprüfen. Ein Vorteil von Exchange Online PowerShell ist, dass Sie mehrere Eigenschaften für mehrere Gruppen anzeigen können. Im ersten Beispiel führen Sie den folgenden Befehl aus, um die neuen Werte zu überprüfen.

```
Get-DynamicDistributionGroup -ResultSize unlimited | Format-List  
Name,HiddenFromAddressListsEnabled,MaxReceiveSize,ModerationEnabled,ModeratedBy
```

Führen Sie diesen Befehl für das vorherige Beispiel aus, in dem die Nachrichtengrenzwerte geändert wurden.

```
Get-Mailbox -OrganizationalUnit "Marketing" | Format-List  
Name,IssueWarningQuota,ProhibitSendQuota,ProhibitSendReceiveQuota,UseDatabaseQuotaDefaults
```

# Anzeigen der Mitglieder einer dynamischen Verteilergruppe

18.12.2018 • 3 minutes to read

Dynamische Verteilergruppen sind Verteilergruppen, deren Mitgliedschaft auf bestimmten Empfängerfiltern statt einer definierten Gruppe von Empfängern basiert. Microsoft Exchange bietet musterfiltern Filter zum Erstellen von Empfängerfiltern für dynamische Verteilergruppen zu vereinfachen. Ein musterfiltern wird eine häufig verwendete Filter, den Sie verwenden können, um verschiedene Empfänger-Filterung Kriterien erfüllen. Sie können die Empfängertypen angeben, den, die Sie in eine dynamische Verteilergruppe einschließen möchten. Darüber hinaus können Sie eine Liste der Bedingungen angeben, die die Empfänger erfüllen muss. Sie können Exchange Online PowerShell verwenden, um die Liste der Empfänger für eine dynamische Verteilergruppe anzuzeigen, die die musterfiltern Filter verwendet.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Dynamische Verteilergruppen" im Thema [Empfängerberechtigungen](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Was möchten Sie tun?

### Verwenden von Exchange Online PowerShell die Liste der Mitglieder einer dynamischen Verteilergruppe Vorschau anzeigen

Dieses Beispiel gibt die Liste der Elemente für die dynamische Verteilergruppe namens Vollzeitmitarbeiter. Der erste Befehl speichert das dynamische Verteilergruppe Group-Objekt in der Variablen `$FTE`. Der zweite Befehl verwendet das Cmdlet **Get-Recipient**, um die Empfänger aufgelistet, die für die dynamische Verteilergruppe definierten Suchkriterien entsprechen.

```
$FTE = Get-DynamicDistributionGroup "Full Time Employees"
```

```
Get-Recipient -RecipientPreviewFilter $FTE.RecipientFilter -OrganizationalUnit $FTE.RecipientContainer
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-DynamicDistributionGroup](#) und [Get-Recipient](#).

**NOTE**

Sie können keine Mitglieder einer Gruppe dynamische Verteilergruppe mithilfe der Exchange-Verwaltungskonsole anzeigen.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie die Mitglieder einer dynamischen Verteilergruppe erfolgreich angezeigt haben, führen Sie folgende Schritte aus:

- In Exchange Online PowerShell wird eine Liste der Elemente zurückgegeben, nach dem Ausführen des vorherigen Befehls aus, um eine Liste der Mitglieder von Verteilergruppen dynamischen Vorschau anzeigen. Angenommen, wenn Sie ein neues Benutzerpostfach mit Eigenschaften, die übereinstimmen des Empfängerfilters für die dynamische Verteilergruppe erstellt, sollte diesen neue Benutzer in der Liste der Mitglieder der Gruppe angezeigt.

# Verwalten von E-Mail-aktivierten Sicherheitsgruppen

18.12.2018 • 26 minutes to read

Eine e-Mail-aktivierte Sicherheitsgruppe kann zum Verteilen von Nachrichten als auch über das Erteilen von Zugriffsberechtigungen auf Ressourcen in Active Directory verwendet werden. Weitere Informationen finden Sie unter [Recipients](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 bis 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Verteilergruppen" im Thema [Recipients Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen einer E-Mail-aktivierten Sicherheitsgruppe

### Erstellen einer Sicherheitsgruppe mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**.
2. Klicken Sie auf **neu**  > **-Sicherheitsgruppe**.
3. Füllen Sie auf der Seite **Neue Sicherheitsgruppe** die folgenden Felder aus:
  - \*\*\* Anzeigename\*\*: Geben Sie den Anzeigennamen in diesem Feld können. Dieser Name erscheint im freigegebenen Adressbuch in der: Linie, wenn e-Mail an diese Gruppe, und klicken Sie in der Liste der Gruppen in der Exchange-Verwaltungskonsole gesendet wird. Der Anzeigename ist erforderlich und sollte benutzerfreundlichen sein, damit Personen erkannt wird. Es muss eindeutig auch in der Gesamtstruktur sein.

### NOTE

Wenn eine gruppenbenennungsrichtlinie angewendet wird, müssen Sie die für Ihre Organisation erzwungen Benennungseinschränkungen befolgen. Weitere Informationen finden Sie unter [Erstellen einer Verteilergruppe naming Policy](#). Wenn Sie Ihrer Organisation gruppenbenennungsrichtlinie außer Kraft setzen möchten, finden Sie unter [außer Kraft setzen die gruppenbenennungsrichtlinie Verteilung](#).

- \*\*\* Alias\*\*: in diesem Feld Geben Sie den Alias für die Sicherheitsgruppe können. Der Alias darf 64 Zeichen nicht überschreiten und muss in der Gesamtstruktur eindeutig sein. Wenn ein Benutzer den Alias in der macht: Zeile einer e-Mail-Nachricht, es in der Gruppe Anzeigennamen aufgelöst wird.
- **Beschreibung**: in diesem Feld können Sie um die Sicherheitsgruppe zu beschreiben, damit die Benutzer wissen, was der Zweck der Gruppe ist.

- **Organisationseinheit:** Sie können eine Organisationseinheit (OU) als die Standardstärke (Dies ist der Empfängerbereich) auswählen. Wenn der Empfängerbereich auf die Gesamtstruktur festgelegt ist, wird der Standardwert in den Container Users in Active Directory-Domäne festgelegt, die den Computer enthält, auf dem der Exchange-Verwaltungskonsole ausgeführt wird. Wenn der Empfängerbereich auf eine bestimmte Domäne festgelegt ist, ist der Container "Users" in dieser Domäne standardmäßig aktiviert. Wenn der Empfängerbereich auf eine bestimmte Organisationseinheit festgelegt ist, ist dieser Organisationseinheit standardmäßig aktiviert.

Um eine andere Organisationseinheit auszuwählen, klicken Sie auf **Durchsuchen**. In diesem Dialogfeld werden alle Organisationseinheiten der Gesamtstruktur angezeigt, die sich in einem bestimmten Bereich befinden. Wählen Sie die gewünschte Organisationseinheit aus, und klicken Sie auf **OK**.

- \*\*\* Besitzer\*\*: die Person, die eine Gruppe erstellt wird standardmäßig der Besitzer. Alle Gruppen müssen Sie mindestens einen Besitzer haben. Sie können Besitzer hinzufügen, indem Sie auf **Hinzufügen**.
- **Member:** Verwenden Sie diesen Abschnitt zum Hinzufügen von Mitgliedern und um anzugeben, ob die Genehmigung erforderlich ist, damit Benutzern beitreten oder diese verlassen der Gruppe.

Besitzer von Gruppen müssen nicht Mitglied der Gruppe sein. Verwenden Sie die Option **Gruppenbesitzer als Mitglieder hinzufügen**, um die Besitzer als Mitglieder hinzuzufügen bzw. zu entfernen.

Klicken Sie auf **Hinzufügen**, um Mitglieder der Gruppe hinzuzufügen, [ ] . Wenn Sie das Hinzufügen von Mitgliedern abgeschlossen haben, klicken Sie auf **OK**, um die Seite **neuen Sicherheitsgruppe** zurückzukehren.

Aktivieren Sie das Kontrollkästchen **Genehmigung durch Besitzer erforderlich**, wenn Gruppenbesitzer Benutzeranforderungen zum Beitritt zur Gruppe erhalten sollen. Wenn Sie diese Option auswählen, können Mitglieder nur durch die Gruppenbesitzer entfernt werden.

4. Klicken Sie nach Abschluss dieses Vorgangs auf **Speichern**, um die Sicherheitsgruppe zu erstellen.

#### **NOTE**

Standardmäßig ist für alle neuen E-Mail-aktivierten Sicherheitsgruppen die Authentifizierung aller Absender erforderlich. Auf diese Weise wird verhindert, dass externe Absender Nachrichten an E-Mail-aktivierte Sicherheitsgruppen senden können. Um eine E-Mail-aktivierte Sicherheitsgruppe für das Annehmen von Nachrichten von allen Absendern zu konfigurieren, müssen Sie die Einstellungen für die Einschränkungen der Nachrichtenübermittlung für die betreffende Gruppe ändern.

#### **Verwenden von Exchange Online PowerShell, eine Sicherheitsgruppe erstellen**

In diesem Beispiel wird eine Sicherheitsgruppe mit dem Alias "fsadmin" und dem Namen "File Server Managers" erstellt. Die Sicherheitsgruppe wird in der Standardorganisationseinheit erstellt, und jeder kann dieser Gruppe mit Genehmigung durch die Gruppenbesitzer beitreten.

```
New-DistributionGroup -Name "File Server Managers" -Alias fsadmin -Type security
```

Weitere Informationen zur Verwendung von Exchange Online PowerShell zum Erstellen von e-Mail-aktivierten Sicherheitsgruppen finden Sie unter [New-DistributionGroup](#).

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Führen Sie einen der folgenden Schritte aus, um zu überprüfen, dass Sie erfolgreich eine e-Mail-aktivierte Sicherheitsgruppe erstellt haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**. Die neue e-Mail-aktivierte Sicherheitsgruppe ist in der Gruppenliste angezeigt. Klicken Sie unter **Gruppentyp** ist der Typ -

## Sicherheitsgruppe.

- Führen Sie in Exchange Online PowerShell den folgenden Befehl zum Anzeigen von Informationen über die neue e-Mail-aktivierte Sicherheitsgruppe.

```
Get-DistributionGroup <Name> | Format-List Name,RecipientTypeDetails,PrimarySmtpAddress
```

# Ändern der Eigenschaften von E-Mail-aktivierten Sicherheitsgruppen

## Ändern der Eigenschaften von E-Mail-aktivierten Sicherheitsgruppen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**.
2. Klicken Sie in der Liste der Gruppen, klicken Sie auf die Sicherheitsgruppe an, die Sie anzeigen oder ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Eigenschaftenseite für die Gruppe auf einen der folgenden Abschnitte, um Eigenschaften anzuzeigen oder zu ändern.

### Allgemein

Verwenden Sie diesen Abschnitt, um grundlegende Informationen zur Gruppe anzuzeigen oder zu ändern.

- \*\*\* Anzeigename\*\*: dieser Name erscheint im Adressbuch in der: Linie, wenn e-Mail an diese Gruppe, und klicken Sie in der Liste Gruppen gesendet wird. Der Anzeigename ist erforderlich und sollte benutzerfreundlichen sein, damit Personen erkannt wird. Es muss auch in Ihrer Domäne eindeutig sein.
- \*\*\* Alias\*\*: Dies ist der Teil der e-Mail-Adresse, die auf der linken Seite des angezeigt wird die am (@) Symbol. Wenn Sie den Alias ändern, die primäre SMTP-Adresse für die Gruppe wird auch geändert werden, und den neuen Alias enthalten. Darüber hinaus wird mit dem vorherigen Alias die e-Mail-Adresse als Proxyadresse für die Gruppe beibehalten.
- **Beschreibung**: in diesem Feld können Sie die Gruppe beschreiben, damit die Benutzer wissen, was der Zweck der Gruppe ist. Diese Beschreibung wird im Adressbuch und in der Exchange-Verwaltungskonsole im Detailfenster angezeigt.
- **Diese Gruppe aus Adresslisten ausgeblendet**: Aktivieren Sie dieses Kontrollkästchen, wenn Sie nicht, dass Benutzer diese Gruppe im Adressbuch angezeigt möchten. Wenn dieses Kontrollkästchen aktiviert ist, muss ein Absender Geben Sie der Gruppe Alias oder die e-Mail-Adresse in der: oder Cc: Zeilen, um e-Mail-Nachrichten an die Gruppe senden.

### TIP

Blenden Sie ggf. Sicherheitsgruppen aus, da sie normalerweise zum Zuweisen von Berechtigungen zu Gruppenmitgliedern und nicht zum Senden von E-Mails verwendet werden.

- **Organisationseinheit**: Dieses schreibgeschützte Feld zeigt die Organisationseinheit (OU), die die Sicherheitsgruppe enthält. Sie müssen Active Directory-Benutzer und-Computer verwenden, um die Gruppe in eine andere Organisationseinheit verschieben.

### Besitz

Verwenden Sie diesen Abschnitt, um Gruppenbesitzer zuzuweisen. Der Gruppenbesitzer kann der Gruppe Mitglieder hinzufügen und Beitrittsanforderungen genehmigen oder ablehnen. Standardmäßig ist die Person, die eine Gruppe erstellt, deren Besitzer. Jede Gruppe muss mindestens einen Besitzer aufweisen.

Sie können Besitzer hinzufügen, indem Sie auf **Hinzufügen**. Sie können einen Besitzer

entfernen, indem Sie den Besitzer auswählen und dann auf **Entfernen**

#### Mitgliedschaft

Verwenden Sie diesen Abschnitt hinzufügen oder Entfernen von Mitgliedern aus. Gruppenbesitzer müssen keine Mitglieder der Gruppe sein. Klicken Sie unter **Mitglieder** können Sie Mitglieder hinzufügen, indem Sie auf **Hinzufügen** . Sie können ein Element entfernen, indem Sie einen Benutzer in der Mitgliederliste auswählen und dann auf **Entfernen** .

#### Genehmigung der Mitgliedschaft

In diesem Abschnitt können Sie angeben, ob eine Genehmigung durch den oder die Besitzer erforderlich ist, damit Benutzer der Gruppe beitreten können. Wenn Sie das Kontrollkästchen **Genehmigung durch Besitzer erforderlich** aktivieren, wird eine E-Mail an den oder die Gruppenbesitzer gesendet, in der die Genehmigung zum Beitritt angefordert wird. Wie bereits erwähnt, können nur Besitzer Mitglieder aus der Gruppe entfernen.

#### NOTE

Diese Option funktioniert aufgrund von Sicherheitseinschränkungen nicht mit E-Mail-aktivierten Sicherheitsgruppen.

#### Zustellungsverwaltung

In diesem Abschnitt können Sie verwalten, von wem E-Mails an diese Gruppe gesendet werden können.

- **Nur Absender innerhalb meiner Organisation:** Wählen Sie diese Option, um nur Absender in Ihrer Organisation Nachrichten an die Gruppe senden können. Dies bedeutet, dass wenn eine Person außerhalb Ihrer Organisation an diese Gruppe eine e-Mail-Nachricht sendet, werden sie abgelehnt, wird. Dies ist die Standardeinstellung.
- **Absender innerhalb und außerhalb meiner Organisation:** Wählen Sie diese Option, damit alle Benutzer Nachrichten an die Gruppe senden können.

Sie können weiter einschränken, wer Nachrichten an die Gruppe durch Zulassen der nur bestimmte Absender zum Senden von Nachrichten an diese Gruppe senden können. Klicken Sie auf **Hinzufügen**  und wählen Sie dann einen oder mehrere Empfänger aus. Wenn Sie diese Liste Absender hinzufügen, werden sie die einzigen Benutzer, die e-Mail-Nachrichten an die Gruppe senden können. E-Mails, die von jeder Person nicht in der Liste gesendet wird zurückgewiesen.

Wenn eine Person oder eine Gruppe aus der Liste entfernen möchten, wählen sie in der Liste aus, und klicken Sie dann auf **Entfernen** .

#### IMPORTANT

Wenn Sie die Gruppe, um nur Absender innerhalb Ihrer Organisation zum Senden von Nachrichten an die Gruppe zulassen konfiguriert haben, wird von einem e-Mail-Kontakt gesendete e-Mail abgelehnt werden, auch wenn in diese Liste aufgenommen.

#### Nachrichtenbestätigung

In diesem Abschnitt können Sie Optionen zum Moderieren der Gruppe festlegen. Moderatoren genehmigen Nachrichten, die an die Gruppe gesendet werden, oder weisen sie zurück, bevor diese die Gruppenmitglieder erreichen.

- **An diese Gruppe gesendete Nachrichten von einem Moderator genehmigt werden müssen:** dieses Kontrollkästchen ist nicht standardmäßig aktiviert. Wenn Sie dieses Kontrollkästchen aktivieren, werden von den gruppenmoderatoren vor der Zustellung eingehende Nachrichten überprüft werden. Gruppenmoderatoren können genehmigen oder ablehnen eingehender Nachrichten.

- **Gruppenmoderatoren:** Klicken Sie auf **Hinzufügen**, um gruppenmoderatoren hinzuzufügen,  Um einen Moderator zu entfernen, wählen Sie aus der Moderator, und klicken Sie dann auf **Entfernen**  Wenn Sie haben "An diese Gruppe gesendete Nachrichten sind vom Moderator genehmigt werden" ausgewählt, und Sie keinen Moderator auswählen, werden Nachrichten an die Gruppe zur Genehmigung an den Gruppenbesitzer gesendet.
- **Absender, die nachrichtengenehmigung erfordern keinen:** Hinzufügen von Personen oder Gruppen, die für diese Gruppe Moderation umgangen werden können, klicken Sie auf **Add**  Um eine Person oder eine Gruppe zu entfernen, wählen Sie das Element aus, und klicken Sie dann auf **Entfernen**
- **Wählen Sie für die Moderation Benachrichtigungen:** Verwenden Sie diesen Abschnitt, um festzulegen, wie Benutzer über nachrichtengenehmigungen benachrichtigt werden.
  - **Wenn ihre Nachrichten genehmigt werden nicht alle Absender benachrichtigen:** Dies ist die Standardeinstellung. Absender innerhalb und außerhalb Ihrer Organisation werden benachrichtigt, wenn ihre Nachrichten genehmigt werden nicht.
  - **Absender benachrichtigen, in Ihrer Organisation, wenn ihre Nachrichten genehmigt werden nicht:** Wenn Sie diese Option auswählen, nur Personen oder Gruppen in Ihrer Organisation werden benachrichtigt, wenn eine Nachricht, die sie an die Gruppe gesendet nicht von einem Moderator genehmigt wird.
  - **Nicht benachrichtigt, wenn eine Nachricht nicht genehmigt wird:** Wenn Sie diese Option auswählen, werden nicht an den Absender einer Nachricht, deren Nachrichten nicht von den gruppenmoderatoren genehmigt, Benachrichtigungen gesendet.

#### E-Mail-Optionen

In diesem Abschnitt können Sie die E-Mail-Adressen anzeigen und ändern, die der Gruppe zugeordnet sind. Dazu gehören die primären SMTP-Adressen der Gruppe sowie alle zugeordneten Proxyadressen. Die primäre SMTP-Adresse (auch als Antwortadresse bezeichnet) wird fettgedruckt in der Adressliste angezeigt. Der Wert **SMTP** in der Spalte **Typ** wird dabei in Großbuchstaben angegeben.

- **Hinzufügen:** Klicken Sie auf **Add**  So fügen Sie eine neue e-Mail-Adresse für dieses Postfach hinzu. Wählen Sie eine der folgenden Adresstypen:
  - **SMTP:** Dies ist die Adresse. Klicken Sie auf diese Schaltfläche, und geben Sie dann die neue SMTP-Adresse in der \*\*\* E-Mail-Adresse\*\* Feld.

#### NOTE

Damit der neuen Adresse die primäre SMTP-Adresse für die Gruppe wird, aktivieren Sie das Kontrollkästchen **in der Antwort-Adresse ändern**. Dieses Kontrollkästchen wird nur angezeigt, wenn das Kontrollkästchen **e-Mail-Adressen basierend auf der e-Mail-Adressrichtlinie angewendet an diesen Empfänger automatisch aktualisieren** nicht ausgewählt ist.

- **Benutzerdefinierte Adresstyp:** Klicken Sie auf diese Schaltfläche, und geben Sie einen der unterstützten nicht-SMTP-e-Mail-Adresstypen in der \*\* \* E-Mail-Adresse\*\* Feld.

#### NOTE

Mit Ausnahme von X.400-Adressen überprüft Exchange benutzerdefinierte Adressen nicht auf ordnungsgemäße Formatierung. Sie müssen sicherstellen, dass die von Ihnen angegebene benutzerdefinierte Adresse die Formatanforderungen für den jeweiligen Adresstyp erfüllt.

- **Bearbeiten:** um eine der Gruppe zugeordnete e-Mail-Adresse zu ändern, wählen Sie sie in der Liste aus, und klicken Sie dann auf **Bearbeiten**

#### NOTE

Um einer vorhandenen Adresse die primäre SMTP-Adresse für die Gruppe zu machen, aktivieren Sie das Kontrollkästchen **in der Antwort-Adresse ändern**. Wie bereits erwähnt ist dieses Kontrollkästchen nur angezeigt, wenn das Kontrollkästchen **e-Mail-Adressen basierend auf der e-Mail-Adressrichtlinie angewendet an diesen Empfänger automatisch aktualisieren** nicht ausgewählt ist.

- **Entfernen:** um eine e-Mail-Adresse der Gruppe zugeordnete zu löschen, wählen Sie sie in der Liste aus, und klicken Sie dann auf **Entfernen**
- **E-Mail-Adressen basierend auf der e-Mail-Adressrichtlinie angewendet an diesen Empfänger automatisch aktualisieren:** Aktivieren Sie dieses Kontrollkästchen, um dem Empfänger der e-Mail-Adressen automatisch aktualisierte basierend auf Änderungen an e-Mail-Adressrichtlinien in Ihrer Organisation. Standardmäßig ist dieses Kontrollkästchen aktiviert.

#### E-Mail-Info

Verwenden Sie diesen Abschnitt, um eine E-Mail-Info hinzuzufügen, in der Benutzer vor möglichen Problemen gewarnt werden, bevor sie eine Nachricht an diese Gruppe senden. Eine E-Mail-Info ist Text, der in der Infoleiste angezeigt wird, wenn diese Gruppe der Zeile "An", "Cc" oder "Bcc" einer neuen E-Mail hinzugefügt wird. Sie könnten z. B. großen Gruppen eine E-Mail-Info hinzufügen, um potenzielle Absender zu warnen, dass ihre Nachricht an viele Personen gesendet wird.

#### NOTE

Eine E-Mail-Info kann HTML-Tags enthalten, Skripts sind jedoch nicht zulässig. Die Länge einer benutzerdefinierten E-Mail-Info darf 175 angezeigte Zeichen nicht überschreiten. HTML-Tags werden bei diesem Zeichenlimit nicht mitgezählt.

#### Gruppendelegierung

In diesem Abschnitt können Sie einem Benutzer (der als Stellvertretung bezeichnet wird) Berechtigungen zuweisen, sodass der Benutzer Nachrichten als die Gruppe oder im Namen der Gruppe senden kann. Sie können die folgenden Berechtigungen zuweisen:

- **Senden als:** Diese Berechtigung ermöglicht es der Stellvertretung zum Senden von Nachrichten als Gruppe. Nachdem diese Berechtigung zugewiesen wurde, verfügt die Stellvertretung über die Option zum Hinzufügen der Gruppe in die Zeile **aus**, um anzugeben, dass die Nachricht von der Gruppe gesendet wurde.
- **Senden im Auftrag von:** mit dieser Berechtigung können auch eine Stellvertretung, Nachrichten im Namen der Gruppe zu senden. Nachdem diese Berechtigung zugewiesen wurde, verfügt die Stellvertretung über die Option zum Hinzufügen der Gruppe in **der Zeile**. Die Nachricht wird angezeigt, die von der Gruppe gesendet werden, und es wird angenommen, dass sie durch den Delegaten im Namen der Gruppe gesendet wurde.

Um Delegaten Berechtigungen zuweisen möchten, klicken Sie auf **Hinzufügen**, wählen Sie die entsprechende Berechtigung zum Anzeigen der Seite **Wählen Sie Empfänger** mit einer Liste aller Empfänger in Ihrer Exchange-Organisation an, die die Berechtigung zugewiesen werden können. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen**

**Verwenden Sie Exchange Online PowerShell, um die Änderung von Gruppeneigenschaften Sicherheit**

Verwenden Sie die Cmdlets **Get-DistributionGroup** und **Set-DistributionGroup**, zum Anzeigen und Ändern

von Eigenschaften für Sicherheitsgruppen. Vorteile der Verwendung von Exchange Online PowerShell sind die Möglichkeit zum Ändern der Eigenschaften, die in der Exchange-Verwaltungskonsole nicht verfügbar sind und Eigenschaften für mehrere Sicherheitsgruppen zu ändern. Informationen zu den Parametern entsprechen, welche Eigenschaften einer Verteilergruppe, finden Sie unter den folgenden Themen:

- [Get-DistributionGroup](#)
- [Set-DistributionGroup](#)

Hier sind einige Beispiele für die Verwendung von Exchange Online PowerShell Sicherheit Gruppeneigenschaften ändern.

In diesem Beispiel wird eine Liste aller Sicherheitsgruppen in der Organisation angezeigt.

```
Get-DistributionGroup -ResultSize unlimited -Filter {((RecipientTypeDetails -eq 'MailUniversalSecurityGroup'))}
```

In diesem Beispiel wird die primäre SMTP-Adresse (auch als Antwortadresse bezeichnet) für die Sicherheitsgruppe "Seattle Administrators" von "admins@contoso.com" zu "seattle admins@contoso.com" geändert. Die vorherige Antwortadresse wird als Proxyadresse beibehalten.

```
Set-DistributionGroup "Seattle Employees" -EmailAddresses SMTP:sea admins@contoso.com,smtp:admins@contoso.com
```

In diesem Beispiel werden alle Sicherheitsgruppen in der Organisation aus dem Adressbuch ausgeblendet.

```
Get-DistributionGroup -ResultSize unlimited -Filter {((RecipientTypeDetails -eq 'MailUniversalSecurityGroup'))} | Set-DistributionGroup -HiddenFromAddressListsEnabled $true
```

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie die Eigenschaften für eine Sicherheitsgruppe erfolgreich geändert haben, führen Sie folgende Schritte aus:

- In der Exchange-Verwaltungskonsole, wählen Sie die Gruppe, und klicken Sie dann auf **Bearbeiten** [ ] anzeigen, die Eigenschaft oder Funktion, die Sie geändert haben. Je nach der Eigenschaft, die Sie geändert haben, kann es im Bereich Details für die ausgewählte Gruppe angezeigt werden.
- Verwenden Sie das Cmdlet **Get-DistributionGroup** in Exchange Online PowerShell um die Änderungen zu überprüfen. Ein Vorteil von Exchange Online PowerShell ist, dass Sie mehrere Eigenschaften für mehrere Gruppen anzeigen können. Führen Sie im Beispiel oben, in dem alle Sicherheitsgruppen aus dem Adressbuch ausgeblendet wurden den folgenden Befehl zum Überprüfen des neuen Werts.

```
Get-DistributionGroup -ResultSize unlimited -Filter {((RecipientTypeDetails -eq 'MailUniversalSecurityGroup'))} | fl Name,HiddenFromAddressListsEnabled
```

# Gewähren/Blockieren des Gastzugriffs auf Office 365-Gruppen

18.12.2018 • 7 minutes to read

Sie können Gastbenutzer zulassen oder blockieren, die eine bestimmte Domäne verwenden. Nehmen wir z. B. an, dass Ihr Unternehmen („Contoso“) über eine Partnerschaft mit einem anderen Unternehmen (Fabrikam) verfügt. Sie können Fabrikam zur Liste zugelassener Domänen hinzufügen, damit Benutzer diese Gastbenutzer zu Gruppen hinzufügen können.

Nehmen wir beispielsweise an, Sie möchten Domänen für persönliche E-Mail-Adressen blockieren. Sie können eine Liste blockierter Domänen erstellen, die Domänen wie Gmail.com und Outlook.com enthält.

## Wichtige Informationen zu Listen blockierter Kontakte

- Dieses Feature ist derzeit nur in der Vorschau und als Teil einer Office 365-Lizenz. Dieses Feature wird ein Azure Active Directory (AAD) Premium-Angebot werden allgemeine Verfügbarkeit und erfordern eine AAD Premium-Lizenz.
- Sie können entweder eine Liste zugelassener oder blockierter Domänen erstellen. **Sie können jedoch nicht beide Arten von Listen einrichten.** Standardmäßig sind alle Domänen, die nicht in der Liste zugelassener Domänen enthalten sind, in der Liste blockierter Domänen enthalten, und umgekehrt.
- Sie können nur eine Richtlinie pro Organisation erstellen. Sie können dieser Richtlinie mehrere Domänen hinzufügen oder diese Richtlinie löschen, um eine neue Richtlinie zu erstellen.
- Diese Liste funktioniert unabhängig von der Liste zugelassener/blockierter Domänen von SPO. Sie müssen eine Liste zugelassener/blockierter Domänen für SPO erstellen, wenn Sie die individuelle Dateifreigabe für eine mit einer Gruppe verbundene Website einschränken möchten.
- Diese Liste gilt nicht für bereits hinzugefügte Gastmitglieder, sondern gilt nur für Gastbenutzer, die nach dem Einrichten dieser Liste hinzugefügt werden. Sie können diese über das Skript entfernen.

## Installieren der Vorschauversion für das Azure Active Directory-Modul für Windows PowerShell

**Wichtig:** Für die Vorgehensweisen in diesem Artikel benötigen Sie die **Vorschauversion** des Azure Active Directory-Moduls für Windows PowerShell, insbesondere die **AzureADPreview**-Modulversion **2.0.0.98** oder höher.

1. Öffnen Sie Windows PowerShell als Administrator:
2. Geben Sie in die Suchleiste Windows PowerShell ein.
3. Klicken Sie mit der rechten Maustaste auf Windows PowerShell, und wählen Sie **Als Administrator ausführen** aus.

```
<span data-ttu-id="86955-p109">Das Windows PowerShell-Fenster wird angezeigt. Die Aufforderung „C:\Windows\system32“ bedeutet, dass Sie es als Administrator geöffnet haben.</span><span class="sxs-lookup"><span data-stu-id="86955-p109">The Windows PowerShell window will pop open. The prompt C:\Windows\system32 means you opened it as an administrator.</span></span>
```

2. Führen Sie den folgenden Befehl aus, um festzustellen, ob eine Version des Azure Active Directory-Moduls für Windows PowerShell auf dem Computer installiert ist:

```
Get-Module -ListAvailable AzureAD*
```

- Wenn keine Ergebnisse zurückgegeben werden, führen Sie den folgenden Befehl aus, um die aktuelle Version des **AzureADPreview**-Moduls zu installieren:

```
Install-Module AzureADPreview
```

- Wenn *nur* das Modul **AzureAD** wird angezeigt, in den Ergebnissen diese Befehle aus, um die Installation des Moduls **AzureADPreview** ausführt:

```
Uninstall-Module AzureAD
```

```
Install-Module AzureADPreview
```

- Wenn *nur* das Modul **AzureADPreview** in den Ergebnissen angezeigt wird, aber die Version kleiner als **2.0.0.98 ist**, führen Sie diese Befehle zum Aktualisieren:

```
Uninstall-Module AzureADPreview
```

```
Install-Module AzureADPreview
```

- Wenn sowohl die **AzureAD** und **AzureADPreview** Module werden in den Ergebnissen angezeigt, aber die Version des Moduls **AzureADPreview** kleiner als **2.0.0.98 ist**, führen Sie diese Befehle zum Aktualisieren:

```
Uninstall-Module AzureAD
```

```
Uninstall-Module AzureADPreview
```

```
Install-Module AzureADPreview
```

## Erstellen einer neuen Richtlinie für Liste zugelassener oder blockierter Domänen

1. Haben Sie das **AzureADPreview**-Modul entsprechend den oben genannten Anweisungen installiert? Das Nichtvorhandensein einer **Vorschauversion** ist der häufigste Grund dafür, dass diese Schritte nicht funktionieren.
2. Wechseln Sie zur [Skript für zulassen/blockieren-Richtlinie](#) auf der Microsoft Download Center zum Herunterladen des Skripts (**Set-GuestAllowBlockDomainPolicy.ps1**) für zulassen/blockieren-Richtlinie.
3. Führen Sie das Skript mit dem folgenden Befehl aus:

```
Set-GuestAllowBlockDomainPolicy.ps1 -Update -AllowList @("contoso.com", "fabrikam.com")
```

```
<span data-ttu-id="86955-140">Ersetzen Sie dabei **contoso.com** und **fabrikam.com** durch die Domänen, die Sie zulassen möchten.</span><span class="sxs-lookup"><span data-stu-id="86955-140">Where you replace **contoso.com** and **fabrikam.com** with the domains you want to allow.</span></span>

<span data-ttu-id="86955-141">ODER</span><span class="sxs-lookup"><span data-stu-id="86955-141">OR</span></span>
```

```
Set-GuestAllowBlockDomainPolicy.ps1 -Update -BlockList @("contoso.com", "fabrikam.com")
```

Sie können nur eine Richtlinie erstellen. Wenn Sie versuchen, eine weitere Richtlinie zu erstellen, tritt ein Fehler auf.

## Ersetzen der vorhandenen Richtlinie durch eine neue Liste der Domänen

Um die vorhandenen Richtlinie durch eine neue Liste der Domänen zu ersetzen, müssen Sie den folgenden Befehl ausführen:

```
Set-GuestAllowBlockDomainPolicy.ps1 -Update -AllowList @("contoso.com", "fabrikam.com")
```

Ersetzen Sie dabei **contoso.com** und **fabrikam.com** durch die Domänen, die Sie zulassen möchten.

ODER

```
Set-GuestAllowBlockDomainPolicy.ps1 -Update -BlockList @("contoso.com", "fabrikam.com")
```

## Hinzufügen weiterer Domänen zur vorhandenen Richtlinie

Um eine neue Domäne zur Richtlinie hinzuzufügen, müssen Sie den folgenden Befehl ausführen:

```
Set-GuestAllowBlockDomainPolicy.ps1 -Append -AllowList @("contoso.com")
```

Ersetzen Sie dabei **contoso.com** und **fabrikam.com** durch die Domänen, die Sie zulassen möchten.

ODER

```
Set-GuestAllowBlockDomainPolicy.ps1 -Append -BlockList @("contoso.com")
```

## Migrieren vorhandener Richtlinie für zugelassene/blockierte Domänen von SharePoint Online

Diese Liste funktioniert unabhängig von der Liste zugelassener/blockierter Domänen von SharePoint Online. Sie müssten eine Liste zugelassener/blockierter Domänen für SharePoint Online erstellen, wenn Sie die individuelle Dateifreigabe für eine mit einer Gruppe verbundene Website einschränken möchten.

Wenn Ihre Organisation bereits über eine Liste zugelassener/blockierter Domänen für SharePoint Online verfügt, können Sie diese Liste mit dem folgenden Befehl migrieren.

1. Installieren Sie das [SharePoint Online-Verwaltungstool](#).
2. Führen Sie den folgenden Befehl aus:

```
Set-GuestAllowBlockDomainPolicy.ps1 -MigrateFromSharepoint
```

## Löschen der Liste der Domänen

Führen Sie den folgenden Befehl aus, um alle Domänen aus der Richtlinie zu entfernen:

```
Set-GuestAllowBlockDomainPolicy.ps1 -Remove
```

## Skript für die Richtlinie zum Zulassen/Blockieren

Wechseln Sie zur [Skript für zulassen/blockieren-Richtlinie](#) auf der Microsoft Download Center zum Herunterladen des Skripts ( **Set-GuestAllowBlockDomainPolicy.ps1** ) für zulassen/blockieren-Richtlinie.

# Verwalten von E-Mail-Kontakten

18.12.2018 • 18 minutes to read

E-Mail-Kontakte sind E-Mail-aktivierte Verzeichnisdienstobjekte, die Informationen über Personen oder Organisationen außerhalb der Exchange- oder Exchange Online-Organisation enthalten. Jeder E-Mail-Kontakt verfügt über eine externe E-Mail-Adresse. Weitere Informationen zu E-Mail-Kontakten finden Sie unter [Empfänger](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berechtigungen für die Empfängerbereitstellung" im Thema [Mailbox Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen eines E-Mail-Kontakts

### Erstellen eines E-Mail-Kontakts mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Kontakte**.
2. Klicken Sie auf **neu**  > **e-Mail-Kontakts**.
3. Füllen Sie auf der Seite **Neuer E-Mail-Kontakt** folgende Felder aus:
  - **Vorname:** in diesem Feld können, geben Sie den Vornamen des Kontakts ein.
  - **Initialen:** Verwenden Sie dieses Feld Initialen des Kontakts eingeben.
  - **Nachname:** in diesem Feld können, geben Sie den Nachnamen des Kontakts ein.
  - **\*\*\* Anzeigename\*\*:** in diesem Feld können Sie einen Anzeigennamen für den Kontakt einzugeben. Dies ist der Name, der in der Kontaktliste in der Exchange-Verwaltungskonsole und im Adressbuch Ihrer Organisation aufgeführt wird. Standardmäßig wird dieses Feld mit dem Namen aufgefüllt, die Sie in den Feldern **Vorname**, **Initialen** und **Nachname** eingeben. Wenn Sie die einzelnen Felder verwendet haben, müssen Sie einen Namen, da es erforderlich ist noch in dieses Feld eingeben. Der Name darf 64 Zeichen nicht überschreiten.
  - **\*\*\* Namen\*\*:** in diesem Feld können Sie einen Namen für den Kontakt eingeben. Dies ist der Name, der im Verzeichnisdienst aufgeführt wird. Wie der Anzeigename wird in diesem Feld standardmäßig mit den Namen aufgefüllt, die Sie in den Feldern **Vorname**, **Initialen** und **Nachname** eingeben. Wenn Sie die einzelnen Felder verwendet haben, müssen Sie einen Namen, da es erforderlich ist noch in dieses Feld eingeben. Der Name darf 64 Zeichen nicht überschreiten.

- \*\*\* Alias\*\*: Geben Sie einen Alias in diesem Feld können (64 Zeichen oder weniger) für den Kontakt. Dieses Feld ist erforderlich.
- \*\*\* Externe e-Mail-Adresse\*\*: in diesem Feld das externen e-Mail-Konto des Kontakts eingeben können. Dieses Feld ist erforderlich. E-Mail an diesen Kontakt gesendet wird an diese e-Mail-Adresse weitergeleitet.
- **Organisationseinheit**: Sie können eine Organisationseinheit (OU) als den Standardwert der Empfängerbereich auswählen. Wenn der Empfängerbereich auf die Gesamtstruktur festgelegt ist, wird der Standardwert in den Container Users in der Domäne festgelegt, die den Computer enthält, auf dem der Exchange-Verwaltungskonsole ausgeführt wird. Wenn der Empfängerbereich auf eine bestimmte Domäne festgelegt ist, ist der Container "Users" in dieser Domäne standardmäßig aktiviert. Wenn der Empfängerbereich auf eine bestimmte Organisationseinheit festgelegt ist, ist dieser Organisationseinheit standardmäßig aktiviert.

Um eine andere Organisationseinheit auszuwählen, klicken Sie auf **Durchsuchen**. In diesem Dialogfeld werden alle Organisationseinheiten der Gesamtstruktur angezeigt, die sich in einem bestimmten Bereich befinden. Wählen Sie die gewünschte Organisationseinheit aus, und klicken Sie dann auf **OK**.

#### **NOTE**

Feld **Organisationseinheit** ist nur verfügbar in Exchange Server. Es ist nicht verfügbar in Exchange Online.

4. Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

### **Verwenden von Exchange Online PowerShell, e-Mail-Kontakt erstellen**

Dieses Beispiel erstellt einen e-Mail-Kontakt für Debra Garcia in Exchange Server.

```
New-MailContact -Name "Debra Garcia" -ExternalEmailAddress dgarcia@tailspintoys.com -OrganizationalUnit Users
```

In diesem Beispiel wird ein E-Mail-Kontakt für Alan Shen in Exchange Online erstellt.

```
New-MailContact -Name "Alan Shen" -ExternalEmailAddress alans@fourthcoffee.com
```

In diesem Beispiel wird e-Mail-Aktivierung ein vorhandenes Kontakts mit dem Namen Karen Toh in Exchange Server.

```
Enable-MailContact -Identity "Karen Toh" -ExternalEmailAddress ktoh@tailspintoys.com
```

### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Führen Sie einen der folgenden Schritte aus, um die erfolgreiche Erstellung eines E-Mail-Kontakts zu überprüfen:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Kontakte**. Der neue E-Mail-Kontakt wird in der Kontaktliste angezeigt. Unter **Kontaktyp** lautet der Typ **E-Mail-Kontakt**.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um Informationen zu den neuen e-Mail-Kontakt anzuzeigen.

```
Get-MailContact <Name> | Format-List Name,RecipientTypeDetails,ExternalEmailAddress
```

## Ändern von E-Mail-Kontakt-Eigenschaften

## Ändern von E-Mail-Kontakt-Eigenschaften mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Kontakte**.
2. In der Liste der e-Mail-Kontakte und e-Mail-Benutzer, klicken Sie auf der e-Mail-Kontakt, dem Sie die Eigenschaften ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite mit den E-Mail-Kontakt-Eigenschaften auf einen der folgenden Abschnitte, um Eigenschaften anzuzeigen oder zu ändern.

### Allgemein

Verwenden Sie den Abschnitt **Allgemein**, um grundlegende Informationen zum E-Mail-Kontakt anzuzeigen oder zu ändern.

- **Vorname, Initialen, Nachname**

- \*\*\* Namen\*\*: Dies ist der Name, der in Active Directory aufgeführt wird. Wenn Sie diesen Namen ändern, kann nicht die 64 Zeichen nicht überschreiten.
- \*\*\* Anzeigenamen\*\*: dieser Name erscheint im Adressbuch Ihrer Organisation, in der und von Zeilen in e-Mail- und in der Liste der Postfächer. Dieser Name kann nicht leere Leerzeichen vor oder nach dem Anzeigenamen enthalten.
- \*\*\* Alias\*\*: Hierbei handelt es sich um Alias des e-Mail-Kontakts. Wenn Sie es ändern, in der Organisation eindeutig sein und muss 64 Zeichen oder weniger.
- \*\*\* Externe e-Mail-Adresse\*\*: Hierbei handelt es sich primäre SMTP-Adresse des e-Mail-Kontakts und ihrem externen e-Mail-Konto. E-Mail an diesen Kontakt gesendet wird an diese e-Mail-Adresse weitergeleitet.
- Klicken Sie auf **Weitere Optionen**, um die Organisationseinheit anzuzeigen, die das Konto des E-Mail-Kontakts enthält. Sie müssen "Active Directory-Benutzer und -Computer" verwenden, um den Kontakt in eine andere Organisationseinheit zu verschieben.

### Kontaktinformationen

Verwenden Sie den Abschnitt **Kontaktinformationen**, um die Kontaktinformationen des Empfängers wie z. B. E-Mail-Adresse und Telefonnummern anzuzeigen oder zu ändern. Diese Informationen werden im Adressbuch angezeigt.

### Organization (Organisation)

Verwenden Sie den Abschnitt **Organization**, um detaillierte Informationen zur Rolle des E-Mail-Kontakts in der Organisation aufzuzeichnen. Diese Informationen werden im Adressbuch angezeigt. Sie können auch ein virtuelles Organisationsdiagramm erstellen, auf das von E-Mail-Clients wie Outlook zugegriffen werden kann.

- **Titel:** Verwenden Sie dieses Feld zum Anzeigen oder Ändern des Titels des Kontakts.
- **Abteilung:** Verwenden Sie dieses Feld zum Anzeigen oder Ändern der Abteilungen, in denen der Kontakt arbeitet. In diesem Feld können Sie Empfängerbedingungen für dynamische Verteilergruppen erstellen und Adresslisten.
- **Unternehmen:** Verwenden Sie dieses Feld zum Anzeigen oder Ändern des Unternehmens, für das der Kontakt arbeitet. In diesem Feld können auch Empfängerbedingungen für dynamische Verteilergruppen erstellen.
- **Manager:** Wenn einen Manager hinzufügen möchten, klicken Sie auf **Durchsuchen**. Wählen Sie im **Select Manager** eine Person aus, und klicken Sie dann auf **OK**.
- **Mitarbeiter:** in diesem Feld können nicht geändert werden. Ein direkter Mitarbeiter ist ein Empfänger, der einem bestimmten Vorgesetzten unterstellt. Wenn Sie einen Manager für den Empfänger angegeben

haben, wird diesen Empfänger als Direct Bericht die Details des Postfach des Managers angezeigt. Verwaltet den beispielsweise Markus Ann und Software, die, die e-Mail-Kontakte befinden, damit Markus im Feld **Manager** in der Organisationseigenschaften für Ann und Software angegeben ist, und Ann und Software, die im Feld **Mitarbeiter** in den Eigenschaften des Markus des Postfachs angezeigt werden.

#### E-Mail-Optionen

Verwenden Sie den Abschnitt **E-Mail-Optionen**, um Proxyadressen für einen E-Mail-Kontakt hinzuzufügen oder daraus zu entfernen oder um vorhandene Proxyadresse zu bearbeiten. Die primäre SMTP-Adresse des E-Mail-Kontakts wird in diesem Abschnitt ebenfalls angezeigt, kann aber nicht geändert werden. Zum Ändern dieser Adresse müssen Sie die externe E-Mail-Adresse des Kontakts im Abschnitt **Allgemein** ändern.

#### NOTE

Im Abschnitt **E-Mail-Optionen** ist nur verfügbar in Exchange Server. Es ist nicht verfügbar in Exchange Online.

#### E-Mail-Info

Verwenden Sie den Abschnitt **E-Mail-Info**, um eine E-Mail-Info hinzuzufügen, in der Benutzer vor möglichen Problemen gewarnt werden, bevor sie eine Nachricht an diesen Empfänger senden. Eine E-Mail-Info ist Text, der in der Infoleiste angezeigt wird, wenn dieser Empfänger dem Feld "An", "Cc" oder "Bcc" einer neuen E-Mail hinzugefügt wird.

#### NOTE

Eine E-Mail-Info kann HTML-Tags enthalten, Skripts sind jedoch nicht zulässig. Die Länge einer benutzerdefinierten E-Mail-Info darf 175 angezeigte Zeichen nicht überschreiten. HTML-Tags werden bei diesem Zeichenlimit nicht mitgezählt.

### Verwenden von Exchange Online PowerShell, e-Mail-Kontakts-Eigenschaften ändern

Die Eigenschaften eines E-Mail-Kontakts werden sowohl in Active Directory als auch in Exchange gespeichert. Im Allgemeinen verwenden Sie die Cmdlets **Get-Contact** und **Set-Contact**, um Eigenschaften von Organisations- und Kontaktinformationen zu ändern. Verwenden Sie die Cmdlets **Get-MailContact** und **Set-MailContact**, um E-Mail-bezogene Eigenschaften wie E-Mail-Adressen, E-Mail-Infos und benutzerdefinierte Attribute anzuzeigen oder zu ändern und um anzugeben, ob der Kontakt in Adresslisten ausgeblendet werden soll.

Weitere Informationen hierzu finden Sie in den folgenden Themen:

- [Get-Contact](#)
- [Set-Contact](#)
- [Get-MailContact](#)
- [Set-MailContact](#)

Hier sind einige Beispiele für die Verwendung von Exchange Online PowerShell Kontakt e-Mail-Eigenschaften ändern.

In diesem Beispiel werden die Eigenschaften für Titel, Abteilung, Unternehmen und Vorgesetzter für den E-Mail-Kontakt Kai Axford konfiguriert.

```
Set-Contact "Kai Axford" _-Title Consultant -Department "Public Relations" -Company Fabrikam -Manager "Karen Toh"
```

In diesem Beispiel wird die Eigenschaft "CustomAttribute1" für alle E-Mail-Kontakte auf den Wert "PartTime" festgelegt, und alle Kontakte werden im Organisationsadressbuch ausgeblendet.

```
Get-MailContact | Set-MailContact -CustomAttribute1 PartTime -HiddenFromAddressListsEnabled $true
```

In diesem Beispiel wird die Eigenschaft "CustomAttribute15" für alle E-Mail-Kontakte in der Abteilung "Public Relations" auf den Wert "TemporaryEmployee" festgelegt.

```
Get-Contact -Filter "Department -eq 'Public Relations'" | Set-MailContact -CustomAttribute15  
TemporaryEmployee
```

### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Gehen Sie folgendermaßen vor, um zu überprüfen, ob die Eigenschaften eines E-Mail-Kontakts erfolgreich geändert wurden:

- In der Exchange-Verwaltungskonsole, wählen Sie den e-Mail-Kontakt, und klicken Sie dann auf **Bearbeiten** um die Eigenschaft anzuzeigen, die Sie geändert haben.
- Verwenden Sie in Exchange Online PowerShell die Cmdlets **Get-Contact** und **Get-MailContact**, um die Änderungen zu überprüfen. Ein Vorteil von Exchange Online PowerShell ist, dass Sie mehrere Eigenschaften für mehrere e-Mail-Kontakte anzeigen können. Führen Sie im Beispiel oben, in dem alle e-Mail-Kontakte die CustomAttribute1-Eigenschaft auf PartTime festgelegt und aus dem Adressbuch ausgeblendet wurden den folgenden Befehl aus, um die Änderungen zu überprüfen.

```
Get-MailContact | Format-List Name,CustomAttribute1,HiddenFromAddressListsEnabled
```

Im oben stehenden Beispiel, in dem die Eigenschaft "CustomAttribute15" für alle E-Mail-Kontakte in der Abteilung "Public Relations" festgelegt wurde, führen Sie folgenden Befehl aus, um die Änderungen zu überprüfen.

```
Get-Contact -Filter "Department -eq 'Public Relations'" | Get-MailContact | Format-List  
Name,CustomAttribute15
```

## **Massenbearbeitung von E-Mail-Kontakten**

Sie können in der Exchange-Verwaltungskonsole ausgewählte Eigenschaften für mehrere E-Mail-Kontakte ändern. Wenn Sie in der Exchange-Verwaltungskonsole mindestens zwei E-Mail-Kontakte aus der Kontaktliste auswählen, werden die Eigenschaften im Detailbereich angezeigt, die per Massenbearbeitung geändert werden können. Wenn Sie eine dieser Eigenschaften ändern, wird die Änderungen auf alle ausgewählten Empfänger angewandt.

Bei der Massenbearbeitung von E-Mail-Kontakten können Sie folgende Eigenschaftsbereiche ändern:

- **Kontaktinformationen:** Ändern Sie freigegebene Eigenschaften wie Straße, PLZ und Ort.
- **Organisation:** Ändern Sie freigegebene Eigenschaften wie Abteilungsname, Firmenname und den Manager, die an die ausgewählte e-Mail-Kontakte oder e-Mail-Benutzer Berichten.

### **Ändern von E-Mail-Kontakten per Massenbearbeitung**

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Kontakte**.
2. Wählen Sie in der Kontaktliste mindestens zwei E-Mail-Kontakte aus. Für Kombinationen aus E-Mail-Kontakten und E-Mail-Benutzern ist keine Massenbearbeitung möglich.

**TIP**

Sie können mehrere benachbarte E-Mail-Kontakte auswählen, indem Sie bei gedrückter UMSCHALTTASTE auf den ersten und anschließend auf den letzten Kontakt klicken. Sie können auch mehrere nicht benachbarte E-Mail-Kontakte auswählen, indem Sie bei gedrückter STRG-TASTE auf die gewünschten Kontakte klicken.

3. Klicken Sie im Detailbereich unter **Massenbearbeitung** unter **Kontaktinformationen** oder **Organisation** auf **Aktualisieren**.

4. Nehmen Sie die Änderungen auf der Eigenschaftenseite vor, und speichern Sie Ihre Änderungen.

**Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Gehen Sie folgendermaßen vor, um die erfolgreiche Massenbearbeitung von E-Mail-Kontakten zu überprüfen:

- In der Exchange-Verwaltungskonsole, wählen Sie alle e-Mail-Kontakte, die Sie Massen bearbeitet aus, und klicken Sie dann auf **Bearbeiten** zum Anzeigen der Eigenschaften, die Sie geändert haben.
- Verwenden Sie mit dem Cmdlet **Get-Contact** in Exchange Online PowerShell um die Änderungen zu überprüfen. Angenommen Sie, dass das Feature der Massenvorgang bearbeiten in der Exchange-Verwaltungskonsole verwendet, so ändern Sie den Manager und im Büro für alle e-Mail-Kontakte von einem Anbieter Unternehmen namens A. Datum Corporation. Um diese Änderungen zu überprüfen, können Sie in Exchange Online PowerShell den folgenden Befehl ausführen.

```
Get-Contact -ResultSize unlimited -Filter {(Company -eq 'Adatum')} | Format-List Name,Office,Manager
```

# Verwalten von E-Mail-Benutzern

18.12.2018 • 37 minutes to read

E-Mail-Benutzer ähneln E-Mail-Kontakten. Beide verfügen über externe E-Mail-Adressen und können Informationen zu Personen außerhalb Ihrer Exchange- oder Exchange Online-Organisation enthalten, und beide können im freigegebenen Adressbuch und in anderen Adresslisten angezeigt werden. Im Gegensatz zu E-Mail-Kontakten verfügen E-Mail-Benutzer jedoch über Anmeldeinformationen in Ihrer Exchange- oder Office 365-Organisation und können auf Ressourcen zugreifen. Weitere Informationen finden Sie unter [Empfänger](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berechtigungen für die Empfängerbereitstellung" im Thema [Mailbox Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen eines E-Mail-Benutzers

### Erstellen eines E-Mail-Benutzers mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Kontakte > Neu > E-Mail-Benutzer**.
2. Geben Sie auf der Seite **Neuer E-Mail-Benutzer** im Feld **\* Alias** einen Alias für den E-Mail-Benutzer ein. Der Alias darf höchstens 64 Zeichen enthalten und muss in der Gesamtstruktur eindeutig sein. Dieses Feld ist erforderlich.
3. Führen Sie einen der folgenden Schritte durch, um den E-Mail-Adresstyp für den E-Mail-Benutzer anzugeben:
  - Um für die externe E-Mail-Adresse des Benutzers eine SMTP-E-Mail-Adresse anzugeben, klicken Sie auf **SMTP**.

### NOTE

Exchange überprüft SMTP-Adressen auf ordnungsgemäße Formatierung. Entspricht Ihr Eintrag nicht dem SMTP-Format, wird eine Fehlermeldung angezeigt, wenn Sie auf **Speichern** klicken, um den E-Mail-Benutzer zu erstellen.

- Um einen benutzerdefinierten Adresstyp anzugeben, aktivieren Sie das Optionsfeld, und geben Sie dann den benutzerdefinierten Adresstyp an. Sie können beispielsweise eine Adresse vom Typ X.500, GroupWise oder Lotus Notes angeben.

4. Geben Sie im Feld **\* Externe E-Mail-Adresse** die externe E-Mail-Adresse des Benutzers ein. An diesen E-Mail-Benutzer gesendete E-Mails werden an diese E-Mail-Adresse weitergeleitet. Dieses Feld ist erforderlich.

5. Wählen Sie eine der folgenden Optionen aus:

- **Vorhandene Benutzer:** Wählen Sie um e-Mail-einen vorhandenen Benutzer zu aktivieren.

Klicken Sie auf **Durchsuchen**, um das Dialogfeld **Benutzer auswählen - Vollständige Gesamtstruktur** zu öffnen. Dieses Dialogfeld enthält eine Liste mit Benutzerkonten in der Organisation, die nicht E-Mail-aktiviert sind bzw. nicht über Postfächer verfügen. Wählen Sie das Benutzerkonto aus, das für E-Mail aktiviert werden soll, und klicken Sie auf **OK**. Wenn Sie diese Option auswählen, brauchen Sie keine Informationen zum Benutzerkonto anzugeben, da diese Informationen bereits in Active Directory vorhanden sind.

- **Neuen Benutzer:** Wählen Sie ein neues Benutzerkonto in Active Directory erstellen und e-Mail-Benutzer zu aktivieren. Wenn Sie diese Option auswählen, müssen Sie die erforderlichen Informationen zum Benutzerkonto bereitstellen.

6. Wenn Sie in Schritt 5 **Neuer Benutzer** ausgewählt haben, füllen Sie die folgenden Felder auf der Seite **Neuer E-Mail-Benutzer** aus. Fahren Sie andernfalls mit Schritt 7 fort.

- **Vorname:** in diesem Feld Geben Sie den Vornamen des e-Mail-Benutzers können.
- **Initialen:** in diesem Feld Geben Sie die Initialen des e-Mail-Benutzers können.
- **Nachname:** in diesem Feld Geben Sie den Nachnamen des e-Mail-Benutzers können.
- **\*\* \* Anzeigennamen\*\*:** in diesem Feld einen Anzeigennamen für den Benutzer eingeben können. Dies ist der Name, der in der Kontaktliste in der Exchange-Verwaltungskonsole und im Adressbuch Ihrer Organisation aufgeführt wird. Standardmäßig wird dieses Feld mit dem Namen aufgefüllt, die Sie in den Feldern **Vorname**, **Initialen** und **Nachname** eingeben. Wenn Sie die einzelnen Felder verwendet haben, müssen Sie einen Namen, da es erforderlich ist noch in dieses Feld eingeben. Der Name darf 64 Zeichen nicht überschreiten.
- **\*\* \* Namen\*\*:** in diesem Feld Geben Sie einen Namen für den e-Mail-Benutzer können. Dies ist der Name, der im Verzeichnisdienst aufgeführt wird. In diesem Feld wird auch mit den Namen aufgefüllt, die Sie in den Feldern **Vorname**, **Initialen** und **Nachname** eingeben. Wenn Sie die einzelnen Felder verwendet haben, müssen Sie noch einen Namen eingeben, da in diesem Feld erforderlich ist. Dieser Name kann nicht auch 64 Zeichen nicht überschreiten.

**NOTE**

**Das Feld** ist nur verfügbar in Exchange Server. Es ist nicht verfügbar in Exchange Online.

- **Organisationseinheit:** Sie können eine Organisationseinheit (OU) als die Standardstärke (Dies ist der Empfängerbereich) auswählen. Wenn der Empfängerbereich auf die Gesamtstruktur festgelegt ist, wird der Standardwert in den Container Users in der Domäne festgelegt, die den Computer enthält, auf dem der Exchange-Verwaltungskonsole ausgeführt wird. Wenn der Empfängerbereich auf eine bestimmte Domäne festgelegt ist, ist der Container "Users" in dieser Domäne standardmäßig aktiviert. Wenn der Empfängerbereich auf eine bestimmte Organisationseinheit festgelegt ist, ist dieser Organisationseinheit standardmäßig aktiviert.

Um eine andere Organisationseinheit auszuwählen, klicken Sie auf **Durchsuchen**. In diesem Dialogfeld werden alle Organisationseinheiten der Gesamtstruktur angezeigt, die sich in einem bestimmten Bereich befinden. Wählen Sie die gewünschte Organisationseinheit aus, und klicken Sie dann auf **OK**.

**NOTE**

Feld **Organisationseinheit** ist nur verfügbar in Exchange Server. Es ist nicht verfügbar in Exchange Online.

- \*\* \* Benutzeranmeldenamen\*\*: in diesem Feld können Sie den Namen eingeben, der der e-Mail-Benutzer zur Anmeldung bei der Domäne verwendet wird. Anmeldenamen des Benutzers besteht aus einer Benutzername auf der linken Seite des am (@)-Symbol und ein Suffix auf der rechten Seite. In der Regel ist das Suffix den Domänenamen an, in der sich das Benutzerkonto befindet.

**NOTE**

In Exchange Online heißt dieses Feld **Benutzer-ID**.

- \*\* \* Neues Kennwort\*\*: in diesem Feld können Sie das Kennwort eingeben, der der e-Mail-Benutzer zur Anmeldung bei der Domäne verwendet werden muss.

**NOTE**

Stellen Sie sicher, dass das angegebene Kennwort den Anforderungen hinsichtlich Länge, Komplexität und Verlauf der Domäne entspricht, in der Sie das Benutzerkonto erstellen.

- \*\* \* Kennwort bestätigen\*\*: Verwenden Sie dieses Feld bestätigen das Kennwort ein, den Sie im Feld **Kennwort** eingegeben haben.
- **Bei der nächsten Anmeldung kennwortänderung anfordern:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie e-Mail-Benutzer das Kennwort zurücksetzen, wenn sie sich zunächst auf die Domäne anmelden möchten.

Wenn Sie dieses Kontrollkästchen aktivieren, wird der neue E-Mail-Benutzer bei der erstmaligen Anmeldung über ein Dialogfeld aufgefordert, das Kennwort zu ändern. Der E-Mail-Benutzer kann erst dann Aufgaben ausführen, wenn das Kennwort erfolgreich geändert wurde.

7. Wenn Sie fertig sind, klicken Sie auf **Speichern**, um den E-Mail-Benutzer zu erstellen.

### Verwenden Sie Exchange Online PowerShell, um einen e-Mail-Benutzer erstellen

In diesem Beispiel wird ein e-Mail-aktivierten Benutzerkonto für Jeffrey Zeng in Exchange Server mit den folgenden Angaben erstellt:

- Der Name und Anzeigename lautet "Jeffrey Zeng".
- Der Alias ist "jeffreyz".
- Die externe E-Mail-Adresse ist "jzeng@tailspintoys.com".
- Der Vorname ist "Jeffrey" und der Nachname ist "Zeng".
- Der Anmeldename ist "jeffreyz@contoso.com".
- Das Kennwort lautet "Pa\$\$word1".
- E-Mail-Benutzers wird in die Standard-OU erstellt werden. Wenn Sie eine andere Organisationseinheit angeben, können Sie den *OrganizationalUnit*-Parameter verwenden.

```
New-MailUser -Name "Jeffrey Zeng" -Alias jeffreyz -ExternalEmailAddress jzeng@tailspintoys.com -FirstName Jeffrey -LastName Zeng -UserPrincipalName jeffreyz@contoso.com -Password (ConvertTo-SecureString -String 'Pa$$word1' -AsPlainText -Force)
```

In diesem Beispiel wird in Exchange Online für Rene Valdes ein E-Mail-aktiviertes Benutzerkonto.

```
New-MailUser -Name "Rene Valdes" -Alias renev -ExternalEmailAddress renevaldes@fineartschool.edu -FirstName Rene -LastName Valdes -MicrosoftOnlineServicesID renev@contoso.com -Password (ConvertTo-SecureString -String 'P@ssw0rd' -AsPlainText -Force)
```

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie wie folgt vor, um die erfolgreiche Erstellung eines E-Mail-Benutzers zu überprüfen:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Kontakte**. Der neue E-Mail-Benutzer wird in der Liste der Kontakte angezeigt. Unter **Kontakttyp** lautet der Typ **E-Mail-Benutzer**.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um Informationen zu den neuen e-Mail-Benutzer anzuzeigen.

```
Get-MailUser <Name> | Format-List Name,RecipientTypeDetails,ExternalEmailAddress
```

## Ändern von E-Mail-Benutzereigenschaften

Nachdem Sie einen e-Mail-Benutzer erstellt haben, können Sie Änderungen vornehmen und mithilfe der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell zusätzliche Eigenschaften festlegen.

Sie können auch Eigenschaften für mehrere Benutzerpostfächer gleichzeitig ändern. Weitere Informationen finden Sie unter [Massenbearbeitung von E-Mail-Benutzern Verwenden mithilfe der Exchange-Verwaltungskonsole](#).

Die geschätzte Zeit bis zum Abschließen des Vorgangs variiert je nach der Anzahl von Eigenschaften, die Sie anzeigen oder ändern möchten.

### Ändern von Benutzerpostfacheigenschaften mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Kontakte**.
2. In der Liste der Kontakte, klicken Sie auf der e-Mail-Benutzer, dem Sie die Eigenschaften ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite mit den Eigenschaften des E-Mail-Benutzers auf einen der folgenden Abschnitte, um Eigenschaften anzuzeigen oder zu ändern.

#### Allgemein

Klicken Sie auf den Abschnitt **Allgemein**, um grundlegende Informationen zum E-Mail-Benutzer anzuzeigen oder zu ändern.

##### • Vorname, Initialen, Nachname

- \*\* \* Namen\*\*: Dies ist der Name, der in Active Directory aufgeführt wird. Wenn Sie diesen Namen ändern, kann nicht die 64 Zeichen nicht überschreiten.
- \*\* \* Anzeigenamen\*\*: dieser Name erscheint im Adressbuch Ihrer Organisation, in der: und aus: Zeilen in e-Mail- und in der Liste der Kontakte in der Exchange-Verwaltungskonsole. Dieser Name kann nicht leere Leerzeichen vor oder nach dem Anzeigenamen enthalten.

- \*\*\* Benutzeranmeldenamen\*\*: Dies ist der Name, der der Benutzer zur Anmeldung bei der Domäne verwendet. In Exchange Online ist dies die Benutzer-ID, die der Benutzer zur Anmeldung bei Office 365 verwendet.
- Ausblenden von Adresslisten:** Aktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass den e-Mail-Benutzer angezeigt wird, in dem Adressbuch und anderen Adresslisten, die in Ihrer Exchange-Organisation definiert sind. Nachdem Sie dieses Kontrollkästchen aktivieren, können Benutzer weiterhin Nachrichten an den Empfänger senden mithilfe der e-Mail-Adresse.
- Bei der nächsten Anmeldung kennwortänderung anfordern:** Aktivieren Sie dieses Kontrollkästchen, wenn das nächste Mal ihr Kennwort zurücksetzen der Anmeldung an der Domäne den Benutzer angezeigt werden soll.

**NOTE**

Dieses Feld ist nicht in Exchange Online verfügbar.

Klicken Sie auf **Weitere Optionen**, um diese zusätzlichen Eigenschaften anzuzeigen oder zu ändern:

- Organisationseinheit:** Dieses schreibgeschützte Feld zeigt die Organisationseinheit (OU), die das Mail-Benutzerkonto enthält. Sie müssen Active Directory-Benutzer und -Computer verwenden, um das Konto in eine andere Organisationseinheit verschieben.

**NOTE**

Dieses Feld ist nicht in Exchange Online verfügbar.

- Benutzerdefinierte Attribute:** in diesem Abschnitt werden die benutzerdefinierten Attribute für den e-Mail-Benutzer definiert ist. Klicken Sie auf **Bearbeiten**, um benutzerdefinierte Attributwerte anzugeben, . Sie können bis zu 15 benutzerdefinierte Attribute für den Empfänger angeben.

#### Kontaktinformationen

Verwenden Sie den Abschnitt **Kontaktinformationen**, um die Kontaktinformationen des Benutzers anzuzeigen oder zu ändern. Die Informationen auf dieser Seite werden im Adressbuch angezeigt. Klicken Sie auf **Weitere Optionen**, um zusätzliche Felder anzuzeigen.

**TIP**

Sie können das Feld **Bundesland/Kanton** verwenden, um Empfängerbedingungen für dynamische Verteilergruppen, Richtlinien für E-Mail-Adressen oder Adresslisten zu erstellen.

#### Organization (Organisation)

Verwenden Sie den Abschnitt **Organisation**, um ausführliche Informationen zur Rolle des Benutzers in der Organisation aufzuziehen. Diese Informationen werden im Adressbuch angezeigt. Sie können auch ein virtuelles Organisationsdiagramm erstellen, auf das von E-Mail-Clients wie Outlook zugegriffen werden kann.

- Titel:** Verwenden Sie dieses Feld zum Anzeigen oder Ändern der Titel des Empfängers.
- Abteilung:** Verwenden Sie dieses Feld zum Anzeigen oder Ändern der Abteilung, in der der Benutzer arbeitet. Verwenden Sie dieses Feld, um Empfängerbedingungen für dynamische Verteilergruppen, e-Mail-Adressrichtlinien zu erstellen oder Adresslisten.
- Unternehmen:** Verwenden Sie dieses Feld zum Anzeigen oder Ändern des Unternehmens, für das der Benutzer arbeitet. Verwenden Sie dieses Feld, um Empfängerbedingungen für dynamische

Verteilergruppen, e-Mail-Adressrichtlinien erstellen oder Adresslisten.

- **Manager:** Wenn einen Manager hinzufügen möchten, klicken Sie auf **Durchsuchen**. Wählen Sie im **Select Manager** eine Person aus, und klicken Sie dann auf **OK**.
- **Mitarbeiter:** in diesem Feld können nicht geändert werden. Ein direkter Mitarbeiter ist ein Benutzer, die einem bestimmten Vorgesetzten unterstellt. Wenn Sie einen Manager für den Benutzer angegeben haben, wird der Benutzer als Direct Bericht die Details des Postfach des Managers angezeigt. Beispielsweise verwaltet Marlies Chris und Kate, Marlies im Feld **Manager** für Chris und Kate angegeben ist, und Chris und Kate werden im Feld **Mitarbeiter** in den Eigenschaften Marliess Konto angezeigt.

#### E-Mail-Adressen

Im Abschnitt **E-Mail-Adressen** können Sie die E-Mail-Adressen anzeigen und ändern, die dem E-Mail-Benutzer zugeordnet sind. Dazu gehören die primäre SMTP-Adresse des E-Mail-Benutzers, alle externen E-Mail-Adressen und alle zugehörigen Proxyadressen. Die primäre SMTP-Adresse (auch als Standardantwortadresse bezeichnet) wird fettgedruckt in der Adressliste angezeigt. Der Wert **SMTP** in der Spalte **Typ** wird dabei in Großbuchstaben angegeben. Nachdem der E-Mail-Benutzer erstellt wurde, sind die primäre SMTP-Adresse und externe E-Mail-Adresse standardmäßig gleich.

- **Hinzufügen:** Klicken Sie auf **Add**  So fügen Sie eine neue e-Mail-Adresse für dieses Postfach hinzu. Wählen Sie eine der folgenden Adresstypen:
  - **SMTP:** Dies ist die Adresse. Klicken Sie auf diese Schaltfläche, und geben Sie dann die neue SMTP-Adresse in der \*\* \* E-Mail-Adresse\*\* Feld.
  - **Benutzerdefinierte Adresstyp:** Klicken Sie auf diese Schaltfläche, und geben Sie einen der unterstützten nicht-SMTP-e-Mail-Adresstypen in der \*\* \* E-Mail-Adresse\*\* Feld.

#### NOTE

Mit Ausnahme von X.400-Adressen überprüft Exchange benutzerdefinierte Adressen nicht auf ordnungsgemäße Formatierung. Sie müssen sicherstellen, dass die von Ihnen angegebene benutzerdefinierte Adresse die Formatanforderungen für den jeweiligen Adresstyp erfüllt.

- **Legen Sie die externe e-Mail-Adresse:** in diesem Feld die e-Mail-Adresse des Benutzers externen ändern können. E-Mail an diesen e-Mail-Benutzer gesendet wird an diese e-Mail-Adresse weitergeleitet.
- **E-Mail-Adressen basierend auf der e-Mail-Adressrichtlinie angewendet an diesen Empfänger automatisch aktualisieren:** Aktivieren Sie dieses Kontrollkästchen, um dem Empfänger der e-Mail-Adressen automatisch aktualisierte basierend auf Änderungen an e-Mail-Adressrichtlinien in Ihrer Organisation. Dieses Feld ist standardmäßig aktiviert.

#### NOTE

Dieses Kontrollkästchen ist nicht in Exchange Online verfügbar.

#### Nachrichtenflusseinstellungen

Im Abschnitt **Nachrichtenübermittlungseinstellungen** können Sie die folgenden Einstellungen anzeigen oder ändern:

- **Nachricht Größeneinschränkungen:** Diese Einstellungen steuern die Größe von Nachrichten, die der e-Mail-Benutzer senden und empfangen kann. Klicken Sie auf **Details anzeigen**, zum Anzeigen und ändern die maximale Größe für gesendete und empfangene Nachrichten.
  - **Gesendete Nachrichten:** zum Angeben der maximal zulässigen Größe für diesen Benutzer

gesendeten Nachrichten aktivieren Sie das Kontrollkästchen **maximale Nachrichtengröße (KB)**, und geben Sie einen Wert in das Feld ein. Die Nachrichtengröße muss zwischen 0 und 2.097.151 KB sein. Wenn der Benutzer eine Nachricht größer als die angegebene Größe sendet, wird die Nachricht mit einer beschreibende Fehlermeldung an den Benutzer zurückgegeben werden soll.

- **Empfangene Nachrichten:** um eine maximale Größe für Nachrichten, die von diesem Benutzer angeben, aktivieren Sie das Kontrollkästchen **maximale Nachrichtengröße (KB)**, und geben Sie einen Wert in das Feld ein. Die Nachrichtengröße muss zwischen 0 und 2.097.151 KB sein. Wenn der Benutzer eine Nachricht größer als die angegebene Größe empfängt, wird die Nachricht mit einer beschreibende Fehlermeldung an den Absender zurückgegeben werden soll.
- **Nachricht Delivery Restrictions:** Diese Einstellungen steuern Sie, wer e-Mail-Nachrichten an diesen Benutzer Nachrichten senden kann. Klicken Sie auf **Details anzeigen**, um anzeigen und ändern diese Beschränkungen.
  - **Nachrichten annehmen von:** Verwenden Sie diesen Abschnitt, um anzugeben, wer Nachrichten an diesen Benutzer senden kann.
  - **Alle Absender:** Wählen Sie diese Option, um anzugeben, dass der Benutzer Nachrichten von allen Absendern annehmen kann. Dazu gehören sowohl Absender in Ihrer Exchange-Organisation und externe Absender. Diese Option ist standardmäßig aktiviert. Diese Option umfasst externe Benutzer nur, wenn Sie das Kontrollkästchen **erforderlich, dass die Authentifizierung aller Absender anfordern** deaktivieren. Wenn Sie dieses Kontrollkästchen aktivieren, werden Nachrichten von externen Benutzern abgelehnt.
  - **Nur Absender in der folgenden Liste:** Wählen Sie diese Option, um anzugeben, dass der Benutzer Nachrichten nur von einer bestimmten Gruppe von Absendern in Ihrer Exchange-Organisation akzeptieren kann. Klicken Sie auf **Hinzufügen** die Seite **Wählen Sie Empfänger** angezeigt werden, die eine Liste aller Empfänger in Ihrer Exchange-Organisation angezeigt wird. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen**.
  - **Erfordern, dass alle Absender authentifiziert werden:** Wählen Sie diese Option aus, um zu verhindern, dass anonyme Benutzer Nachrichten an die Benutzer senden können.
  - **Nachrichten ablehnen von:** Verwenden Sie diesen Abschnitt zu hindern, Nachrichten an diesen Benutzer zu senden.
  - **Kein Absender:** Wählen Sie diese Option, um anzugeben, dass das Postfach ablehnen von Nachrichten von beliebigen Absendern in der Exchange-Organisation wird nicht aus. Diese Option ist standardmäßig aktiviert.
  - **Absender in der folgenden Liste:** Wählen Sie diese Option, um anzugeben, dass das Postfach ablehnen von Nachrichten von einer bestimmten Gruppe von Absendern in Ihrer Exchange-Organisation wird. Klicken Sie auf **Hinzufügen** die Seite **Wählen Sie Empfänger** angezeigt werden, die eine Liste aller Empfänger in Ihrer Exchange-Organisation angezeigt wird. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen**.

#### Mitglied von

Im Abschnitt **Mitglied von** können Sie eine Liste der Verteiler- oder Sicherheitsgruppen anzeigen, denen dieser Benutzer angehört. Informationen zur Mitgliedschaft können auf dieser Seite nicht geändert werden. Beachten Sie, dass der Benutzer möglicherweise den Kriterien für mindestens eine dynamische Verteilergruppe in Ihrer Organisation entspricht. Dynamische Verteilergruppen werden auf dieser Seite jedoch nicht angezeigt, da ihre

Mitgliedschaft zum Zeitpunkt ihrer Verwendung stets neu berechnet wird.

#### E-Mail-Info

Verwenden Sie den Abschnitt **E-Mail-Info**, um eine E-Mail-Info hinzuzufügen, in der Benutzer vor möglichen Problemen gewarnt werden, bevor sie eine Nachricht an diesen Empfänger senden. Eine E-Mail-Info ist Text, der in der Infoleiste angezeigt wird, wenn dieser Empfänger dem Feld "An", "Cc" oder "Bcc" einer neuen E-Mail hinzugefügt wird.

#### NOTE

Eine E-Mail-Info kann HTML-Tags enthalten, Skripts sind jedoch nicht zulässig. Die Länge einer benutzerdefinierten E-Mail-Info darf 175 angezeigte Zeichen nicht überschreiten. HTML-Tags werden bei diesem Zeichenlimit nicht mitgezählt.

### Verwenden von Exchange Online PowerShell, Mail-Benutzereigenschaften ändern

Die Eigenschaften eines E-Mail-Benutzers sind in Active Directory und in Exchange gespeichert. Im Allgemeinen verwenden Sie die Cmdlets **Get-User** und **Set-User**, um Organisations- und Kontaktinformationseigenschaften zu ändern. Sie verwenden die Cmdlets **Get-MailUser** und **Set-MailUser**, um E-Mail-bezogene Eigenschaften wie E-Mail-Adressen, E-Mail-Infos und benutzerdefinierte Attribute anzuzeigen und zu ändern. Hier können Sie auch festlegen, ob der E-Mail-Benutzer in Adresslisten ausgeblendet werden soll.

Mit den Cmdlets **Get-MailUser** und **Set-MailUser** können Sie die Eigenschaften von E-Mail-Benutzern anzeigen und ändern. Weitere Informationen finden Sie unter den folgenden Themen:

- [Get-User](#)
- [Set-User](#)
- [Get-MailUser](#)
- [Set-MailUser](#)

Hier sind einige Beispiele für die Verwendung von Exchange Online PowerShell Mail Benutzereigenschaften ändern.

In diesem Beispiel wird die externe E-Mail-Adresse für Pilar Pinilla festgelegt.

```
Set-MailUser "Pilar Pinilla" -ExternalEmailAddress pilarp@tailspintoys.com
```

In diesem Beispiel werden alle E-Mail-Benutzer im Adressbuch der Organisation ausgeblendet.

```
Get-MailUser | Set-MailUser -HiddenFromAddressListsEnabled $true
```

In diesem Beispiel wird die Eigenschaft "Company" für alle E-Mail-Benutzer in "Contoso" geändert.

```
Get-User -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'mailuser')} | Set-User -Company Contoso
```

In diesem Beispiel wird die Eigenschaft "CustomAttribute1" für alle E-Mail-Benutzer, deren Eigenschaft "Company" den Wert "Contoso" aufweist, in den Wert "ContosoEmployee" geändert.

```
Get-User -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'mailuser') -and (Company -eq 'Contoso')} | Set-MailUser -CustomAttribute1 ContosoEmployee
```

**Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Gehen Sie wie folgt vor, um die erfolgreiche Änderung der Eigenschaften von E-Mail-Benutzern zu überprüfen:

- In der Exchange-Verwaltungskonsole, wählen Sie den e-Mail-Benutzer aus, und klicken Sie dann auf **Bearbeiten** um die-Eigenschaft anzuzeigen, die Sie geändert haben.
- Verwenden Sie in Exchange Online PowerShell die Cmdlets **Get-User** und **Get-MailUser**, um die Änderungen zu überprüfen. Ein Vorteil von Exchange Online PowerShell ist, dass Sie mehrere Eigenschaften für mehrere e-Mail-Kontakte anzeigen können.

```
Get-MailUser | Format-List Name,CustomAttribute1
```

Führen Sie für das Beispiel oben, in dem die Eigenschaft "Company" für alle E-Mail-Kontakte auf "Contoso" festgelegt wurde, den folgenden Befehl aus, um die Änderungen zu überprüfen:

```
Get-User -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'mailuser')} | Format-List Name,Company
```

Führen Sie im Beispiel oben, in dem die Eigenschaft "CustomAttribute1" auf "ContosoEmployee" festgelegt wurde, den folgenden Befehl aus, um die Änderungen zu überprüfen.

```
Get-MailUser | Format-List Name,CustomAttribute1
```

## Massenbearbeitung von E-Mail-Benutzern

Sie können mithilfe der Exchange-Verwaltungskonsole auch ausgewählte Eigenschaften für mehrere E-Mail-Benutzer ändern. Wenn Sie in der Kontaktliste in der Exchange-Verwaltungskonsole zwei oder mehr Benutzer auswählen, werden die Eigenschaften, für die eine Massenbearbeitung möglich ist, im Detailbereich angezeigt. Wenn Sie eine dieser Eigenschaften ändern, wird die Änderungen auf alle ausgewählten Empfänger angewandt.

Bei der Massenbearbeitung von E-Mail-Benutzern können Sie die folgenden Eigenschaftsbereiche ändern:

- **Kontaktinformationen:** Ändern Sie freigegebene Eigenschaften wie Straße, PLZ und Ort.
- **Organisation:** Ändern Sie freigegebene Eigenschaften wie Abteilungsname, Firmenname und den Manager, die an die ausgewählte e-Mail-Kontakte oder e-Mail-Benutzer Berichten.

### Massenbearbeitung von E-Mail-Benutzern Verwenden mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Kontakte**.
2. Wählen Sie in der Liste der Kontakte mindestens zwei E-Mail-Benutzer aus. Für Kombinationen aus E-Mail-Kontakten und E-Mail-Benutzern ist keine Massenbearbeitung möglich.

#### TIP

Sie können mehrere benachbarte E-Mail-Benutzer auswählen, indem Sie bei gedrückter UMSCHALTTASTE auf den ersten und anschließend auf den letzten E-Mail-Benutzer klicken, den Sie bearbeiten möchten. Sie können auch mehrere nicht benachbarte E-Mail-Benutzer auswählen, indem Sie bei gedrückter STRG-TASTE auf die Einträge klicken, die Sie bearbeiten möchten.

3. Klicken Sie im Detailbereich unter **Massenbearbeitung** unter **Kontaktinformationen** oder **Organisation** auf **Aktualisieren**.
4. Nehmen Sie die Änderungen auf der Eigenschaftenseite vor, und speichern Sie Ihre Änderungen.

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie wie folgt vor, um die erfolgreiche Massenbearbeitung von E-Mail-Benutzern zu überprüfen:

- In der Exchange-Verwaltungskonsole, wählen Sie alle e-Mail-Benutzer, die Sie Massen bearbeitet aus, und klicken Sie dann auf **Bearbeiten** zum Anzeigen der Eigenschaften, die Sie geändert haben.
- Verwenden Sie das Cmdlet **Get-User** in Exchange Online PowerShell um die Änderungen zu überprüfen. Angenommen Sie, dass das Feature der Massenvorgang bearbeiten in der Exchange-Verwaltungskonsole verwendet, so ändern Sie den Manager und im Büro für alle e-Mail-Benutzer von einem Anbieter Unternehmen namens A. Datum Corporation. Um diese Änderungen zu überprüfen, können Sie in Exchange Online PowerShell den folgenden Befehl ausführen:

```
Get-User -ResultSize unlimited -Filter {{(RecipientTypeDetails -eq 'mailuser') -and (Company -eq 'Adatum')}} | Format-List Name,Office,Manager
```

## Verwenden der Verzeichnissynchronisierung zum Verwalten von E-Mail-Benutzern in Exchange Online

In diesem Abschnitt finden Sie weitere Informationen zum Verwalten von E-Mail-Benutzern mithilfe der Verzeichnissynchronisierung in Exchange Online. Die Verzeichnissynchronisierung steht für Kunden mit einer Hybridbereitstellung (lokale und cloudgehostete Postfächer) sowie für vollständig gehostete Exchange Online-Kunden zur Verfügung, die über ein lokales Active Directory verfügen.

### NOTE

Wenn Sie Verzeichnissynchronisierung zur Verwaltung der Empfänger verwenden, können Sie Benutzer dennoch im Office 365 Admin Center hinzufügen und verwalten. Sie werden dann jedoch nicht mit dem lokalen Active Directory synchronisiert. Dies liegt daran, dass bei der Verzeichnissynchronisierung nur Empfänger aus dem lokalen Active Directory mit der Cloud synchronisiert werden.

### NOTE

Verzeichnissynchronisierung wird empfohlen, für die Verwendung mit den folgenden Features: > **Outlook sicherer Absender und blockierter Absenderlisten**: Wenn mit dem Dienst synchronisiert, haben diese Listen Vorrang vor Spamfilterung im Dienst. Auf diese Weise können Benutzer ihre eigenen sicherer und blockierter Absenderlisten auf Basis pro Benutzer oder pro Domäne verwalten. > **Directory basierend Edge-Blockierung (DBEB)**: Weitere Informationen zu Verzeichnisbasierter finden Sie unter [Use Directory Based Edge Blocking ablehnen von Nachrichten an ungültige Empfänger gesendet](#). > **Endbenutzer Spam-Quarantäne**: für den Zugriff auf die Endbenutzer-Spamquarantäne Endbenutzer benötigen einen gültigen Office 365-Benutzer-ID und ein Kennwort. Kunden mit lokalen Postfächern muss ein gültiger e-Mail-Benutzer. > **Transportregeln**: Wenn Sie die verzeichnissynchronisierung verwenden, die bestehende Active Directory-Benutzer und-Gruppen in die Cloud automatisch hochgeladen werden und anschließend Sie Transportregeln, die auf bestimmte Benutzer und/oder Gruppen erstellen können ohne abzielen Fügen Sie sie manuell über die Exchange-Verwaltungskonsole oder die remote Windows PowerShell hinzu. Hinweis: Diese [dynamische Verteilergruppen](#) nicht über die verzeichnissynchronisierung synchronisiert werden können.

## Bevor Sie beginnen

Rufen Sie die erforderlichen Berechtigungen ab, und bereiten Sie die Verzeichnissynchronisierung vor, wie unter [Vorbereiten der Verzeichnissynchronisierung](#) beschrieben.

## So synchronisieren Sie Benutzerverzeichnisse

1. Aktivieren Sie die Verzeichnissynchronisierung, wie unter [Aktivieren der Verzeichnissynchronisierung](#)

beschrieben.

2. Richten Sie den Computer für die Verzeichnissynchronisierung ein, wie unter [Einrichten des Computers für die Verzeichnissynchronisierung](#) beschrieben.
3. Synchronisieren Sie die Verzeichnisse, wie unter [Synchronisieren der Verzeichnisse mithilfe des Konfigurations-Assistenten](#) beschrieben.

**IMPORTANT**

Wenn Sie den Konfigurationsassistent für Azure Active Directory-Synchronisierungstool abschließen, wird in Ihrer Active Directory-Gesamtstruktur das Konto **MSOL\_AD\_SYNC** erstellt. Dieses Konto wird zum Lesen und Synchronisieren der lokalen Active Directory-Informationen verwendet. Damit die Verzeichnissynchronisierung ordnungsgemäß ausgeführt wird, müssen Sie sicherstellen, dass TCP 443 auf dem lokalen Verzeichnissynchronisierungsserver geöffnet ist.

4. Aktivieren Sie die synchronisierten Benutzer, wie unter [Aktivieren synchronisierter Benutzer](#) beschrieben.
5. Verwalten Sie die Verzeichnissynchronisierung, wie unter [Verwalten der Verzeichnissynchronisierung](#) beschrieben.
6. Überprüfen Sie, ob Exchange Online korrekt synchronisiert. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Kontakte**, und vergewissern Sie sich, dass die Liste der Benutzer in Ihrer lokalen Umgebung korrekt synchronisiert wird.

# Erstellen und Verwalten von Raumpostfächern

18.12.2018 • 25 minutes to read

Ein Raumpostfach ist ein Ressourcenpostfach, das einem physischen Standort, wie einem Konferenzraum, ein Auditorium oder einen Chatroom Schulung zugeordnet ist. Nachdem ein Administrator Besprechungsraum-Postfächern erstellt hat, können Benutzer Chatrooms auf einfache Weise reservieren, durch das Einbeziehen von Besprechungsraum-Postfächern in Besprechungsanfragen. Checken Sie [Empfänger](#) für weitere Details.

Weitere Informationen zu anderen Ressourcenpostfachtypen finden Sie unter [Verwalten von Gerätepostfächern](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berechtigungen für die Empfängerbereitstellung" im Thema [Mailbox Permissions](#).

### IMPORTANT

Wenn Sie in einem hybridszenario Exchange-Server ausführen, stellen Sie sicher, dass Sie in der entsprechenden Stelle der raumpostfächer erstellen. Erstellen Ihre raumpostfächer für Ihre lokale Organisation lokale und Besprechungsraum-Postfächern für Exchange Online-Seite in der Cloud erstellt werden soll.

## Erstellen eines Raumpostfachs

### Mithilfe der Exchange-Verwaltungskonsole zum Erstellen eines raumpostfachs

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Ressourcen**.
  2. Klicken Sie auf **neu**, um das Erstellen eines raumpostfachs  > **Raumpostfach**.
  3. Verwenden Sie die Optionen auf der Seite, um die Einstellungen für das neue Ressourcenpostfach festzulegen.
- \*\*\* Raumname\*\*: in diesem Feld können Sie einen Namen für das Raumpostfach eingeben. Dies ist der Name, der in der Liste der Ressourcen-Postfach in der Exchange-Verwaltungskonsole und im Adressbuch Ihrer Organisation aufgeführt wird. Dieser Name ist erforderlich, und es darf 64 Zeichen nicht überschreiten.

### TIP

Zwar enthalten auch andere Felder Details zum Raum (beispielsweise "Ort" und "Kapazität"), es empfiehlt sich jedoch, die wichtigsten Details unter Verwendung einer konsistenten Benennungskonvention im Raumnamen zusammenzufassen. Der Grund: Benutzer erhalten so auf einfache Weise Informationen zu dem Raum, wenn sie ihn in der Besprechungsanfrage aus dem Adressbuch auswählen.

- \*\*\* E-Mail-Adresse\*\*: ein Raumpostfach hat eine e-Mail-Adresse aus, damit es buchungsanfragen empfangen kann. Die e-Mail-Adresse eines Alias auf der linken Seite des besteht aus dem @-Zeichen, die muss eindeutig sein in der Gesamtstruktur und den Namen Ihrer Domäne auf der rechten Seite. Die e-Mail-Adresse ist erforderlich.
- **Speicherort, Telefon, Kapazität:** Sie können diese Felder verwenden, um Details zu den Raum einzugeben.

Jedoch können wie bereits erwähnt, Sie umfassen einige oder alle dieser Informationen in der Raumname, damit Benutzer wird angezeigt.

#### 4. Wenn Sie alle Felder ausgefüllt haben, klicken Sie auf **Speichern**, um das Raumpostfach zu erstellen.

Nachdem Sie Ihre Raumpostfach erstellt haben, können Sie Ihre Raumpostfach zum Aktualisieren von Informationen zu den Optionen, e-Mail-Infos und Postfach Delegierung buchungs-bearbeiten. Checken Sie die Verwendung im Exchange Admin Center-Abschnitt, um raumpostfacheigenschaften ändern.

#### **Erstellen eines raumpostfachs mithilfe von Exchange Online PowerShell**

In diesem Beispiel wird ein Raumpostfach mit der folgenden Konfiguration erstellt:

- Name des Postfachs ist ConfRoom1. Dieser Name wird auch zum Erstellen von e-Mail-Adresse des Raums verwendet werden.
- Der Anzeigename in der Exchange-Verwaltungskonsole und des Adressbuchs werden Conference Room 1.
- Die Option *Room* gibt an, dass dieses Postfach als Raumpostfach erstellt wird.

```
New-Mailbox -Name ConfRoom1 -DisplayName "Conference Room 1" -Room
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-Mailbox](#).

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Sie können sicherstellen, dass Sie das Raumpostfach ordnungsgemäß eine Reihe von verschiedenen Methoden erstellt haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Ressourcen**. Das neue Raumpostfach wird in der Liste angezeigt. Klicken Sie unter **Postfachtyp** ist der Typ **Raum**.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um Informationen über das neue Raumpostfach anzuzeigen.

```
Get-Mailbox <Name> | Format-List Name,RecipientTypeDetails,PrimarySmtpAddress
```

#### **Erstellen einer Raumliste**

Wenn Sie planen, mehr als 100 Räume haben oder bereits über 100 Räume erstellt haben, verwenden Sie eine Raumliste auf um Ihre Chatrooms zu organisieren. Wenn Ihr Unternehmen über mehrere Gebäude mit Räumen, die für Besprechungen gebucht werden können verfügt, kann es hilfreich sein, zum Erstellen von Listen für jede Erstellen von Raum-. Raumlisten werden speziell Verteilergruppen markiert, die Sie verwenden können die gleiche Weise, wie Sie Verteilergruppen verwenden. Sie können jedoch nur Raumlisten von Exchange Online PowerShell erstellen.

#### **Verwenden von Exchange Online PowerShell zum Erstellen einer Raumliste**

In diesem Beispiel erstellen wir eine Raumliste für Gebäude 32.

```
New-DistributionGroup -Name "Building 32 Conference Rooms" -OrganizationalUnit "contoso.com/rooms" -RoomList
```

#### **Verwenden von Exchange Online PowerShell, einen Chatroom in eine Raumliste hinzufügen**

In diesem Beispiel fügen wir confroom3223 zur Raumliste von Gebäude 32 hinzu.

```
Add-DistributionGroupMember -Identity "Building 32 Conference Rooms" -Member confroom3223@contoso.com
```

#### **Verwenden Sie Exchange Online PowerShell, um eine Verteilergruppe in eine Raumliste zu konvertieren**

Sie haben möglicherweise bereits in der Vergangenheit Verteilergruppen erstellt, in denen Ihre Konferenzräume

enthalten sind. Sie müssen sie nicht neu erstellen. Wir können sie schnell in eine Raumliste konvertieren.

In diesem Beispiel konvertieren wir die Verteilergruppe für die Konferenzräume von Gebäude 34 in eine Raumliste.

```
Set-DistributionGroup -Identity "Building 34 Conference Rooms" -RoomList
```

## Ändern von Raumpostfacheigenschaften

Nachdem Sie ein Raumpostfach erstellt haben, können Sie Änderungen vornehmen und mithilfe der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell zusätzliche Eigenschaften festlegen.

### Verwenden Sie die Exchange-Verwaltungskonsole zum Ändern von raumpostfacheigenschaften

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Ressourcen**.
2. In der Liste der Ressourcenpostfächer, klicken Sie auf das Raumpostfach, dem Sie die Eigenschaften ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite mit den Raumpostfacheigenschaften auf einen der folgenden Abschnitte, um Eigenschaften anzuzeigen oder zu ändern.

#### Allgemein

Verwenden Sie den Abschnitt **Allgemein**, um grundlegende Informationen zur Ressource anzuzeigen oder zu ändern.

- \*\*\* Raumname\*\*: dieser Name wird in der Liste der Ressourcen-Postfach in der Exchange-Verwaltungskonsole und im Adressbuch Ihrer Organisation angezeigt. Es darf 64 Zeichen nicht überschreiten, wenn Sie ihn ändern.
- \*\*\* E-Mail-Adresse\*\*: Dieses schreibgeschützte Feld zeigt die e-Mail-Adresse für das Raumpostfach. Sie können sie im Abschnitt **E-Mail-Adresse** ändern.
- **Kapazität:** in diesem Feld können Sie die maximale Anzahl von Personen eingeben, die sicher den Raum belegt werden kann.

Klicken Sie auf **Weitere Optionen**, um diese zusätzlichen Eigenschaften anzuzeigen oder zu ändern:

- **Organisationseinheit:** Dieses schreibgeschützte Feld zeigt die Organisationseinheit (OU), das Konto für das Raumpostfach enthält. Sie müssen Active Directory-Benutzer und-Computer verwenden, um das Konto in eine andere Organisationseinheit verschieben.
- **Postfachdatenbank:** Dieses schreibgeschützte Feld zeigt den Namen der Postfachdatenbank an, der das Raumpostfach hostet. Verwenden Sie die Seite **Migration** in der Exchange-Verwaltungskonsole, um das Postfach in eine andere Datenbank verschieben.
- \*\*\* Alias\*\*: in diesem Feld können Sie den Alias für das Raumpostfach ändern.
- **Ausblenden von Adresslisten:** Aktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass das Raumpostfach angezeigt wird, in dem Adressbuch und andere Adresslisten, die in Ihrer Exchange-Organisation definiert sind. Nachdem Sie dieses Kontrollkästchen aktivieren, können Benutzer weiterhin buchen Nachrichten an das Raumpostfach senden mithilfe der e-Mail-Adresse.
- **Abteilung:** Verwenden Sie dieses Kontrollkästchen, um das angeben eine Abteilung benennen, die dem Raum zugeordnet ist. Verwenden Sie diese Eigenschaft, um empfängerbedingungen für dynamische Verteilergruppen erstellen und Adresslisten.
- **Unternehmen:** Verwenden Sie dieses Feld an ein Unternehmen, das der Raum zugeordnet ist, falls zutreffend. Wie die Abteilung-Eigenschaft können Sie diese Eigenschaft verwenden, um empfängerbedingungen für dynamische Verteilergruppen erstellen und Adresslisten.

- **Adressbuchrichtlinie:** Verwenden Sie diese Option für das Raumpostfach eine adressbuchrichtlinie (ABP) angeben. Adressbuchrichtlinien enthalten eine globale Adressliste (GAL), eines Offlineadressbuchs (OAB), eine Raumliste und eine Reihe von Adresslisten. Weitere Informationen finden Sie unter [adressbuchrichtlinien](#).

Wählen Sie in der Dropdownliste die Richtlinie aus, die diesem Postfach zugeordnet werden soll.

- **Benutzerdefinierte Attribute:** in diesem Abschnitt werden die benutzerdefinierten Attribute für das Raumpostfach definiert. Klicken Sie auf **Bearbeiten**, um benutzerdefinierte Attributwerte anzugeben,  . Sie können bis zu 15 benutzerdefinierte Attribute für den Empfänger angeben.

#### **Stellvertretungen**

Verwenden Sie diesen Abschnitt, um anzuzeigen oder zu ändern, wie der Reservierungsanfragen vom Raumpostfach behandelt werden und definieren, die annehmen oder ablehnen von buchungsanfragen, wenn dies nicht automatisch erfolgt.

- **Buchungs-Anfragen:** Wählen Sie eine der folgenden Optionen, um buchungsanfragen zu verarbeiten.

- **Annehmen oder ablehnen Buchen automatisch angefordert wird:** eine gültige Besprechungsanfrage automatisch Raum reserviert. Wenn ein Konflikt mit einer bestehenden Reservierung vorhanden ist oder wenn die Anforderung buchen die Grenzwerte für die Planung der Ressource verletzt, beispielsweise die Reservierung Dauer zu lang ist, wird die Besprechungsanfrage automatisch abgelehnt.
- **Wählen Sie Stellvertretungen, wer annehmen oder ablehnen kann buchungsanfragen:** Ressourcenstellvertretungen Verantwortung für die Annahme oder Ablehnung von Besprechungsanfragen an, die an das Raumpostfach gesendet werden. Wenn Sie mehr als eine Ressource Stellvertretung zuweisen, hat nur eine von ihnen, die für eine bestimmte Besprechungsanfrage fungiert.

- **Stellvertretungen:** Bei Auswahl der Option erfordern, dass buchungsanfragen Stellvertretung gesendet werden, werden die angegebenen Delegaten aufgeführt. Klicken Sie auf **Hinzufügen**  oder **Entfernen von**  hinzufügen oder Entfernen von Delegaten aus dieser Liste.

#### **Buchungsoptionen**

Im Abschnitt **Buchungsoptionen** können Sie die Einstellungen für die Buchungsrichtlinien anzeigen oder ändern. Diese Buchungsrichtlinien legen fest, wann der Raum eingeplant, wie lange er reserviert und wie weit im Voraus er reserviert werden kann.

- **Wiederholte Besprechungen zulassen:** Diese Einstellung ermöglicht oder verhindert, dass sich wiederholender Besprechungen für den Chatroom. Standardmäßig ist diese Einstellung aktiviert, sodass wiederholte Besprechungen zulässig sind.
- **Planung nur während der Arbeitszeit:** Diese Einstellung annimmt oder ablehnt, Besprechungsanfragen, die nicht während der Arbeitszeiten für den Raum definiert sind. Standardmäßig ist diese Einstellung deaktiviert, weshalb Besprechungsanfragen außerhalb der Arbeitszeit zulässig sind. Standardmäßig sind die Arbeitszeiten 8:00 Uhr bis 5:00 Uhr bis Freitag Montag. Sie können die Arbeitsstunden das Raumpostfach im Abschnitt Darstellung auf der Seite Kalender konfigurieren.
- **Immer ablehnen, wenn das Enddatum hinter diesem Grenzwert liegt:** Diese Einstellung steuert das Verhalten von wiederholten Besprechungen, die durch die Einstellung Maximale buchen Lead angegebenen Datum hinausgehen.
  - Wenn Sie diese Einstellung aktivieren, wird eine Serienbuchungsanfrage automatisch abgelehnt, wenn die Buchung an oder vor dem Datum beginnt, das durch den Wert im Feld **Maximale Vorlaufzeit für Buchungen** angegeben ist, und über das angegebene Datum hinausgeht. Dies ist

die Standardeinstellung.

- Wenn Sie diese Einstellung deaktivieren, wird eine Serienbuchungsanfrage automatisch angenommen, wenn Buchungsanfragen an oder vor dem Datum beginnen, das durch den Wert im Feld **Maximale Buchungsvorlaufzeit** angegeben ist, und über das angegebene Datum hinausgehen. Allerdings wird die Anzahl von Buchungen reduziert, sodass nach dem angegebenen Datum keine Buchungen möglich sind.
- **Maximum buchen Lead Zeit (in Tagen):** Diese Einstellung gibt die maximale Anzahl der Tage im voraus, die der Raum gebucht werden kann. Eine gültige Eingabe ist eine ganze Zahl zwischen 0 und 1080. Der Standardwert ist nach 180 Tagen.
- **Maximale Dauer (in Stunden):** Diese Einstellung gibt die maximale Dauer, die der Raum reserviert werden kann in einer Anforderung buchen an. Der Standardwert ist 24 Stunden.

Bei serienbuchungsanfragen, betrifft die Länge des Exchange Admin Center Instanz der serienbuchungsanfrage die maximale buchungsdauer.

Auf dieser Seite befindet sich auch ein Feld, in dem Sie eine Nachricht eingeben können, die an Benutzer gesendet wird, die Buchungsanfragen für die Reservierung des Raums senden.

#### Kontaktinformationen

Im Abschnitt **Kontaktinformationen** können Sie Kontaktinformationen anzeigen oder ändern. Die Informationen auf dieser Seite werden im Adressbuch angezeigt.

##### TIP

Sie können das Feld **Bundesland/Kanton** verwenden, um Empfängerbedingungen für dynamische Verteilergruppen, Richtlinien für E-Mail-Adressen oder Adresslisten zu erstellen.

#### E-Mail-Adresse

Im Abschnitt **E-Mail-Adresse** können Sie die E-Mail-Adressen anzeigen und ändern, die dem Raumpostfach zugeordnet sind. Dazu gehören die primäre SMTP-Adresse des Postfachs und alle zugehörigen Proxyadressen. Die primäre SMTP-Adresse (auch als Antwortadresse bezeichnet) wird fettgedruckt in der Adressliste angezeigt. Der Wert **SMTP** in der Spalte **Typ** wird dabei in Großbuchstaben angegeben.

- **Hinzufügen:** Klicken Sie auf **Add**  So fügen Sie eine neue e-Mail-Adresse für dieses Postfach hinzu. Wählen Sie eine der folgenden Adresstypen:
  - **SMTP:** Dies ist die Adresse. Klicken Sie auf diese Schaltfläche, und geben Sie dann die neue SMTP-Adresse in der \*\*\* E-Mail-Adresse\*\* Feld.
  - **EUM:** Adresse eines EUM (Exchange Unified Messaging) wird vom Microsoft Exchange Unified Messaging-Dienst verwendet, um die UM-aktivierten Empfänger in einer Exchange-Organisation zu suchen. EUM Adressen bestehen die Durchwahlnummer und die UM-Wähleinstellungen für den UM-aktivierten Benutzer. Klicken Sie auf diese Schaltfläche, und geben Sie im Feld **Adresse/Erweiterung** die Durchwahlnummer ein. Klicken Sie dann auf **Durchsuchen**, und wählen Sie aus einem Wählplan für das Postfach.
  - **Benutzerdefinierte Adresstyp:** Klicken Sie auf diese Schaltfläche, und geben Sie einen der unterstützten nicht-SMTP-e-Mail-Adresstypen in der \*\*\* E-Mail-Adresse\*\* Feld.

#### **NOTE**

Mit Ausnahme von X.400-Adressen überprüft Exchange benutzerdefinierte Adressen nicht auf ordnungsgemäße Formatierung. Sie müssen sicherstellen, dass die von Ihnen angegebene benutzerdefinierte Adresse die Formatanforderungen für den jeweiligen Adresstyp erfüllt.

#### **NOTE**

Wenn Sie eine neue E-Mail-Adresse hinzufügen, können Sie diese als primäre SMTP-Adresse festlegen.

- **E-Mail-Adressen basierend auf der e-Mail-Adressrichtlinie angewendet an diesen Empfänger automatisch aktualisieren:** Aktivieren Sie dieses Kontrollkästchen, um dem Empfänger der e-Mail-Adressen automatisch aktualisierte basierend auf Änderungen an e-Mail-Adressrichtlinien in Ihrer Organisation.

#### **E-Mail-Info**

Im Abschnitt **E-Mail-Info** können Sie eine E-Mail-Info hinzuzufügen, in der Benutzer vor möglichen Problemen gewarnt werden, bevor sie eine Buchungsanfrage an das Raumpostfach senden. Eine E-Mail-Info ist Text, der in der Infoleiste angezeigt wird, wenn dieser Empfänger dem Feld "An", "Cc" oder "Bcc" einer neuen E-Mail hinzugefügt wird.

#### **NOTE**

Eine E-Mail-Info kann HTML-Tags enthalten, Skripts sind jedoch nicht zulässig. Die Länge einer benutzerdefinierten E-Mail-Info darf 175 angezeigte Zeichen nicht überschreiten. HTML-Tags werden bei diesem Zeichenlimit nicht mitgezählt.

#### **Verwenden von Exchange Online PowerShell raumpostfacheigenschaften ändern**

Mit den folgenden Cmdlets können Sie die Eigenschaften des Raumpostfachs anzeigen und ändern: **Get-Mailbox** und **Set-Mailbox** zum Anzeigen und Ändern von allgemeinen Eigenschaften und E-Mail-Adressen für Raumpostfächer. Verwenden Sie die Cmdlets **Get-CalendarProcessing** und **Set-CalendarProcessing**, um Stellvertretungen und Buchungsoptionen anzuzeigen und zu ändern.

- **Get-User** und **Set-User**: Verwenden Sie diese Cmdlets zum Anzeigen und Ändern von allgemeinen Eigenschaften wie Standort, Abteilung und Firmennamen.
- **Get-Mailbox** und **Set-Mailbox**: Verwenden Sie diese Cmdlets zum Anzeigen und Ändern der Eigenschaften von Benutzerpostfächern wie e-Mail-Adressen und die Postfachdatenbank.
- **Get-CalendarProcessing** und **Set-CalendarProcessing**: Verwenden Sie diese Cmdlets anzeigen und Festlegen von Optionen für buchen und Stellvertretungen.

Weitere Informationen über diese Cmdlets finden Sie in de folgenden Themen:

- [Get-User](#)
- [Set-User](#)
- [Get-Mailbox](#)
- [Set-Mailbox](#)
- [Get-CalendarProcessing](#)
- [Set-CalendarProcessing](#)

Hier sind einige Beispiele für die Verwendung von Exchange Online PowerShell raumpostfacheigenschaften

ändern.

In diesem Beispiel werden der Anzeigename, die primäre SMTP-Adresse (auch als Standardantwortadresse bezeichnet) und die Raumkapazität geändert. Außerdem wird die vorherige Antwortadresse als Proxyadresse gespeichert.

```
Set-Mailbox "Conf Room 123" -DisplayName "Conf Room 31/123 (12)" -EmailAddresses  
SMTP:Rm33.123@contoso.com,smtp:rm123@contoso.com -ResourceCapacity 12
```

In diesem Beispiel werden Raumpostfächer so konfiguriert, dass Buchungsanfragen nur während der Arbeitszeit eingeplant werden können und auf maximal neun Stunden ausgelegt sind.

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'RoomMailbox')} | Set-CalendarProcessing  
-ScheduleOnlyDuringWorkHours $true -MaximumDurationInMinutes 540
```

In diesem Beispiel werden mit dem Cmdlet **Get-User** alle Raumpostfächer gesucht, die privaten Konferenzräumen entsprechen, und dann werden mit dem Cmdlet **Set-CalendarProcessing** Buchungsanfragen zur Annahme oder Ablehnung an einen Stellvertreter namens "Robin Wood" gesendet.

```
Get-User -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'RoomMailbox') -and (DisplayName -like  
'Private*')} | Set-CalendarProcessing -AllBookInPolicy $false -AllRequestInPolicy $true -ResourceDelegates  
"Robin Wood"
```

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie folgendermaßen vor, um zu überprüfen, ob Sie die Eigenschaften für ein Raumpostfach erfolgreich geändert haben:

- In der Exchange-Verwaltungskonsole, wählen Sie das Postfach aus, und klicken Sie dann auf **Bearbeiten** [ ] anzeigen, die Eigenschaft oder Funktion, die Sie geändert haben. Je nach der Eigenschaft, die Sie geändert haben, kann es im Bereich Details für das ausgewählte Postfach angezeigt werden.
- Verwenden Sie das Cmdlet **Get-Mailbox** in Exchange Online PowerShell um die Änderungen zu überprüfen. Ein Vorteil von Exchange Online PowerShell ist, dass Sie mehrere Eigenschaften für mehrere Postfächer anzeigen können. Führen Sie im obigen Beispiel, in dem buchungsanfragen nur während der Arbeitszeit eingeplant werden konnte und verfügen über die maximale Dauer 9 Stunden den folgenden Befehl aus, um die neuen Werte zu überprüfen.

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'RoomMailbox')} | Get-  
CalendarProcessing | Format-List Identity,ScheduleOnlyDuringWorkHours,MaximumDurationInMinutes
```

Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Verwalten von Gerätepostfächern

18.12.2018 • 23 minutes to read

Ein gerätepostfach ist ein Ressourcenpostfach auf eine Ressource, die nicht spezifisch sind, beispielsweise eines portablen Computers, Projektor, Mikrofon oder ein Unternehmen Auto Speicherort ist zugewiesen. Nachdem ein Administrator ein gerätepostfach erstellt, können Benutzer auf einfache Weise Ausrüstung reservieren, indem das entsprechende gerätepostfach in einer Besprechungsanfrage einschließlich. Sie können die Exchange-Verwaltungskonsole und Exchange Online PowerShell zum Erstellen eines gerätepostfachs oder Ändern der gerätepostfacheigenschaften verwenden. Weitere Informationen finden Sie unter [Recipients](#).

Informationen zu anderen Ressourcenpostfachtyp, einem Raumpostfach, finden Sie unter [Erstellen und Verwalten von raumpostfächern](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 bis 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berechtigungen für die Empfängerbereitstellung" im Thema [Mailbox Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen eines Gerätepostfachs

### Erstellen eines Gerätepostfachs mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Ressourcen**.
  2. Zum Erstellen des Gerätepostfachs klicken Sie auf **Neu > Gerätepostfach**. Zum Erstellen eines Raumpostfachs klicken Sie auf **Neu > Raumpostfach**.
  3. Verwenden Sie die Optionen auf der Seite, um die Einstellungen für das neue Ressourcenpostfach festzulegen.
- \*\*\* Equipment Namen\*\*: in diesem Feld können Sie einen Namen für das gerätepostfach eingeben. Dies ist der Name, der in der Liste der Ressourcen-Postfach in der Exchange-Verwaltungskonsole und im Adressbuch Ihrer Organisation aufgeführt wird. Dieser Name ist erforderlich, und es darf 64 Zeichen nicht überschreiten.

#### TIP

Zwar enthalten auch andere Felder Details zum Raum (z. B. die Kapazität), es empfiehlt sich jedoch, die wichtigsten Details unter Verwendung einer konsistenten Benennungskonvention im Gerätenamen zusammenzufassen. Der Grund: Benutzer erhalten so auf einfache Weise Informationen zu dem Gerät, wenn sie es in einer Besprechungsanfrage im Adressbuch auswählen.

- \*\*\* E-Mail-Adresse\*\*: ein gerätepostfach hat eine e-Mail-Adresse aus, damit es buchungsanfragen empfangen kann. Die e-Mail-Adresse eines Alias auf der linken Seite des besteht aus dem @-Zeichen, die muss eindeutig sein in der Gesamtstruktur und den Namen Ihrer Domäne auf der rechten Seite. Die e-Mail-Adresse ist erforderlich.

4. Klicken Sie nach Abschluss dieses Vorgangs auf **Speichern**, um das Gerätepostfach zu erstellen.

Nachdem Sie Ihre gerätepostfach erstellt haben, können Sie Ihre gerätepostfach zum Aktualisieren von Informationen über buchen Optionen, e-Mail-Infos und Stellvertretungen bearbeiten. Checken Sie die Änderung Equipment Mailbox Eigenschaftenabschnitt unten, um raumpostfacheigenschaften ändern

#### Erstellen eines gerätepostfachs mithilfe von Exchange Online PowerShell

In diesem Beispiel wird ein Gerätepostfach mit der folgenden Konfiguration erstellt:

- Das Gerätepostfach befindet sich in der Postfachdatenbank "Mailbox Database 1".
- Der Name des Geräts lautet "MotorVehicle2", und er wird in der globalen Adressliste als "Motor Vehicle 2" angezeigt.
- Die E-Mail-Adresse lautet "MotorVehicle2@contoso.com".
- Das Postfach befindet sich in der Organisationseinheit "Equipment".
- Der Parameter *Equipment* gibt an, dass dieses Postfach als gerätepostfach erstellt wird.

```
New-Mailbox -Database "Mailbox Database 1" -Name MotorVehicle2 -OrganizationalUnit Equipment -DisplayName "Motor Vehicle 2" -Equipment
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-Mailbox](#).

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um die erfolgreiche Erstellung eines Benutzerpostfachs zu überprüfen:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Ressourcen**. Das neue Benutzerpostfach wird in der Postfachliste angezeigt. Unter **Postfachtyp** lautet der Typ **Gerät**.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um Informationen zum neuen gerätepostfach anzuzeigen.

```
Get-Mailbox <Name> | Format-List Name,RecipientTypeDetails,PrimarySmtpAddress
```

## Ändern der Gerätepostfacheigenschaften

Nachdem Sie ein gerätepostfach erstellt haben, können Sie Änderungen vornehmen und zusätzliche Eigenschaften festlegen, mithilfe der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell.

#### Ändern der Gerätepostfacheigenschaften mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Ressourcen**.
2. In der Liste der Ressourcenpostfächer, klicken Sie auf das Gerätepostfach, dem Sie die Eigenschaften ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite mit den Gerätepostfacheigenschaften auf einen der folgenden Abschnitte, um Eigenschaften anzuzeigen oder zu ändern.

#### Allgemein

Verwenden Sie den Abschnitt **Allgemein**, um grundlegende Informationen zur Ressource anzuzeigen oder zu ändern.

- \*\* \* Equipment Namen\*\*: dieser Name wird in der Liste der Ressourcen-Postfach in der Exchange-Verwaltungskonsole und im Adressbuch Ihrer Organisation angezeigt. Es darf 64 Zeichen nicht überschreiten, wenn Sie ihn ändern.
- \*\* \* E-Mail-Adresse\*\*: Dieses schreibgeschützte Feld zeigt die e-Mail-Adresse für das Gerätepostfach. Sie können sie im Abschnitt **E-Mail-Adresse** ändern.
- **Kapazität:** in diesem Feld können Sie die maximale Anzahl von Personen, die diese Ressource verwenden können, geben, falls zutreffend, beispielsweise, wenn das Gerätepostfach ein compact Auto, entspricht Sie 4 eingeben können.

Klicken Sie auf **Weitere Optionen**, um diese zusätzlichen Eigenschaften anzuzeigen oder zu ändern:

- **Organisationseinheit:** Dieses schreibgeschützte Feld zeigt die Organisationseinheit (OU), das Konto für das Gerätepostfach enthält. Sie müssen Active Directory-Benutzer und-Computer verwenden, um das Konto in eine andere Organisationseinheit verschieben.
- **Postfachdatenbank:** Dieses schreibgeschützte Feld zeigt den Namen der Postfachdatenbank an, der das Gerätepostfach hostet. Verwenden Sie die Seite **Migration** in der Exchange-Verwaltungskonsole, um das Postfach in eine andere Datenbank verschieben.
- \*\* \* Alias\*\*: in diesem Feld können Sie um den Alias für das Gerätepostfach zu ändern.
- **Ausblenden von Adresslisten:** Aktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass Gerätepostfach angezeigt wird, in dem Adressbuch und andere Adresslisten, die in Ihrer Exchange-Organisation definiert sind. Nachdem Sie dieses Kontrollkästchen aktivieren, können Benutzer weiterhin buchen Nachrichten an das Gerätepostfach senden mithilfe der e-Mail-Adresse.
- **Abteilung:** Verwenden Sie dieses Kontrollkästchen, um das angegebene Abteilung benennen, die die Ressource zugeordnet ist. Verwenden Sie diese Eigenschaft, um Empfängerbedingungen für dynamische Verteilergruppen erstellen und Adresslisten.
- **Unternehmen:** in diesem Feld können Sie einen Mandanten angeben, der die Ressource zugeordnet ist. Wie die Abteilung-Eigenschaft können Sie diese Eigenschaft verwenden, um Empfängerbedingungen für dynamische Verteilergruppen erstellen und Adresslisten.
- **Adressbuchrichtlinie:** mit dieser Option können Sie eine Adressbuchrichtlinie (ABP) für die Ressource angeben. Adressbuchrichtlinien enthalten eine globale Adressliste (GAL), eines Offlineadressbuchs (OAB), eine Raumliste und eine Reihe von Adresslisten. Weitere Informationen finden Sie unter [adressbuchrichtlinien](#).

Wählen Sie in der Dropdownliste die Richtlinie aus, die diesem Postfach zugeordnet werden soll.

- **Benutzerdefinierte Attribute:** in diesem Abschnitt werden die benutzerdefinierten Attribute für das Gerätepostfach definiert. Klicken Sie auf **Bearbeiten**, um benutzerdefinierte Attributwerte anzugeben, . Sie können bis zu 15 benutzerdefinierte Attribute für den Empfänger angeben.

## **Stellvertretungen**

Mithilfe dieses Abschnitts können Sie anzeigen oder ändern, wie Reservierungsanfragen vom Gerätepostfach verarbeitet werden. Außerdem können Sie festlegen, wer Buchungsanfragen annehmen oder ablehnen darf, sofern dieser Vorgang nicht automatisch ausgeführt wird.

- **Buchungs-Anfragen:** Wählen Sie eine der folgenden Optionen, um buchungsanfragen zu verarbeiten.

- **Annehmen oder ablehnen Buchen automatisch angefordert wird:** eine gültige Besprechungsanfrage automatisch die Ressource reserviert. Wenn ein Konflikt mit einer bestehenden Reservierung vorhanden ist oder wenn die Anforderung buchen die Grenzwerte für die Planung der Ressource verletzt, beispielsweise die Reservierung Dauer zu lang ist, wird die Besprechungsanfrage automatisch abgelehnt.
- **Wählen Sie Stellvertretungen, wer annehmen oder ablehnen kann buchungsanfragen:** Ressourcenstellvertretungen Verantwortung für die Annahme oder Ablehnung von Besprechungsanfragen, die an das gerätepostfach gesendet werden. Wenn Sie mehr als eine Ressource Stellvertretung zuweisen, hat nur eine von ihnen, die für eine bestimmte Besprechungsanfrage fungiert.

- **Stellvertretungen:** Bei Auswahl der Option erfordern, dass buchungsanfragen Stellvertretung gesendet werden, werden die angegebenen Delegaten aufgeführt. Klicken Sie auf **Hinzufügen**  oder **Entfernen von**  hinzufügen oder Entfernen von Delegaten aus dieser Liste.

## **Buchungsoptionen**

Über den Abschnitt **Buchungsoptionen** können Sie die Einstellungen für die Buchungsrichtlinie anzeigen oder ändern, die festlegt, wann die Ressource geplant werden kann, für welchen Zeitraum und wie weit im Voraus sie reserviert werden kann.

- **Wiederholte Besprechungen zulassen:** Diese Einstellung ermöglicht oder verhindert, dass sich wiederholender Besprechungen für die Ressource. Standardmäßig ist diese Einstellung aktiviert, sodass wiederholte Besprechungen zulässig sind.
- **Planung nur während der Arbeitszeit:** Diese Einstellung annimmt oder ablehnt, Besprechungsanfragen, die nicht während der Arbeitszeit für die Ressource definiert sind. Standardmäßig ist diese Einstellung deaktiviert, weshalb Besprechungsanfragen außerhalb der Arbeitszeit zulässig sind. Standardmäßig sind die Arbeitszeiten 8:00 Uhr bis 5:00 Uhr bis Freitag Montag. Sie können die Arbeitsstunden das gerätepostfach im Abschnitt Darstellung auf der Seite Kalender konfigurieren.
- **Immer ablehnen, wenn das Enddatum hinter diesem Grenzwert liegt:** Diese Einstellung steuert das Verhalten von wiederholten Besprechungen, die durch die Einstellung Maximale buchen Lead angegebenen Datum hinausgehen.
  - Wenn Sie diese Einstellung aktivieren, wird eine Serienbuchungsanfrage automatisch abgelehnt, wenn die Buchung an oder vor dem Datum beginnt, das durch den Wert im Feld **Maximale Vorlaufzeit für Buchungen** angegeben ist, und über das angegebene Datum hinausgeht. Dies ist die Standardeinstellung.
  - Wenn Sie diese Einstellung deaktivieren, wird eine Serienbuchungsanfrage automatisch angenommen, wenn die Buchungsanfrage an oder vor dem Datum beginnt, das durch den Wert im Feld **Maximale Buchungsvorlaufzeit** angegeben ist, und über das angegebene Datum hinausgeht. Allerdings wird die Anzahl von Buchungen reduziert, sodass nach dem angegebenen Datum keine Buchungen möglich sind.
- **Maximum buchen Lead Zeit (in Tagen):** Diese Einstellung gibt die maximale Anzahl der Tage im voraus, die die Ressource gebucht werden kann. Eine gültige Eingabe ist eine ganze Zahl zwischen 0 und 1080. Der Standardwert ist nach 180 Tagen.

- **Maximale Dauer (in Stunden):** Diese Einstellung gibt die maximale Dauer, die die Ressource reserviert werden kann in einer Anforderung buchen an. Der Standardwert ist 24 Stunden.

Bei Serienbuchungsanfragen gilt die maximale Buchungsdauer für die Länge jeder einzelnen Instanz der Serienbuchungsanfrage.

Auf dieser Seite ist auch ein Feld enthalten, in das Sie eine Nachricht eingeben können, die an Benutzer gesendet wird, die Besprechungsanfragen senden, um die Ressource zu reservieren.

#### Kontaktinformationen

Verwenden Sie den Abschnitt **Kontaktinformationen**, um die Kontaktinformationen für die Ressource anzuzeigen oder zu ändern. Die Informationen auf dieser Seite werden im Adressbuch angezeigt.

##### TIP

Sie können das Feld **Bundesland/Kanton** verwenden, um Empfängerbedingungen für dynamische Verteilergruppen, Richtlinien für E-Mail-Adressen oder Adresslisten zu erstellen.

#### E-Mail-Adresse

In dem Abschnitt **E-Mail-Adresse** können Sie die E-Mail-Adressen anzeigen und ändern, die dem Gerätewechsel zugeordnet sind. Dazu gehören die primäre SMTP-Adresse des Postfachs und alle zugehörigen Proxyadressen. Die primäre SMTP-Adresse (auch als Antwortadresse bezeichnet) wird fettgedruckt in der Adressliste angezeigt. Der Wert **SMTP** in der Spalte **Typ** wird dabei in Großbuchstaben angegeben.

- **Hinzufügen:** Klicken Sie auf **Add**  So fügen Sie eine neue e-Mail-Adresse für dieses Postfach hinzu. Wählen Sie eine der folgenden Adresstypen:
  - **SMTP:** Dies ist die Adresse. Klicken Sie auf diese Schaltfläche, und geben Sie dann die neue SMTP-Adresse in der \*\* \* E-Mail-Adresse\*\* Feld.
  - **EUM:** Adresse eines EUM (Exchange Unified Messaging) wird vom Microsoft Exchange Unified Messaging-Dienst verwendet, um die UM-aktivierten Empfänger in einer Exchange-Organisation zu suchen. EUM Adressen bestehen die Durchwahlnummer und die UM-Wähleinstellungen für den UM-aktivierten Benutzer. Klicken Sie auf diese Schaltfläche, und geben Sie im Feld **Adresse/Erweiterung** die Durchwahlnummer ein. Klicken Sie dann auf **Durchsuchen**, und wählen Sie aus einem Wählerplan für das Postfach.
  - **Benutzerdefinierte Adresstyp:** Klicken Sie auf diese Schaltfläche, und geben Sie einen der unterstützten nicht-SMTP-e-Mail-Adresstypen in der \*\* \* E-Mail-Adresse\*\* Feld.

##### NOTE

Mit Ausnahme von X.400-Adressen überprüft Exchange benutzerdefinierte Adressen nicht auf ordnungsgemäße Formatierung. Sie müssen sicherstellen, dass die von Ihnen angegebene benutzerdefinierte Adresse die Formatanforderungen für den jeweiligen Adresstyp erfüllt.

##### NOTE

Wenn Sie eine neue E-Mail-Adresse hinzufügen, können Sie diese als primäre SMTP-Adresse festlegen.

- **E-Mail-Adressen basierend auf der e-Mail-Adressrichtlinie angewendet an diesen Empfänger automatisch aktualisieren:** Aktivieren Sie dieses Kontrollkästchen, um dem Empfänger der e-Mail-Adressen automatisch aktualisierte basierend auf Änderungen an e-Mail-Adressrichtlinien in Ihrer Organisation.

## E-Mail-Info

Verwenden Sie den Abschnitt **E-Mail-Info**, um eine E-Mail-Info hinzuzufügen, in der Benutzer vor möglichen Problemen gewarnt werden, bevor sie eine Buchungsanfrage an das Gerätepostfach senden. Eine E-Mail-Info ist Text, der in der Infoleiste angezeigt wird, wenn dieser Empfänger dem Feld "An", "Cc" oder "Bcc" einer neuen E-Mail hinzugefügt wird.

### NOTE

Eine E-Mail-Info kann HTML-Tags enthalten, Skripts sind jedoch nicht zulässig. Die Länge einer benutzerdefinierten E-Mail-Info darf 175 angezeigte Zeichen nicht überschreiten. HTML-Tags werden bei diesem Zeichenlimit nicht mitgezählt.

## Verwenden von Exchange Online PowerShell, Ändern der gerätepostfacheigenschaften

Verwenden Sie die folgenden Cmdlets, um die Eigenschaften des Gerätepostfachs anzuzeigen oder zu ändern: **Get-Mailbox** und **Set-Mailbox**, um allgemeine Eigenschaften und E-Mail-Adressen für Gerätepostfächer anzuzeigen oder zu ändern. Verwenden Sie die Cmdlets **Get-CalendarProcessing** und **Set-CalendarProcessing**, um Stellvertretungen und Buchungsoptionen anzuzeigen und zu ändern.

- **Get-User** und **Set-User**: Verwenden Sie diese Cmdlets zum Anzeigen und Ändern von allgemeinen Eigenschaften wie abteilungs- und Firmennamen.
- **Get-Mailbox** und **Set-Mailbox**: Verwenden Sie diese Cmdlets zum Anzeigen und Ändern der Eigenschaften von Benutzerpostfächern wie e-Mail-Adressen und die Postfachdatenbank.
- **Get-CalendarProcessing** und **Set-CalendarProcessing**: Verwenden Sie diese Cmdlets anzeigen und Festlegen von Optionen für buchen und Stellvertretungen.

Weitere Informationen über diese Cmdlets finden Sie in den folgenden Themen:

- [Get-User](#)
- [Set-User](#)
- [Get-Mailbox](#)
- [Set-Mailbox](#)
- [Get-CalendarProcessing](#)
- [Set-CalendarProcessing](#)

Hier sind einige Beispiele für die Verwendung von Exchange Online PowerShell gerätepostfacheigenschaften zu ändern.

In diesem Beispiel werden der Anzeigename und die primäre SMTP-Adresse (auch als Standardantwortadresse bezeichnet) für das Gerätepostfach "MotorPool 1" geändert. Die vorherige Antwortadresse wird als Proxyadresse beibehalten.

```
Set-Mailbox "MotorPool 1" -DisplayName "Motor Pool 1 - Compact" -EmailAddresses  
SMTP:MP1.compact@contoso.com,smtp:MP.1@contoso.com
```

In diesem Beispiel werden Gerätepostfächer so konfiguriert, dass sie das Planen von Buchungsanfragen nur während der Arbeitszeiten gestatten.

```
Get-Mailbox -ResultSize unlimited -Filter {((RecipientTypeDetails -eq 'EquipmentMailbox'))} | Set-CalendarProcessing -ScheduleOnlyDuringWorkHours $true
```

In diesem Beispiel wird das Cmdlet **Get-User** verwendet, um alle Gerätepostfächer in der Abteilung "Audio Visual" zu finden. Dann werden mit dem Cmdlet **Set-CalendarProcessing** Buchungsanfragen an eine Stellvertretung namens "Ann Beebe" gesendet, um diese anzunehmen oder abzulehnen.

```
Get-User -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'EquipmentMailbox') -and (Department -eq 'Audio Visual')} | Set-CalendarProcessing -AllBookInPolicy $false -AllRequestInPolicy $true -ResourceDelegates "Ann Beebe"
```

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie die folgenden Schritte aus, um die erfolgreiche Änderung von Gerätepostfacheigenschaften zu überprüfen:

- In der Exchange-Verwaltungskonsole, wählen Sie das Postfach aus, und klicken Sie dann auf **Bearbeiten** [ ] anzeigen, die Eigenschaft oder Funktion, die Sie geändert haben. Je nach der Eigenschaft, die Sie geändert haben, kann es im Bereich Details für das ausgewählte Postfach angezeigt werden.
- Verwenden Sie das Cmdlet **Get-Mailbox** in Exchange Online PowerShell um die Änderungen zu überprüfen. Ein Vorteil von Exchange Online PowerShell ist, dass Sie mehrere Eigenschaften für mehrere Postfächer anzeigen können. Führen Sie den folgenden Befehl zum Überprüfen des neuen Werts im Beispiel oben, in dem buchungsanfragen nur während der Arbeitszeit eingeplant werden konnte.

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'EquipmentMailbox')} | Get-CalendarProcessing | Format-List Identity,ScheduleOnlyDuringWorkHours
```

# Verwalten von Berechtigungen für Empfänger

18.12.2018 • 27 minutes to read

Sie können die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell zum Zuweisen von Berechtigungen zu Benutzern oder Gruppen (als Stellvertreter bezeichnet), mit denen sie zum Öffnen oder Senden von Nachrichten aus anderen Postfächern verwenden. Berechtigungen von Benutzerpostfächern, verknüpfte Postfächer, Ressourcenpostfächer zugewiesen werden können und freigegebene Postfächer. Sie können auch Verteilergruppen, dynamische Verteilergruppen und e-Mail-aktivierte Sicherheitsgruppen zu Delegaten zum Senden von Nachrichten im Namen der Gruppe Berechtigungen zuweisen. Sie können Delegaten weisen die folgenden Berechtigungen auf Postfächer zugreifen oder Senden von Nachrichten im Auftrag von Postfächern oder Gruppen:

- **Vollzugriff:** Diese Berechtigung ermöglicht es einer Stellvertretung zum Öffnen des Postfachs eines Benutzers und Zugreifen auf den Inhalt des Postfachs an. Die Berechtigung Vollzugriff zuweisen kann jedoch nicht die Stellvertretung zum Senden von Nachrichten aus dem Postfach. Sie müssen der Stellvertretung senden als "oder" Senden im Auftrag Berechtigung zum Senden von e-Mail-Nachrichten zuweisen.
- Die Berechtigung "Vollzugriff" steht nicht zur Verfügung, wenn Berechtigungen für Gruppen konfiguriert werden.
- **Senden als:** mit dieser Berechtigung können Delegaten das Postfach zum Senden von Nachrichten verwenden. Nachdem diese Berechtigung Stellvertreter zugewiesen ist, wird jede Nachricht, die aus dem Postfach des Delegaten sendet angezeigt, an den Postfachbesitzer gesendet wurden. Mit dieser Berechtigung kann jedoch keine Stellvertretung das Postfach des Benutzers anmelden. Es kann nur Benutzer das Postfach zu öffnen. Wenn diese Berechtigung zu einer Gruppe zugewiesen ist, erscheint eine Nachricht, durch die Delegaten von der Gruppe gesendet wurden.
- **Senden im Auftrag von:** mit dieser Berechtigung können auch eine Stellvertretung das Postfach zum Senden von Nachrichten verwenden. Nachdem diese Berechtigung Stellvertreter zugewiesen ist, gibt **Absenderadresse in jede Nachricht, die von der Stellvertretung gesendet**, dass die Nachricht vom Delegaten im Namen der Postfachbesitzer gesendet wurde.

## Hinweise:

- Wenn Sie den Vollzugriff senden als zuweisen oder Senden im Auftrag Berechtigung zum Zugriff auf ein Postfach, das ausgeblendet ist in Adresslisten, wird nicht die Stellvertretung möglicherweise öffnen Sie das Postfach oder Senden von Nachrichten.
- Wenn Sie sowohl das Senden als zuweisen und Senden im Auftrag senden im Auftrag wird immer verwendet.

## Was sollten Sie wissen, bevor Sie beginnen?

- Die geschätzte Zeit zum Ausführen der einzelnen Verfahren beträgt 2 Minuten.
- Wenn Berechtigungen für den Zugriff auf ein Postfach ein Benutzer über eine Gruppe erteilt werden, werden nicht das Postfach das Profil des Benutzers automatisch hinzugefügt werden. Der Benutzer muss das Postfach auf das Profil manuell hinzufügen.
- Wenn ein Postfach Outlook mithilfe von Erweiterte Einstellungen hinzugefügt wird, wird nur das primäre Postfach werden hinzugefügt. das Archivpostfach wird nicht hinzugefügt werden. Wenn ein Benutzer auch

das Archivpostfach zugreifen muss, sollte das Postfach in Outlook als zweite Konto in das gleiche Outlook-Profil hinzugefügt werden.

- Für die Verfahren in diesem Thema sind bestimmte Berechtigungen erforderlich. Informationen zu den Berechtigungen finden Sie in den einzelnen Verfahren.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Zuweisen von Berechtigungen zu einem Postfach

Wie bereits zuvor erwähnt können Sie Stellvertretungen Benutzerpostfächer, verknüpfte Postfächer, Ressourcenpostfächer und freigegebene Postfächer zuweisen. Exchange Online PowerShell können Delegaten Zuweisen von Berechtigungen auf ein discoverypostfach zuzugreifen.

Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Berechtigungen und Delegierung" im Abschnitt "Berechtigungen für die Empfängerbereitstellung" im Thema [Recipients Permissions](#).

### Zuweisen von Berechtigungen mithilfe der Exchange-Verwaltungskonsole

Das folgende Verfahren veranschaulicht, wie einem Benutzerpostfach Berechtigungen zugewiesen werden. Das Verfahren zum Zuweisen von Berechtigungen zu Ressourcen- und freigegebenen Postfächern ist ähnlich. Sie navigieren in der Exchange-Verwaltungskonsole zur Seite **Ressourcen** oder **Freigegeben** und wählen das Postfach aus, dem die Berechtigungen zugewiesen werden sollen.

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Klicken Sie in der Liste der Postfächer, klicken Sie auf das Postfach, das Sie Berechtigungen zuweisen möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachstellvertretung**.
4. Klicken Sie auf **Hinzufügen**, um Stellvertretungen Berechtigungen zuzuweisen, wählen Sie die entsprechende Berechtigung zum Anzeigen einer Seite, die alle Empfänger in Ihrer Exchange-Organisation aufgeführt werden, die die Berechtigung zugewiesen werden können. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen**.

Klicken Sie zum Entfernen einer Berechtigung für einen Empfänger, wählen Sie die gewünschte Berechtigung aus, und klicken Sie dann auf **Entfernen**.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

### Massenzuweisung von Berechtigungen mithilfe der Exchange-Verwaltungskonsole

Verwenden Sie die folgenden Schritte für die Massenzuweisung von Berechtigungen

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Wählen Sie die Postfächer aus, denen Sie Berechtigungen zuweisen möchten.
3. Klicken oder tippen Sie auf **Weitere Optionen** im rechten Bereich, und klicken Sie unter **Stellvertretung**

für Postfächer auf Hinzufügen.

4. Klicken Sie auf der Seite **massenhinzufügen Delegierung**, klicken Sie auf, oder tippen Sie auf **Hinzufügen**  wählen Sie die entsprechende Berechtigung zum Anzeigen einer Seite, die alle Empfänger in Ihrer Exchange-Organisation aufgeführt werden, die die Berechtigung zugewiesen werden können. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**.

So entfernen Sie eine Berechtigung für Empfänger, wählen Sie die entsprechende Berechtigung, wählen Sie die Empfänger, und klicken Sie dann auf **Entfernen** .

#### Weisen Sie eine Benutzer die Berechtigung zum Senden von e-Mails aus dem Postfach eines anderen Benutzers mithilfe der Exchange-Verwaltungskonsole

Das folgende Verfahren zeigt, wie eine Benutzer die Berechtigung zum Senden von e-Mails aus dem Postfach eines anderen Benutzers zuweisen.

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Klicken Sie in der Liste der Postfächer, klicken Sie auf das Postfach, das Sie senden als für Berechtigungen zuweisen möchten, und klicken Sie dann auf **Bearbeiten** .
3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachstellvertretung**.
4. Klicken Sie auf **Hinzufügen**, um Stellvertretungen Berechtigungen zuzuweisen,  unter **Senden als** oder **Senden im Auftrag von** einer Seite angezeigt, die alle Empfänger in Ihrer Exchange-Organisation aufgeführt werden, die die Berechtigung zugewiesen werden können. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen** .

Die Berechtigung **Senden als** ermöglicht es der Stellvertretung, Nachrichten von diesem Postfach zu senden.

Die Berechtigung **Senden im Auftrag von** ermöglicht es der Stellvertretung, Nachrichten im Auftrag von diesem Postfach zu senden. Die Zeile **Von** gibt in allen von der Stellvertretung gesendeten Nachrichten an, dass die Nachricht im Auftrag des Postfachbesitzers von der Stellvertretung gesendet wurde.

#### NOTE

Falls der Benutzer außerdem den Inhalt des Postfachs öffnen und anzeigen soll, müssen Sie dem Benutzer die Berechtigung **Vollzugriff** zuweisen.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

#### Zuweisen von Benutzerberechtigungen für das Senden von E-Mails von einer Gruppe mithilfe der Exchange-Verwaltungskonsole

Das folgende Verfahren beschreibt, wie Sie eine Benutzerberechtigung für das Senden von E-Mails von einer Gruppe zuweisen.

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**.
2. Klicken Sie in der Liste der Gruppen, klicken Sie auf die Gruppe, die Sie senden als für Berechtigungen zuweisen möchten, und klicken Sie dann auf **Bearbeiten** .
3. Klicken Sie auf der Eigenschaftenseite der Gruppe auf **Gruppendelegierung**.
4. Klicken Sie auf **Hinzufügen**, um Stellvertretungen Berechtigungen zuzuweisen,  unter **Senden als** oder **Senden im Auftrag von** einer Seite angezeigt, die alle Empfänger in Ihrer Exchange-Organisation aufgeführt werden, die die Berechtigung zugewiesen werden können. Wählen Sie die

Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen**

Die Berechtigung **Senden als** ermöglicht es der Stellvertretung, Nachrichten von dieser Gruppe zu senden.

Die Berechtigung **Senden im Auftrag von** ermöglicht es der Stellvertretung, Nachrichten im Auftrag von dieser Gruppe zu senden. Die Zeile **Von** gibt in allen von der Stellvertretung gesendeten Nachrichten an, dass die Nachricht im Auftrag der Gruppe von der Stellvertretung gesendet wurde.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

#### Zuweisen von Vollzugriffsberechtigungen über die Exchange-Verwaltungskonsole

Das folgende Verfahren veranschaulicht, wie einem Benutzerpostfach Vollzugriffsberechtigungen zugewiesen werden.

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Klicken Sie in der Liste der Postfächer, klicken Sie auf das Postfach, dem Sie Vollzugriffsberechtigungen zuweisen möchten, und klicken Sie dann auf **Bearbeiten**
3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachstellvertretung**.
4. Klicken Sie auf **Hinzufügen**, um Stellvertretungen Berechtigungen zuzuweisen,  unter **Vollzugriff** auf eine Seite angezeigt, die alle Empfänger in Ihrer Exchange-Organisation aufgeführt werden, die die Berechtigung zugewiesen werden können. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen** .

Die Berechtigung **Vollzugriff** ermöglicht es einer Stellvertretung zum Öffnen des Postfachs eines Benutzers und Zugreifen auf den Inhalt des Postfachs an.

#### NOTE

Durch Zuweisen der Berechtigung **Vollzugriff** kann die Stellvertretung jedoch keine E-Mail aus dem Postfach senden. Sie müssen der Stellvertretung die Berechtigung **Senden als** oder **Senden im Auftrag von** zuweisen, damit sie E-Mails senden kann.

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

#### Verwenden von Exchange Online PowerShell Zuweisen von Berechtigungen

In den folgenden Abschnitten wird gezeigt, wie Sie mit Exchange Online PowerShell Vollzugriff senden als verwalten und Senden im Auftrag von Berechtigungen für Postfächer.

#### Verwalten der Berechtigung "Vollzugriff"

Die folgenden Beispiele zeigen, wie Sie mit den Cmdlets **Add-MailboxPermission** und **Remove-MailboxPermission** die Berechtigung "Vollzugriff" verwalten.

Bei diesem Beispiel wird der Stellvertretung Raymond Sam die Berechtigung "Vollzugriff" für das Postfach von Terry Adams zugewiesen.

```
Add-MailboxPermission -Identity "Terry Adams" -User raymonds -AccessRights FullAccess -InheritanceType all
```

Bei diesem Beispiel wird Esther Valle die Berechtigung "Vollzugriff" für das Standardpostfach für die Discoverysuche der Organisation zugewiesen.

```
Add-MailboxPermission -Identity "DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-7E09334BB852}" -User estherv  
-AccessRights FullAccess -InheritanceType all
```

Bei diesem Beispiel wird Mitgliedern der Verteilergruppe "Helpdesk" die Berechtigung "Vollzugriff" für das freigegebene Postfach "Helpdesk Tickets" zugewiesen.

```
Add-MailboxPermission "HelpdeskTickets" -User helpdesk -AccessRights FullAccess -InheritanceType all
```

Dieses Beispiel entfernt die Berechtigung "Vollzugriff" Hance Postfach von ayla KOL.

```
Remove-MailboxPermission -Identity ayla -User "Jim Hance" -AccessRights FullAccess -Inheritance
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter den folgenden Themen:

- [Add-MailboxPermission](#)
- [Remove-MailboxPermission](#)

### Verwalten der Berechtigung "Senden als"

Die folgenden Beispiele zeigen, wie Sie senden als Berechtigungen in Exchange Server und Exchange Online zu verwalten. In Exchange müssen Sie die **Add-ADPermission** und **Remove-ADPermission** -Cmdlets verwenden. In Exchange Online müssen Sie die **Add-recipientpermission können** und **Remove-recipientpermission können** Cmdlets verwenden. In beiden Fällen verwenden Sie den *Identity* -Parameter angeben den Namen der das Postfach auf dem die Berechtigung "Senden als" hinzugefügt oder entfernt werden soll und der *Benutzer* oder die *Vertrauensnehmergruppe* -Parameter des Delegaten (beispielsweise Benutzer oder Gruppe) angeben, der werden zugewiesen oder nicht die Berechtigung "Senden als" zugewiesen.

#### TIP

Verwenden Sie das Cmdlet **Get-Recipient**, um die Eigenschaft *Name* für das Postfach und die Stellvertretung abzurufen. Verwenden Sie diese Werte, um die Berechtigung "Senden als" zuzuweisen.

### Exchange Server

Bei diesem Beispiel wird die Berechtigung "Senden als" der Gruppe "Helpdesk" für das freigegebene Postfach "Helpdesk Support Team" zugewiesen.

```
Add-ADPermission -Identity helpdesksupport -User helpdeskgroup -ExtendedRights "Send As"
```

Bei diesem Beispiel wird die Berechtigung "Senden als" der Benutzerin Pilar Pinilla für das Postfach von James Alvord entzogen.

```
Remove-ADPermission -Identity "James Alvord" -User pilarp -ExtendedRights "Send As"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter:

- [Add-ADPermission](#)
- [Remove-ADPermission](#)

### Exchange Online

Bei diesem Beispiel wird die Berechtigung "Senden als" der Gruppe "Printer Support" für das freigegebene Postfach "Contoso Printer Support" zugewiesen.

```
Add-RecipientPermission -Identity "Contoso Printer Support" -Trustee "Printer Support" -AccessRights SendAs
```

Bei diesem Beispiel wird die Berechtigung "Senden als" der Benutzerin Karen Toh für das Postfach von Yan Li entzogen.

```
Remove-RecipientPermission -Identity "Yan Li" -Trustee "Karen Toh" -ExtendedRights SendAs
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter:

- [Add-recipientpermission](#) können
- [Remove-recipientpermission](#) können

### Verwalten der Berechtigung "Senden im Auftrag von"

Die folgenden Beispiele zeigen, wie Sie mit dem Cmdlet **Set-Mailbox** die Berechtigung "Senden im Auftrag von" verwalten.

Bei diesem Beispiel wird der Stellvertretung Holly Holt die Berechtigung "Senden im Auftrag von" für das Postfach von Sean Chai zugewiesen.

```
Set-Mailbox -Identity seanc@contoso.com -GrantSendOnBehalfTo hollyh
```

Bei diesem Beispiel wird die Berechtigung "Senden im Auftrag von" für das freigegebene Postfach "Contoso Executives" der Gruppe "Temporary Executive Assistants" entzogen.

```
Set-Mailbox "Contoso Executives" -GrantSendOnBehalfTo @{remove="tempassistants@contoso.com"}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailbox](#).

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie einen der folgenden Schritte aus, um die erfolgreiche Zuweisung von Berechtigungen zu einem Postfach bzw. einem freigegebenen Postfach zu überprüfen:

- In der Exchange-Verwaltungskonsole:
  1. Navigieren Sie zu **Empfänger > Postfach** oder **Shared**, klicken Sie auf das Postfach, und klicken Sie dann auf **Bearbeiten**.
  2. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachstellvertretung**.
  3. Wenn Sie einem Empfänger Berechtigungen zugewiesen haben, prüfen Sie, ob der Benutzer oder die Gruppe unter der entsprechenden Berechtigung angegeben ist. Wenn Sie Berechtigungen entzogen haben, stellen Sie sicher, dass der Benutzer oder die Gruppe nicht unter der entsprechenden Berechtigung angegeben ist.

– oder –

- Führen Sie einen der folgenden Befehle, je nach der verwalteten Berechtigung, in Exchange Online PowerShell aus.
  - **Vollzugriff**

```
Get-MailboxPermission -Identity <mailbox>
```

Um zu prüfen, ob einer bestimmten Stellvertretung die Berechtigung "Vollzugriff" für ein Postfach zugewiesen ist, führen Sie den folgenden Befehl aus.

```
Get-MailboxPermission -Identity <mailbox> -User <delegate>
```

- **Senden als**

Führen Sie den folgenden Befehl in Exchange Server.

```
Get-ADPermission -Identity <name of mailbox> -User <delegate>
```

Führen Sie in Exchange Online den folgenden Befehl aus.

```
Get-RecipientPermission -Identity <mailbox> -Trustee <delegate>
```

- **Senden im Auftrag von**

```
Get-Mailbox -Identity <mailbox> | Format-List GrantSendOnBehalfTo
```

## Zuweisen von Berechtigungen zu einer Gruppe

Wie bereits erwähnt, können Sie die Berechtigungen "Senden als" und "Senden im Auftrag von" Verteilergruppen, dynamischen Verteilergruppen und für E-Mail aktivierten Sicherheitsgruppen zuweisen, damit Stellvertretungen Nachrichten als Gruppe oder im Auftrag der Gruppe senden können.

Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter der "Verteilergruppen" und "dynamische Verteilergruppen" im Abschnitt "Empfängerbereitstellungsberechtigungen" im Thema [Recipients Permissions](#).

### Zuweisen von Berechtigungen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**.
2. Klicken Sie in der Liste der Gruppen, klicken Sie auf die Gruppe, die Sie Berechtigungen zuweisen möchten, und klicken Sie dann auf **Bearbeiten**
3. Klicken Sie auf der Eigenschaftenseite der Gruppe auf **Gruppendelegierung**.
4. Klicken Sie auf **Hinzufügen**, um Stellvertretungen Berechtigungen zuzuweisen,  wählen Sie die entsprechende Berechtigung zum Anzeigen einer Seite, die eine Liste aller Empfänger in Ihrer Exchange-Organisation anzeigt, die die Berechtigung zugewiesen werden können. Wählen Sie die Empfänger, die Liste hinzufügen, und klicken Sie dann auf **OK**. Sie können auch für einen bestimmten Empfänger suchen, indem Sie den Namen des Empfängers in das Suchfeld eingeben und dann auf **Suchen** .
- Entfernen der Berechtigung für einen Empfänger, wählen Sie die gewünschte Berechtigung aus, und klicken Sie dann auf **Entfernen** .

5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

### Verwenden von Exchange Online PowerShell Zuweisen von Berechtigungen

In den folgenden Abschnitten wird gezeigt, wie Sie mit Exchange Online PowerShell senden als verwalten und Senden im Auftrag von Berechtigungen für Gruppen.

#### Verwalten der Berechtigung "Senden als"

Die folgenden Beispiele zeigen, wie Sie Berechtigungen "Senden als" für Gruppen im Exchange Online zu verwalten. In Exchange Online müssen Sie die **Add-recipientpermission können** und **Remove-recipientpermission können** Cmdlets verwenden. Verwenden Sie den *Identity*-Parameter, geben Sie den Namen der Gruppe auf dem die Berechtigung "Senden als" hinzugefügt oder entfernt werden soll und der *Benutzer* oder die *Vertrauensnehmergruppe*-Parameter, der Stellvertretung (beispielsweise Benutzer oder Gruppe) an, die zugewiesen werden oder nicht die Berechtigung "Senden als" zugewiesen.

**TIP**

Verwenden Sie das Cmdlet **Get-Recipient**, um die Eigenschaft *Name* für die Gruppe und die Stellvertretung abzurufen. Verwenden Sie diese Werte, um die Berechtigung "Senden als" zuzuweisen.

Bei diesem Beispiel wird die Berechtigung "Senden als" der Gruppe "Contoso Admins" für die dynamische Verteilergruppe "Emergency Broadcast Messages" zugewiesen.

```
Add-RecipientPermission -Identity emergencybroadcast@contoso.com -Trustee "Contoso Admins" -AccessRights SendAs
```

Bei diesem Beispiel wird die Berechtigung "Senden als" dem Benutzer Walter Harp für die Sicherheitsgruppe "Printer Resources" entzogen.

```
Remove-RecipientPermission -Identity "Printer Resources" -Trustee walterh@contoso.com ExtendedRights SendAs
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter:

- [Add-recipientpermission können](#)
- [Remove-recipientpermission können](#)

**Verwalten der Berechtigung "Senden im Auftrag von"**

Die folgenden Beispiele zeigen, wie Sie mit den Cmdlets **Set-DistributionGroup** und **Set-DynamicDistributionGroup** die Berechtigung "Senden im Auftrag von" für Gruppen verwalten.

Bei diesem Beispiel wird der Stellvertretung Sara Davis die Berechtigung "Senden im Auftrag von" für die Verteilergruppe "Printer Support" zugewiesen.

```
Set-DistributionGroup -Identity printersupport@contoso.com -GrantSendOnBehalfTo sarad
```

Bei diesem Beispiel wird der Stellvertretung "Administrator" die Berechtigung "Senden im Auftrag von" für die dynamische Verteilergruppe "All Employees" zugewiesen.

```
Set-DynamicDistributionGroup -Identity "All Employees" -GrantSendOnBehalfTo administrator
```

Bei diesem Beispiel wird die Berechtigung "Senden im Auftrag von" für die dynamische Verteilergruppe "All Employees" dem Administrator entzogen.

```
Set-DynamicDistributionGroup "All Employees" -GrantSendOnBehalfTo @{remove="administrator"}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter:

- [Set-DistributionGroup](#)
- [Set-DynamicDistributionGroup](#)

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Führen Sie einen der folgenden Schritte aus, um die erfolgreiche Zuweisung von Berechtigungen zu einer Gruppe zu überprüfen:

In der Exchange-Verwaltungskonsole:

1. Navigieren Sie zu **Empfänger > Gruppen**, klicken Sie auf die Gruppe, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie auf der Eigenschaftenseite der Gruppe auf **Gruppendelegierung**.
3. Wenn Sie einem Empfänger Berechtigungen zugewiesen haben, prüfen Sie, ob der Benutzer oder die Gruppe unter der entsprechenden Berechtigung angegeben ist. Wenn Sie Berechtigungen entzogen haben, stellen Sie sicher, dass der Benutzer oder die Gruppe nicht unter der entsprechenden Berechtigung angegeben ist.

Führen Sie einen der folgenden Befehle je nach der Berechtigung verwalteten, in Exchange Online PowerShell aus.

- **Senden als**

```
Get-RecipientPermission -Identity <group> -Trustee <delegate>
```

- **Senden im Auftrag von**

```
Get-DistributionGroup -Identity <group> | Format-List GrantSendOnBehalfTo
```

– oder –

```
Get-DynamicDistributionGroup -Identity <group> | Format-List GrantSendOnBehalfTo
```

# Verwalten der Facebook-Kontaktsynchronisierung in Ihrer Organisation

18.12.2018 • 3 minutes to read

Kontakt Facebook-Synchronisierung kann Personen, die eine Verbindung zwischen ihren Facebook-Konto und ihr Office 365-Konto mithilfe von Outlook Web App eingerichtet. Nachdem sie eine Facebook-Verbindung eingerichtet haben, werden ihre Facebook-Freunde als Kontakte in Personen in Office 365 aufgelistet. Sie können klicken Sie dann für Freunde Facebook interagieren, wie ihre Kontakte. Facebook-kontaktsynchronisierung ist standardmäßig aktiviert, wenn das Feature in Ihrer Region verfügbar ist.

## TIP

Als Administrator möchten Sie wahrscheinlich auch behalten Facebook-kontaktsynchronisierung aktiviert, wenn Ihre Organisation geschäftlich, wie Netzwerk und marketing Facebook verwendet. Schalten Sie ihn aus, wenn Sie nicht, dass Ihre Benutzer ihre Facebook-Freunde als Kontakte in Outlook Web App heruntergeladen möchten. Erhalten Sie Informationen zu Personen wie richte Facebook ein Sync, finden Sie unter [Hinzufügen von Facebook Freunde als Kontakte](#).

## NOTE

Die für Ihre Office 365-Organisation verfügbaren Features richten sich nach dem Serviceplan für Ihr Konto. Einige Features sind für Postfächer oder Organisationen in bestimmten Regionen nicht verfügbar.

## Aktivieren oder Deaktivieren der Facebook-Kontaktsynchronisierung

Sie aktivieren mithilfe von Outlook Web App-Einstellungen für Postfachrichtlinien Facebook – Kontakte synchronisieren aktiviert oder deaktiviert für Benutzer in Ihrer Organisation. Ähnlich wie bei anderen postfachrichtlinieneinstellungen für Outlook Web App, können Sie die Einstellungen für Facebook – Kontakte synchronisieren ändern mithilfe der Exchange-Verwaltungskonsole (EAC) oder Exchange Online PowerShell. Ausführliche Informationen zum Verwalten von Outlook Web App-Einstellungen für Postfachrichtlinien, finden Sie unter [anzeigen oder Konfigurieren der Eigenschaften für Outlook Web App-Postfachrichtlinie](#).

## Weitere Informationen

Die Informationen für jede Facebook Friend wird als nur-Lese-Kontakt Datensatz im Personen Facebook-Ordner gespeichert. Die Informationen, die zwischen Facebook und Outlook Web App synchronisiert ist enthält Vorname, Nachname, alle Rufnummern, alle e-Mail-Adressen und alle Adressen. Facebook-Kontakte werden im Postfach des Benutzers gespeichert und werden gemäß der Vereinbarung zum Office 365 beibehalten.

Während der Einrichtung des Outlook Web App und Facebook-Verbindung werden die Kontakte des Benutzers Standardordner Kontakte auf Facebook als Teil einer einmaligen Synchronisation mit Facebook hochgeladen. Facebook verwendet diese Kontaktinformationen als Teil der "Personen möglicherweise wissen" Friend Vorschläge auf Facebook. Einmalige Hochladen von Informationen kann auch die Informationen für Ihre Benutzer Outlook Web App-Kontakte in Facebook-Anwendung bereit, die Ihre Benutzer auswählen können, beispielsweise Mobiltelefon Applications Facebook.

Informationen dazu, wie Ihre Benutzer eine Verbindung mit Facebook einrichten können mit einer desktop-Version von Outlook finden Sie unter [Für Microsoft Outlook Connector für soziale Netzwerke](#).

# LinkedIn-kontaktsynchronisierung in Ihrer Organisation verwalten

18.12.2018 • 3 minutes to read

Kontakt LinkedIn-Synchronisierung kann Personen, die eine Verbindung zwischen ihrem LinkedIn-Konto und ihr Office 365-Konto mithilfe von Outlook Web App eingerichtet. Nachdem sie LinkedIn-kontaktsynchronisierung eingerichtet haben, werden alle ihre LinkedIn-Verbindungen als Kontakte in Personen in Office 365 aufgelistet. Sie können die LinkedIn-Verbindungen Interaktion mit wie für andere Kontakte. LinkedIn-kontaktsynchronisierung ist standardmäßig aktiviert, wenn das Feature für Ihre Region verfügbar ist.

## TIP

Als Administrator möchten Sie wahrscheinlich auch behalten LinkedIn-kontaktsynchronisierung aktiviert, wenn Ihre Organisation LinkedIn geschäftlich, wie Netzwerk und "Marketing" verwendet. Schalten Sie ihn aus, wenn Sie nicht, dass Ihre Benutzer die LinkedIn-Verbindungen mit den Kontakten in Outlook Web App heruntergeladen möchten. Weitere Informationen dazu, wie LinkedIn Personen einrichten können kontaktsynchronisierung, finden Sie unter [Verwaltete LinkedIn Sync in Ihrer Organisation wenden Sie sich an](#).

## NOTE

Die für Ihre Office 365-Organisation verfügbaren Features richten sich nach dem Serviceplan für Ihr Konto. Einige Features sind für Postfächer oder Organisationen in bestimmten Regionen nicht verfügbar.

## Aktivieren oder Deaktivieren der LinkedIn-Kontaktsynchronisierung

Sie aktivieren mithilfe von Outlook Web App-Einstellungen für Postfachrichtlinien LinkedIn – Kontakte synchronisieren aktiviert oder deaktiviert für Benutzer in Ihrer Organisation. Ähnlich wie bei anderen postfachrichtlinieneinstellungen für Outlook Web App, können Sie die Einstellungen für LinkedIn-kontaktsynchronisierung ändern mithilfe der Exchange-Verwaltungskonsole (EAC) oder Exchange Online PowerShell. Ausführliche Informationen zum Verwalten von Outlook Web App-Einstellungen für Postfachrichtlinien, finden Sie unter [anzeigen oder Konfigurieren der Eigenschaften für Outlook Web App-Postfachrichtlinie](#).

## Weitere Informationen

Die Informationen für jeden LinkedIn-Kontakt wird als nur-Lese-Kontakt Datensatz im Personen LinkedIn-Ordner gespeichert. Die Informationen, die zwischen LinkedIn und Outlook Web App synchronisiert ist enthält Vorname, Nachname, alle Rufnummern, alle e-Mail-Adressen und alle Adressen. LinkedIn-Kontakte werden im Postfach des Benutzers gespeichert und werden gemäß der Office 365-Dienstplan beibehalten. Informationen dazu, wie die Benutzer eine Verbindung mit LinkedIn einrichten können mit einer desktop-Version von Outlook haben sie das Auschecken [Für Microsoft Outlook Connector für soziale Netzwerke](#).

# Konfigurieren eines moderierten Empfängers in Exchange Online

18.12.2018 • 6 minutes to read

In Ihrer Exchange Online-Organisation kann es erforderlich sein, den Zugriff auf bestimmte Empfänger einzuschränken. Die ist besonders dann der Fall, wenn die an große Verteilergruppen gesendeten Nachrichten gesteuert werden müssen. Abhängig von den Anforderungen Ihrer Organisation müssen Sie möglicherweise auch die Nachrichten steuern, die an Postfächer von hochrangigen Führungskräften oder an Partnerkontakte gesendet werden. Diese Aufgaben können mit moderierten Empfängern ausgeführt werden. Wenn Sie einen Empfänger für die Moderation konfigurieren, müssen alle Nachrichten, die an diesen Empfänger gesendet werden, von den angegebenen Moderatoren genehmigt werden.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 15 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Moderierter Transport" im Thema [Transport Permissions](#).
- Eine Verteilergruppe für die Moderation können Sie in der Exchange-Verwaltungskonsole konfigurieren. Alle anderen Empfängertypen können für die Moderation nur mit PowerShell konfiguriert werden. Wie Sie mit Windows PowerShell eine Verbindung mit Exchange Online herstellen, können Sie unter [Herstellen einer Verbindung mit Exchange Online PowerShell](#) nachlesen.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Was möchten Sie machen?

### Erstellen einer Verteilergruppe für die Moderation mithilfe der Exchange-Verwaltungskonsole

In diesem Beispiel werden die folgenden Moderationseinstellungen für die Verteilergruppe "All Employees" konfiguriert:

- Moderation für die Verteilergruppe aktivieren.
- David Hamilton und Yossi Ran als Moderatoren festlegen.
- Den Mitgliedern der Verteilergruppe "Personalabteilung" ermöglichen, die Moderation zu umgehen.
- Interne Absender benachrichtigen, wenn ihre Nachricht an die Verteilergruppe abgelehnt wird, aber keine Benachrichtigungen an externe Absender senden.

Führen Sie das folgende Verfahren aus, um die Aufgaben in diesem Beispielszenario abzuschließen:

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Gruppen**.

2. Klicken Sie im Ergebnisbereich die Verteilergruppe **alle Mitarbeiter** auszuwählen, und klicken Sie auf **Bearbeiten**
3. Klicken Sie auf der Eigenschaftenseite auf **Nachrichtengenehmigung**, und führen Sie die folgenden Schritte aus:
4. Aktivieren Sie das Kontrollkästchen **An diese Gruppe gesendete Nachrichten müssen von einem Moderator genehmigt werden.**
5. Klicken Sie auf **Hinzufügen**, in der Liste **gruppenmoderatoren** .
6. Suchen Sie im Dialogfeld **Gruppenmoderatoren auswählen** den Benutzer "David Hamilton", markieren Sie ihn, und klicken Sie auf **Hinzufügen**. Suchen Sie anschließend nach "Yossi Ran", markieren Sie den Benutzer, und klicken Sie auf **Hinzufügen**. Klicken Sie nach Abschluss des Vorgangs auf **OK**.
7. Klicken Sie auf **Hinzufügen**, in der Liste **Absender, die nachrichtengenehmigung erfordern keinen** .
8. Wählen Sie im Dialogfeld **Absender auswählen** "HR" in der Liste aus, und klicken Sie dann auf **Hinzufügen**. Klicken Sie nach Abschluss des Vorgangs auf **OK**.
9. Aktivieren Sie im Bereich **Moderationsbenachrichtigungen auswählen** die Option **Alle Absender bei Nichtgenehmigung ihrer Nachrichten benachrichtigen.**
10. Klicken Sie auf **Speichern**.

#### **Verwenden von Exchange Online PowerShell so konfigurieren Sie einen moderierten Empfänger**

Führen Sie den folgenden Befehl aus:

```
Set-<RecipientType> <Identity> -ModerationEnabled $true -ModeratedBy <recipient1,recipient2...> -  
ByPassModerationFromSendersOrMembers <recipient1,recipient2...> -SendModerationNotifications <Never | Always |  
Internal>
```

In diesem Beispiel werden die folgenden Moderationseinstellungen für die Verteilergruppe "All Employees" konfiguriert:

- Moderation für die Verteilergruppe aktivieren.
- David Hamilton und Yossi Ran als Moderatoren festfestlegen.
- Den Mitgliedern der Verteilergruppe "Personalabteilung" ermöglichen, die Moderation zu umgehen.
- Interne Absender benachrichtigen, wenn ihre Nachricht an die Verteilergruppe abgelehnt wird, aber keine Benachrichtigungen an externe Absender senden.

Führen Sie den folgenden Befehl aus, um die Aufgaben in diesem Beispieldaten abzuschließen:

```
Set-DistributionGroup "All Employees" -ModerationEnabled $true -ModeratedBy "David Hamilton","Yossi Ran" -  
ByPassModerationFromSendersOrMembers HR -SendModerationNotifications Internal
```

Verwenden Sie die folgende Syntax, um Benutzer oder Empfänger zur Liste der Moderatoren mit Umgehung der Moderation hinzuzufügen oder aus dieser zu entfernen, ohne dass dies auf andere Einträge auswirkt:

```
Set-<RecipientType> <Identity> -ModeratedBy @{@Add="<>recipient1>","<recipient2>"...; Remove="<recipient1>","  
<recipient2>"...} -ByPassModerationFromSendersOrMembers @{@Add="<>recipient1>","<recipient2>"...; Remove="<  
recipient1>","<recipient2>"...}
```

In diesem Beispiel werden die folgenden Moderationseinstellungen für die Verteilergruppe "All Employees" konfiguriert:

- Fügen Sie den Benutzer "chris@contoso.com" der Liste der vorhandenen Moderatoren hinzu.
- Entfernen Sie die Benutzerin "michelle@contoso.com" aus der Liste der vorhandenen Absender, die die Moderation umgehen.

```
Set-DistributionGroup "All Employees" -ModeratedBy @{Add="chris@contoso.com"} -  
ByPassModerationFromSendersOrMembers @{Remove="michelle@contoso.com"}
```

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie folgendermaßen vor, um sicherzustellen, dass ein Empfänger erfolgreich für die Moderation konfiguriert wurde:

1. Senden Sie eine Testnachricht an den moderierten Empfänger.
2. Vergewissern Sie sich, dass die festgelegten Moderatoren eine Benachrichtigung erhalten.
3. Überprüfen Sie, ob Empfänger mit Umgehung der Moderation die Nachricht direkt erhalten.

# Methoden zum Migrieren mehrerer E-Mail-Konten zu Office 365

18.12.2018 • 7 minutes to read

□ Ihre Organisation kann E-Mails aus anderen Systemen zu Office 365 migrieren. Ihre Administratoren können [Migrieren von Postfächern aus Exchange Server](#) migrieren oder [Migrieren von E-Mails aus einem anderen IMAP-fähigen E-Mail-System](#). Und die Benutzer können ihre eigenen E-Mails, Kontakte und sonstigen Postfachinformationen in ein für sie erstelltes Office 365-Postfach [Veranlassen, dass Benutzer ihre eigenen E-Mails importieren](#). Ihre Organisation kann darüber hinaus [Arbeiten mit einem Partner, um E-Mails zu migrieren](#), um E-Mails zu migrieren.

Bevor Sie mit einer E-Mail-Migration beginnen, sollten Sie [Begrenzungen](#) und [bewährte Methoden](#) für Exchange Online lesen, damit sichergestellt ist, dass Sie nach der Migration die erwartete Leistung und das erwartete Verhalten bekommen.

Unterstützung bei der Auswahl der besten Option für Ihre Organisation finden Sie unter [Auswählen eines Migrationspfads](#) oder unter [Exchange-Migrationsratgeber](#).

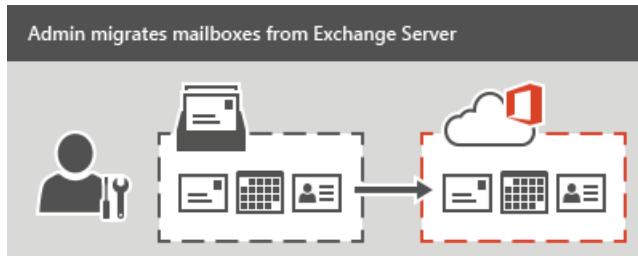
## TIP

Eine weitere Option zur Erleichterung der e-Mail-Migration ist [Der schnelle Center Vorteil für Office 365](#). Schnelle Spezialisten helfen Ihnen beim Planen und Ausführen der Migrations. Weitere Informationen finden Sie unter [Datenmigration](#).

Sie können auch ein Übersichtsvideo anzeigen:

## Migrieren von Postfächern aus Exchange Server

Für Migrationen aus einer vorhandenen lokalen Exchange Server-Umgebung kann ein Administrator alle E-Mails, Kalenderinformationen und Kontakte aus Benutzerpostfächern zu Office 365 migrieren.



Es gibt drei Methoden zum Migrieren von E-Mails aus Exchange Server:

- **Migrieren aller Postfächer in einem Schritt (Übernahmemigration) oder Expressmigration**

Verwenden Sie diese Migrationsmethode, wenn Sie mit Exchange 2003, Exchange 2007, Exchange Server 2010 oder Exchange 2013 arbeiten und weniger als 2.000 Postfächer vorhanden sind. Sie können eine Übernahmemigration durch Starten aus dem Exchange Admin Center (EAC) durchführen. Lesen Sie dazu [Durchführen einer Übernahmemigration zu Office 365](#). Informationen zur Expressmigration finden Sie unter [Verwenden der Expressmigration zum Migrieren von Exchange-Postfächern zu Office 365](#).

#### **IMPORTANT**

Mit der Übernahmemigration können Sie bis zu 2.000 Postfächer verschieben. Angesichts der langen Zeit, die das Erstellen und Migrieren von 2.000 Benutzern dauert, ist es jedoch sinnvoller, maximal 150 Benutzer zu migrieren.

- **Migrieren von Postfächern in Batches (mehrstufige Migration)**

Verwenden Sie diese Migrationsmethode, wenn Sie mit Exchange 2003 oder Exchange 2007 arbeiten und mehr als 2.000 Postfächer vorhanden sind. Einen Überblick über eine mehrstufige Migration finden Sie unter [Wichtige Informationen zur mehrstufigen E-Mail-Migration zu Office 365](#). Informationen zum Ausführen der Migrationsaufgaben finden Sie unter [Ausführen einer mehrstufigen Migration von Exchange Server 2003 und Exchange 2007 zu Office 365](#).

- **Migrieren mit einer integrierten Exchange Server- und Office 365-Umgebung (hybride Umgebung)**

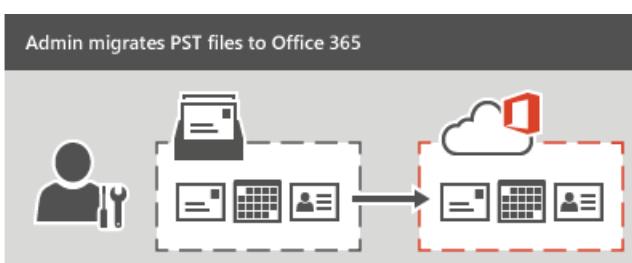
Verwenden Sie diese Migrationsmethode, wenn Sie sowohl die lokalen als auch die Online-Postfächer für Ihre Organisation behalten und Benutzer sowie E-Mails schrittweise zu Office 365 migrieren möchten. Verwenden Sie diese Migrationsmethode, wenn Folgendes zutrifft:

- Sie arbeiten mit Exchange Server 2010, und es gibt mehr als 150-2.000 Postfächer.
- Sie arbeiten mit Exchange Server 2010 und möchten die Postfächer nach und nach in kleinen Batches migrieren.
- Sie arbeiten mit Exchange 2013.

Weitere Informationen hierzu finden Sie unter [Planen einer Exchange Online-Hybridbereitstellung in Office 365](#).

## Verwenden des Office 365-Importdiensts zum Migrieren von PST-Dateien

Wenn Ihre Organisation über viele große PST-Dateien verfügt, können Sie den Office 365-Importdienst nutzen, um E-Mail-Daten zu Office 365 migrieren.



Mithilfe des Office 365-Importdiensts können Sie die PST-Dateien entweder über ein Netzwerk hochladen oder sie auf einem von Ihnen vorbereiteten Laufwerk senden (Laufwerkversand).

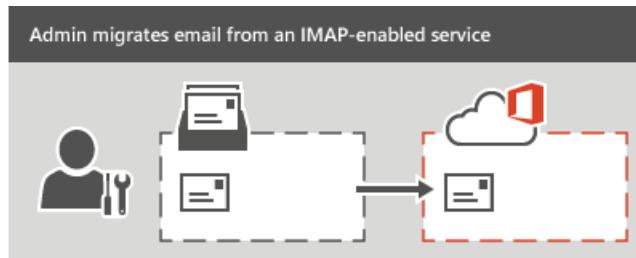
Entsprechende Anweisungen finden Sie unter [Office 365-Importdienst](#).

## Migrieren von E-Mails aus einem anderen IMAP-fähigen E-Mail-System

Sie können auch IMAP (Internet Message Access Protocol) verwenden, um Benutzer-E-Mails aus Gmail-, Exchange-, Outlook.com- und anderen E-Mail-Systemen zu migrieren, die IMAP-Migration unterstützen. Wenn Sie die E-Mails eines Benutzers mithilfe der IMAP-Migration migrieren, werden nur die Elemente aus dem Posteingang oder aus anderen E-Mail-Ordnern des Benutzers migriert. Kontakte, Kalenderelemente und

Aufgaben können mit IMAP nicht migriert werden, doch können sie von einem Benutzer migriert werden.

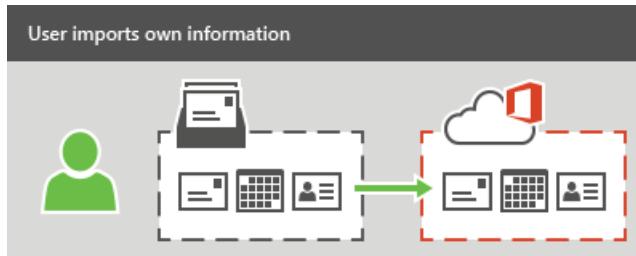
Außerdem werden bei einer IMAP-Migration keine Postfächer in Office 365 erstellt. Sie müssen vor dem Migrieren der E-Mails ein Postfach für jeden Benutzer erstellen.



Informationen, wie E-Mails aus einem anderen E-Mail-System migriert werden, finden Sie unter [Migrieren von IMAP-Postfächern zu Office 365](#). Nachdem die E-Mail-Migration abgeschlossen ist, werden neue E-Mails, die an die Quell-E-Mail-Adresse gesendet wurden, nicht migriert.

## Veranlassen, dass Benutzer ihre eigenen E-Mails importieren

Benutzer können ihre eigenen e-Mail, Kontakte und andere Postfachinformationen zu Office 365 importieren. Finden Sie unter [Migrate e-Mails und Kontakte zu Office 365](#) Hier erfahren, wie.



## Arbeiten mit einem Partner, um E-Mails zu migrieren

Ist keine der beschriebenen Migrationsmethode für Ihre Organisation geeignet, besteht die Möglichkeit, E-Mails mithilfe eines Partners zu Office 365 zu migrieren.

METHODE	BESCHREIBUNG
 Use a third-party migration tool	<b>Verwenden eines E-Mail-Migrationstools eines Drittanbieters</b> Mit Migrationstools lässt sich eine E-Mail-Migration beschleunigen und vereinfachen. Eine Liste entsprechender Tools finden Sie in <a href="#">Office 365 Marketplace</a> .
 Hire a partner	<b>Beauftragen eines Partners, Sie beim Migrieren Ihrer E-Mails zu unterstützen</b> Eine Liste von Partnern finden Sie in <a href="#">Office 365 Marketplace</a> .

## Verwandte Themen

[Verwenden von PowerShell für die E-Mail-Migration zu Office 365](#)

# Auswählen eines Migrationspfads

18.12.2018 • 10 minutes to read

Die Auswahl des besten Migrationspfads für das E-Mail-System Ihrer Benutzer zu Office 365 kann eine schwierige Entscheidung sein. Dieser Artikel bietet eine Entscheidungshilfe basierend auf Ihrem aktuellen E-Mail-System und anderen Faktoren, beispielsweise wie schnell Sie zu Office 365 migrieren möchten. Die Migrationsleistung variiert je nach Netzwerk, Postfachgröße, Migrationsgeschwindigkeit und so weiter.

## IMPORTANT

In diesem Thema wird für Office 365 globale Administratoren vorgesehen. Wenn Sie e-Mails für ein einziges Konto migrieren möchten, finden Sie stattdessen unter [Migrate e-Mails und Kontakte zu Office 365](#).

## Wie entscheide ich, welche Methode verwendet werden soll?

Bevor Sie mit einer E-Mail-Migration beginnen, sollten Sie sich über die [Begrenzungen](#) sowie über die [Office 365-Migrationsleistung und bewährte Methoden](#) für Exchange Online informieren, um sicherzustellen, dass Sie nach der Migration die erwartete Leistung und das erwartete Verhalten bekommen.

Als globaler Office 365-Administrator können Sie Postfächer von einem [Exchange-Server](#) oder [von einem anderen E-Mail-System](#) migrieren. Der Inhalt in den folgenden Abschnitten ist nach E-Mail-System organisiert, und mithilfe der verknüpften Themen, können Sie die beste Methode basierend auf der Anzahl der Postfächer, Ihren zeitlichen Beschränkungen und den Größenbeschränkungen für Postfächer ermitteln.

## Ihr vorhandenes System ist ein Exchange-Server

Bei Migrationen von einer vorhandenen lokalen Exchange Server-Umgebung können Sie alle E-Mails, Kalenderelemente, Aufgaben und Kontakte aus Benutzerpostfächern zu Office 365 migrieren. Bei den verfügbaren Methoden handelt es sich um [Übernahme-](#), [mehrstufige](#) und [hybride Exchange](#)-Migrationen. Bei diesen Migrationsmethoden werden alle E-Mail-Daten einschließlich aller Kontakte, Kalenderelemente und Aufgaben kopiert. Sie können auch die [IMAP](#)-Migration (Internet Message Access Protocol) von Exchange-Servern verwenden, und wenn Ihre Version älter als Exchange 2003 ist, stellt die IMAP-Migration die einzige Option dar. Beachten Sie, dass bei der IMAP-Migration nur E-Mail-Daten kopiert werden.

## IMPORTANT

Bei mehrstufigen und hybriden Exchange-Migrationen müssen Sie auch die Verzeichnissynchronisierung einrichten. Weitere Informationen finden Sie unter [Office 365-Integration in lokale Umgebungen](#).

Wenn Sie Migrationsempfehlungen erhalten möchten, erweitern Sie je nach verwendetem Quellsystem einen der folgenden Abschnitte:

## Exchange 2003 oder Exchange 2007

Wenn Ihr Quellsystem Exchange 2003 oder Exchange 2007 ist, ziehen Sie die folgenden Optionen in Betracht.

**NOTE**

Obwohl bei einer Übernahmemigration bis zu 2.000 Postfächer verschoben werden können, ist es angesichts der langen Zeit, die das Erstellen und Migrieren von 2.000 Benutzern dauert, sinnvoller, maximal 150 Benutzer zu migrieren.

ANZAHL DER POSTFÄCHER	WIE SCHNELL MÖCHTEN SIE MIGRIEREN?	VERWENDUNG
Weniger als 150	Im Verlauf eines Wochenendes oder innerhalb von ein paar Tagen	<b>Übernahmemigration</b> Eine Übersicht finden Sie unter <a href="#">Wichtige Informationen zur E-Mail-Übernahmemigration zu Office 365</a> .
Weniger als 150	Langsam, indem nur ein paar Benutzer gleichzeitig migriert werden	<b>Mehrstufige Migration</b> Eine Übersicht finden Sie unter <a href="#">Wichtige Informationen zur mehrstufigen E-Mail-Migration zu Office 365</a> .
Über 150	Im Verlauf eines Wochenendes oder innerhalb von ein paar Tagen	<b>Mehrstufige Migration</b> Wenn Sie über mehr als 150 Postfächer verfügen, stellt die mehrstufige Migration die beste Methode dar, bei der Sie eine begrenzte Anzahl von Benutzern gleichzeitig migrieren können. Bei der Übernahmemigration kommt es zu Leistungseinbußen, wenn Sie versuchen, mehr als 150 Postfächer zu migrieren.
Über 150	Langsam, indem nur ein paar Benutzer gleichzeitig migriert werden	<b>Mehrstufige Migration</b>

Wenn die zu migrierenden Postfächer große Datenmengen enthalten, können Sie auch den [Office 365-Importdienst](#) verwenden, um PST-Dateien in Office 365 zu importieren. Sie können den Office 365-Importdienst verwenden, um die Dateien entweder (auf einem Datenträger) postalisch zu verschicken oder über das Netzwerk zu importieren.

Wenn Sie über eine sehr große Anzahl von Postfächern (über 5.000) verfügen, möchten Sie möglicherweise einen Partner beauftragen, Sie bei der Migration Ihrer E-Mail-Daten zu unterstützen.

Eine Liste von Partnern finden Sie im [Microsoft Partner Center](#).

## Exchange 2010, 2013 oder 2016

Wenn Ihr Quellsystem Exchange Server 2010, Exchange 2013 oder Exchange Server 2016 ist, ziehen Sie die folgenden Optionen in Betracht.

**NOTE**

Obwohl bei einer Übernahmemigration bis zu 2.000 Postfächer verschoben werden können, ist es angesichts der langen Zeit, die das Erstellen und Migrieren von 2.000 Benutzern dauert, sinnvoller, maximal 150 Benutzer zu migrieren.

ANZAHL DER POSTFÄCHER	WIE SCHNELL MÖCHTEN SIE MIGRIEREN?	VERWENDUNG
Weniger als 150	Im Verlauf eines Wochenendes oder innerhalb von ein paar Tagen	<b>Übernahmemigration</b> oder <b>Expressmigration</b> .

ANZAHL DER POSTFÄCHER	WIE SCHNELL MÖCHTEN SIE MIGRIEREN?	VERWENDUNG
Weniger als 150	Langsam, indem nur ein paar Benutzer gleichzeitig migriert werden	<a href="#">Exchange Hybrid</a>
Über 150	Im Verlauf eines Wochenendes oder innerhalb von ein paar Tagen	<a href="#">Exchange Hybrid</a> Wenn Sie über mehr als 150 Postfächer verfügen, stellt eine hybride Exchange-Migration die beste Methode dar, bei der Sie eine begrenzte Anzahl von Benutzern gleichzeitig migrieren können. Bei der Übernahmemigration kommt es zu Leistungseinbußen, wenn Sie versuchen, mehr als 150 Postfächer zu migrieren.
Über 150	Langsam, indem nur ein paar Benutzer gleichzeitig migriert werden	<a href="#">Exchange Hybrid</a>

Wenn die zu migrierenden Postfächer große Datenmengen enthalten, können Sie auch den [Office 365-Importdienst](#) verwenden, um PST-Dateien in Office 365 zu importieren. Sie können den Office 365-Importdienst verwenden, um die Dateien entweder (auf einem Datenträger) postalisch zu verschicken oder über das Netzwerk zu importieren.

Wenn Sie über eine sehr große Anzahl von Postfächern (über 5.000) verfügen, möchten Sie möglicherweise einen Partner beauftragen, Sie bei der Migration Ihrer E-Mail-Daten zu unterstützen.

Eine Liste von Partnern finden Sie im [Microsoft Partner Center](#).

## Exchange Server 2000 oder frühere Versionen

Bei früheren Versionen von Exchange Server müssen Sie die [IMAP-Migration](#) verwenden.

## Andere E-Mail-Systeme

Bei anderen E-Mail-Systemen, die IMAP unterstützen, können Sie [IMAP-Migrationen](#) verwenden.

Lesen Sie abhängig von Ihrem Quellsystem einen der folgenden Artikel:

- [Migrieren von G Suite-Postfächern zu Office 365](#)
- [Migrieren anderer Typen von IMAP-Postfächern zu Office 365](#)

Dieses Thema enthält Anweisungen für die Migration von CSV-Dateien für Exchange, Mirapoint, Dovecoat und Courier IMAP.

- [IMAP-Migration im Office 365 Admin Center](#)

Wenn die zu migrierenden Postfächer große Datenmengen enthalten, können Sie auch den [Office 365-Importdienst](#) verwenden, um PST-Dateien in Office 365 zu importieren. Sie können den Office 365-Importdienst verwenden, um die Dateien entweder (auf einem Datenträger) postalisch zu verschicken oder über das Netzwerk zu importieren.

Sie können auch einen Partner beauftragen, Sie bei der Migration Ihrer E-Mail-Daten zu unterstützen. Eine Liste von Partnern finden Sie im [Microsoft Partner Center](#).

## Bitte geben Sie uns Feedback

Waren diese Anleitungen hilfreich? Wenn das der Fall ist, lassen Sie uns dies bitte am Ende des Themas wissen. Wenn dies nicht der Fall war, und Sie immer noch Probleme haben, sich für eine Migrationsstrategie zu entscheiden, teilen Sie uns das Quell-E-Mail-System mit, von dem Sie migrieren möchten, und wir verwenden Ihr Feedback, um unsere Inhalte zu verbessern.

# Verwenden Sie die minimale Hybrid schnell Migration von Exchange-Postfächern zu Office 365

18.12.2018 • 9 minutes to read

Sie können das minimale Hybrid verwenden, auch bekannt als express Migration, Option in Exchange Hybrid Configuration Wizard zum Migrieren des Inhalts von Benutzerpostfächern zu Office 365 einen Verlauf einer Reihe von Wochen oder weniger.

## Voraussetzungen

E-Mails mit minimaler Hybrid migrieren, wenn Sie:

- Mindestens eine Exchange 2010, Exchange 2013 und/oder 2016 Exchange Server lokal ausführen.
- Planen Sie einen Verlauf von einigen Wochen oder weniger zu Exchange Online verschieben.
- Nicht planen Sie, weiterhin Directory-Synchronisierung zum Verwalten von Ihren Benutzern ausgeführt werden.

## Schritt 1: Stellen Sie sicher, dass Sie die Domäne besitzen

Während der Migration wird die Adresse Simple Mail Transfer Protocol (SMTP) jedes lokale Postfach verwendet, um die e-Mail-Adresse für eine neue Office 365-Postfach zu erstellen. Um eine Migration von express ausgeführt werden soll, muss die lokale Domäne einer überprüften Domäne in Office 365-Organisation.

1. Melden Sie sich mit Ihrem Geschäfts- oder Schulkonto bei Office 365 an.
2. Wählen Sie **Setup > Domänen**.
3. Klicken Sie auf der Seite **Domänen** - auf \*\* Hinzufügen Domäne \*\* um die Domäne-Assistenten zu starten.  

  4. Geben Sie auf der Seite **Domäne hinzufügen** den Domänennamen (z. B. "contoso.com"), die Sie für Ihre lokale Exchange-Organisation verwenden, und klicken Sie dann auf **Weiter**.
  5. Wählen Sie auf der Seite **Domäne überprüfen** oder (sofern Ihre DNS-Datensätze durch GoDaddy verwaltet werden) **Melden Sie sich bei "GoDaddy" Hinzufügen ein TXT-Eintrags stattdessen** für alle anderen Registrierungsstellen > **Weiter**.
  6. Befolgen Sie die Anweisungen für Ihren DNS-Hostinganbieter bereitgestellt. TXT-Eintrag wird in der Regel ausgewählt, so überprüfen Sie den Besitz.  
Sie können auch die Anweisungen in [Erstellen von DNS-Datensätzen bei jeder DNS-Hostinganbieter für Office 365](#) suchen.  
Nach dem Hinzufügen des txt- oder MX-Eintrags, warten Sie 15 Minuten, ehe Sie mit dem nächsten Schritt fortfahren.
  7. Klicken Sie im Assistenten für Office 365-Domänen **durchgeführt, vergewissern Sie sich nun wählen**, und sehen Sie eine Seite Überprüfung. Wählen Sie auf **Fertig stellen**.

Wenn die Überprüfung, unter fehlschlägt zuerst, warten Sie einen Moment, und versuchen Sie es erneut.

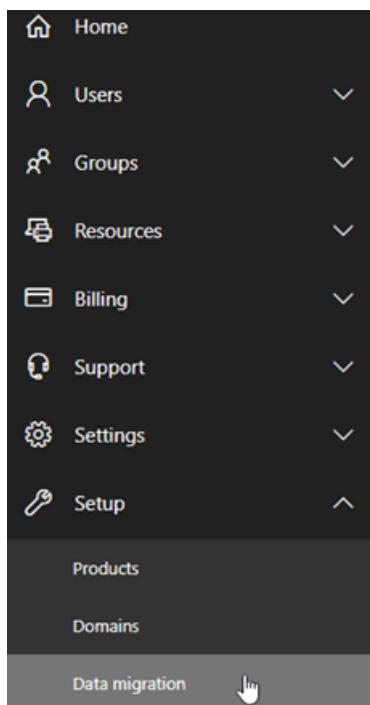
**Führen Sie mit dem nächsten Schritt im Assistenten Domänen nicht fortgesetzt werden.** Sie haben nun sichergestellt, dass Sie die Domäne des lokalen Exchange-Organisation besitzen und bereit sind, eine e-Mail-Migration fortzusetzen.

Einstellung wird die Domäne eingerichtet abgeschlossen werden, wenn die Migration abgeschlossen sind.

## Schritt 2: Express Migration starten

Melden Sie auf einem Computer, der Domäne zu Ihrer lokalen Organisation verbunden ist sich bei Ihrem Office 365-Konto mithilfe Ihrer Anmeldeinformationen globaler Administrator, und starten Sie das Exchange Hybrid Configuration Wizard auf der Seite **Datenmigration** der Office 365-Admin-Seite.

1. Wechseln Sie in der Office 365 Admin Center zu **Setup > Datenmigration**.



2. **Migration** Seite unter **Wählen Sie den Datendienst**, wählen Sie **Exchange** aus.

Select your data service

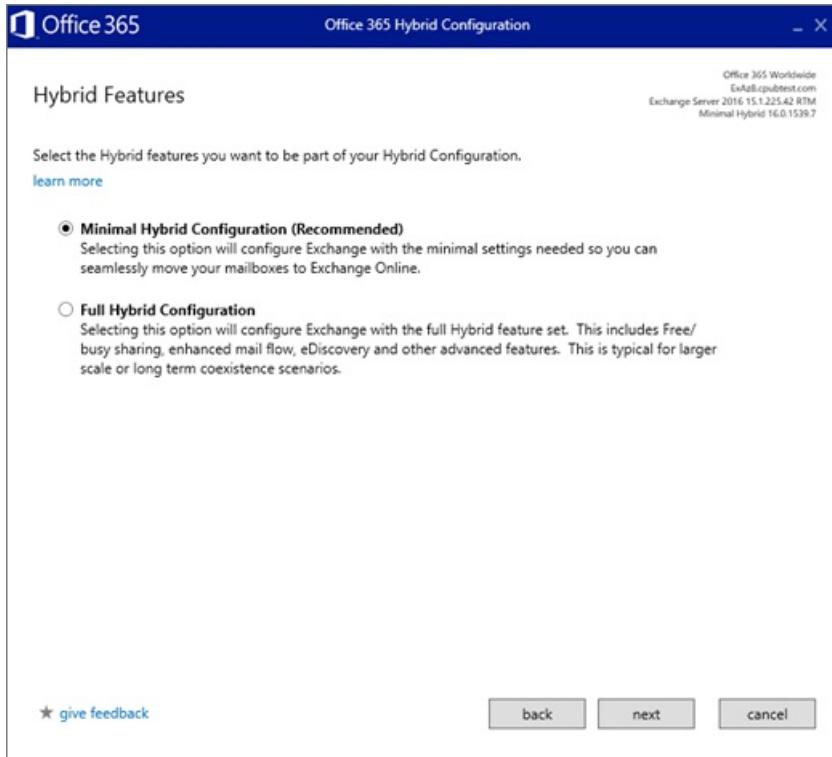
Select the appropriate source where you plan on migrating data from. We will then guide

<a href="#">Upload PST files</a>	<a href="#">Import to OneDrive</a>	 <a href="#">Gmail</a> Important: Before you migrate data, you need to complete a few steps to prepare.
 <a href="#">Yahoo</a>	<a href="#">Other email sources...</a>	 <a href="#">Exchange</a> Use this option if your environment has at least one Exchange 2010, 2013, and/or 2016 server.

3. Wählen Sie auf der ersten Seite der **Hybrid Configuration Wizard Weiter**, und akzeptieren Sie die Standardwerte auf der Seite **Lokale Exchange Server-Organisation**, und klicken auf **Weiter**.

Standardmäßig eine Verbindung mit dem Exchange-Server mit der neuesten Version des Assistenten.

4. Klicken Sie auf der Seite Anmeldeinformationen auswählen, **Verwenden Sie die aktuelle Windows-Anmeldeinformationen** für lokale Exchange-Server, und geben Sie Administratoranmeldeinformationen ein, für sie und Ihre Office 365-Mandanten wählen Sie **Weiter**, und klicken Sie dann auf **Weiter** erneut einmal die Verbindungen und Anmeldeinformationen überprüft haben.
5. Wählen Sie auf der Seite **Hybriden Features Minimale Hybrid Configuration > Weiter**.



6. Wählen Sie auf der Seite **bereit für die Aktualisierung** zur Vorbereitung der Migration der lokalen Postfächer **zu aktualisieren**.

## Schritt 3: Führen Sie zum Erstellen von Benutzern in Office 365 Directory-Synchronisierung

1. Wählen Sie auf der Seite **Benutzerbereitstellung Meine Benutzern und Kennwörtern einmal synchronisieren**.

Zu diesem Zeitpunkt werden Sie aufgefordert, herunterladen und installieren den **Azure AD-Connect-Assistenten**, um Ihre Benutzer lokal zu Office 365 synchronisieren.

2. Nachdem Azure AD-Connect heruntergeladen, führen Sie es aus, und wählen Sie die **Standardoptionen für Express Einstellungen**.

Nachdem die Synchronisierung abgeschlossen ist, gelangen Sie zur Seite Office 365- **Datenmigration**, in dem Sie alle Benutzer sehen, die mit Office 365 synchronisiert wurden.

Nach Abschluss die einmalige Synchronisierung ist Directory-Synchronisierung für Ihre Office 365-Mandanten deaktiviert.

Office 365 Hybrid Configuration

User Provisioning

Office 365 Worldwide  
exmail.cpubment.com  
exmail.cpubment.com  
Exchange Server 2016 15.1.225.42 RTM  
Minimal Hybrid 16.0.1539.7

Hybrid services are now configured between Exchange Online and your on-premises Exchange environment.

Please choose an option for how you would like to handle synchronizing users in your environment.

**Synchronize my users and passwords one time (Recommended)**  
Select this option if you intend on moving all of your mailboxes to Office 365. This wizard will download Azure Active Directory Connect on this page and then launch the tool after you press 'next' below. Follow the instructions to completion (in most cases the default options are desired). After you perform this initial synchronization we will walk you through migrating your mailboxes and switching your DNS records to point to Office 365.  
[learn more](#)

**I will install Azure Active Directory Connect later on my own**  
If you intend on keeping Exchange on-premises or you intend on using advanced features (such as Identity Federation), then you should install and maintain a Directory Synchronization deployment.  
[learn more](#)

AzureADConnect.msi [learn more](#) - Downloaded Successfully

★ [give feedback](#) [back](#) [next](#) [cancel](#)

## Schritt 4: Geben Sie Office 365-Lizenzen für Ihre Benutzer

Nach dem Verbinden von Azure Active Directory synchronisiert die Benutzer und ihre Kennwörter zu Office 365, weisen Sie müssen Office 365 lizenziert werden, damit sie eine cloupostfach, in ihrer lokalen Postfachdaten migrieren besitzen.

Der Status auf der Seite **Datenmigration** gibt an, dass eine Lizenz erforderlich ist, wie in der Abbildung dargestellt.

Wechseln Sie in der Verwaltungskonsole **Benutzern > aktive Benutzer** und befolgen Sie diese Anweisungen zum [Zuweisen von Lizenzen für Benutzer in Office 365 für Unternehmen](#).

User name	Status
bobby@Contoso.com	<span style="color: red;">✖</span> License required <a href="#">details</a>
irwin@Contoso.com	<span style="color: red;">✖</span> License required <a href="#">details</a>
Jakob@Contoso.com	<span style="color: red;">✖</span> License required <a href="#">details</a>
katrina@Contoso.com	<span style="color: red;">✖</span> License required <a href="#">details</a>

## Schritt 5: Start Benutzer Postfachdaten migrieren

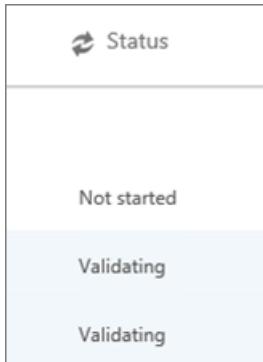
Nachdem Sie den Benutzern Lizenzen zuweisen navigieren Sie zu der Seite Daten Migration zu migrieren, ihren Postfächern.

1. Wechseln Sie zu **Setup > Datenmigration**, und wählen Sie auf der Seite **Migration Exchange** für den Datendienst.
2. Wählen Sie auf der Seite **Datenmigration** die Benutzer, deren Postfächer migriert, und wählen Sie dann die **Migration gestartet** werden soll.

Es wird empfohlen, dass Sie migrieren von Postfächern für zwei oder drei Benutzer als Test vor der

Migration Ihrer Benutzer, um sicherzustellen, dass alles wie erwartet funktioniert.

Migration der Datenzugriffsseite wird den Migrationsstatus angezeigt, wechselt. Eine vollständige Liste finden Sie unter [Migration Benutzer Statusbericht](#), der auch in der Exchange-Verwaltungskonsole angezeigt werden können.



## Schritt 6: Aktualisieren von DNS-Einträgen

E-Mail-Systemen verwenden einen DNS-Eintrag ein MX-Eintrags aufgerufen, um herauszufinden, wo Sie-e-Mails zu übermitteln. Während des Migrationsprozesses e-Mail wurde Ihres MX-Eintrags auf Ihrem lokalen Exchange e-Mail-System zeigen. Nun, da die e-Mail-Migration zu Office 365 abgeschlossen ist, ist es Zeit, zeigen Sie Ihren MX-Eintrag bei Office 365. Sie müssen auch das Einrichten Ihrer DNS-Einträge abzuschließen. Wechseln Sie in das Office 365 Admin Center auf **Einstellungen > Domänen** und wählen Sie dann den Domänennamen, die Sie aktualisieren beispielsweise "contoso.com, möchten". Der Domänen-Assistent führt Sie durch die Updateschritte. Finden Sie in diesem Artikel finden Sie Anweisungen, die speziell für die Registrierung oder Host: [Erstellen von DNS-Datensätze an alle DNS-Hostinganbieter für Office 365](#).

## Siehe auch

[Office 365-migrationsleistung und bewährte Methoden](#)

[Gewusst wie: Außerbetriebsetzen des Exchange-Servers in einer hybridumgebung](#)

[Ändern oder Entfernen von Exchange 2010](#)

[Gewusst wie: entfernen eine Exchange 2007-Organisation](#)

# Wichtige Informationen zur E-Mail-Übernahmemigration zu Office 365

18.12.2018 • 7 minutes to read

Im Rahmen einer Office 365-Bereitstellung können Sie die Inhalte von Benutzerpostfächern aus einem Quell-E-Mail-System nach Office 365 migrieren. Wenn Sie dies alles auf einmal erledigen, handelt es sich um eine so genannte "Übernahmemigration". Die Wahl einer Übernahmemigration wird in folgenden Fällen empfohlen:

- Ihre aktuelle lokale Exchange-Organisation ist Microsoft Exchange Server 2003, Microsoft Exchange Server 2007, Microsoft Exchange Server 2010, Microsoft Exchange Server 2013 oder Exchange Server 2016.
- Ihre lokale Exchange-Organisation enthält weniger als 2.000 Postfächer.

## NOTE

Obwohl bei einer Übernahmemigration bis zu 2.000 Postfächer verschoben werden können, ist es angesichts der langen Zeit, die das Erstellen und Migrieren von 2.000 Benutzern dauert, sinnvoller, maximal 150 Benutzer zu migrieren.

Wenn eine Übernahmemigration für Sie nicht funktioniert, lesen Sie [Möglichkeiten zum Migrieren von E-Mail nach Office 365](#), um Informationen zu weiteren Optionen zu erhalten.

## Zu berücksichtigende Faktoren

Das Einrichten einer E-Mail-Übernahmemigration nach Office 365 muss sorgfältig geplant werden. Nachstehend finden Sie einige wichtige Hinweise, die Sie vor Beginn des Vorgangs berücksichtigen sollten:

- Sie können Ihre gesamte E-Mail-Organisation innerhalb weniger Tage in Office 365 verschieben und Benutzerkonten in Office 365 verwalten.
- Mit einer Exchange-Übernahmemigration können maximal 2.000 Postfächer nach Office 365 migriert werden. Es wird jedoch empfohlen, dass Sie nur 150 Postfächer migrieren.
- Der primäre Domänenname, der für Ihre lokale Exchange-Organisation verwendet wird, muss als eine Domäne akzeptiert sein, deren Besitzer Sie in Ihrer Office 365-Organisation sind.
- Nach Abschluss der Migration ist jeder Benutzer, der über ein lokales Exchange-Postfach verfügt, auch ein neuer Benutzer in Office 365. Sie müssen aber Benutzern, deren Postfächer migriert wurden, weiterhin Lizenzen zuweisen.

## Auswirkungen auf die Benutzer

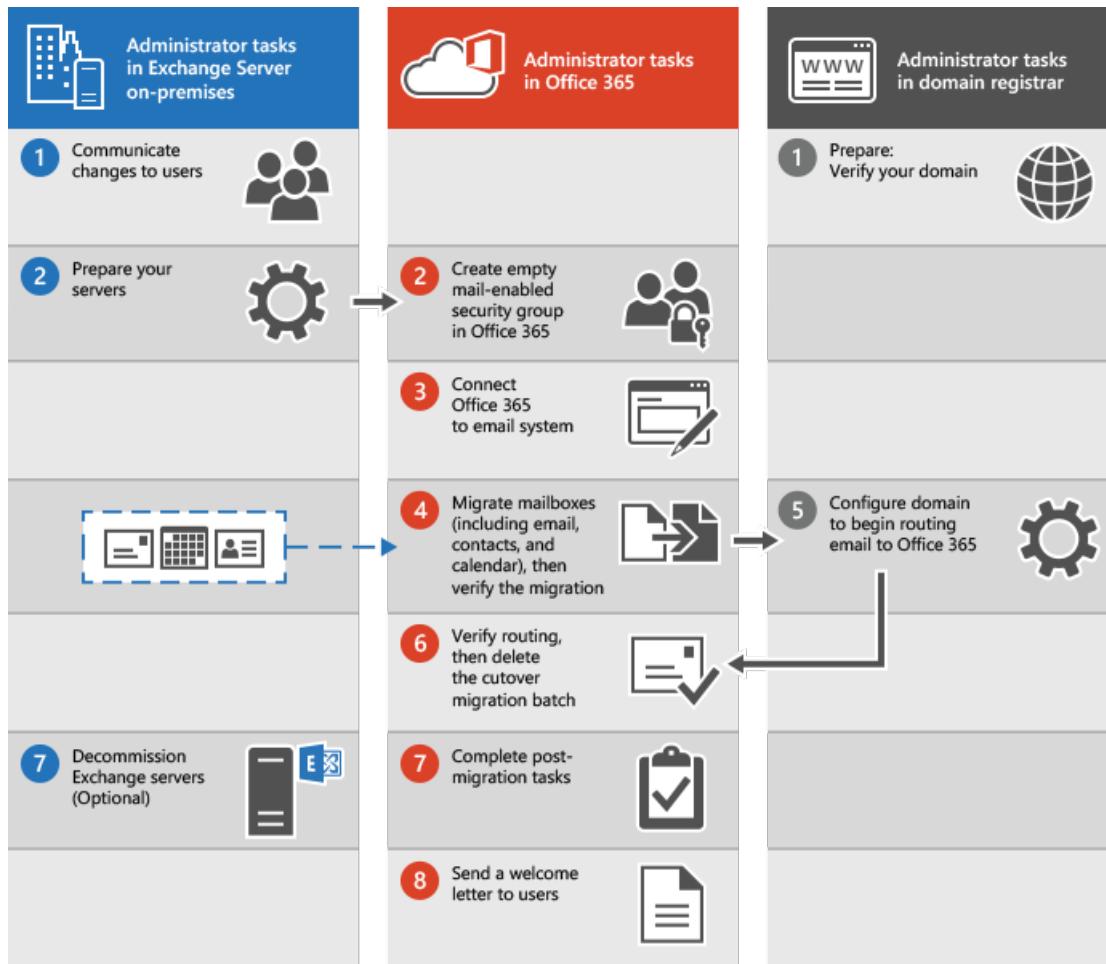
Nachdem Ihre lokalen Organisationen und Office 365-Organisationen für eine Übernahmemigration eingerichtet wurden, könnten sich die nach dem Setup erforderlichen Aufgaben auf Ihre Benutzer auswirken.

- **Administratoren oder Benutzer müssen Desktopcomputer konfigurieren:** sicherstellen, dass Desktopcomputer aktualisierte und Set up für eine Verwendung mit Office 365 sind. Diese Aktionen können Benutzer mit lokalen Benutzeranmeldeinformationen über desktopanwendungen zu Office 365 anmelden. Benutzer mit Berechtigung zum Installieren können aktualisieren und ihren eigenen Desktop einrichten. Oder für diese Updates installiert werden können. Nach Updates vorgenommen wurde, können Benutzer von Outlook 2013, Outlook 2010 oder Outlook 2007 e-Mail senden.

- **Potenzial Verzögerung in e-Mail-routing:** an lokale Benutzer, deren Postfächer zu Office 365 migriert wurden, gesendeten E-Mails werden an ihre lokale Exchange-Postfächer weitergeleitet, bis der MX-Eintrag geändert wird.

## Wie funktioniert die Übernahmemigration?

Die wichtigsten Schritte, die Sie für eine Übernahmemigration ausführen, werden in der folgenden Abbildung gezeigt.



1. Der Administrator benachrichtigt die Benutzer über anstehende Änderungen und überprüft den Domänenbesitz bei der Domänenregistrierungsstelle.
2. Der Administrator bereitet die Server für eine Übernahmemigration vor und erstellt leere E-Mail-aktivierte Sicherheitsgruppen in Office 365.
3. Der Administrator verbindet Office 365 mit dem lokalen E-Mail-System (dieser Vorgang wird als das "Erstellen eines Migrationsendpunkts" bezeichnet).
4. Der Administrator migriert die Postfächer und überprüft dann die Migration.
5. Weisen Sie Ihren Benutzern Office 365-Lizenzen zu.
6. Der Administrator konfiguriert die Domäne, um mit der Weiterleitung von E-Mails direkt an Office 365 zu beginnen.
7. Der Administrator überprüft, ob die Weiterleitung geändert wurde und löscht dann den Übernahmemigrationsbatch.
8. Der Administrator führt die nach der Migration erforderlichen Aufgaben in Office 365 aus (Zuweisen von Lizenzen an Benutzer und Erstellen eines DNS-Eintrags für AutoErmittlung) und nimmt die lokalen Exchange-Server optional außer Betrieb.

Siehe die schrittweisen Anleitungen in [Ausführen der nach der Migration erforderlichen Aufgaben](#).

9. Der Administrator sendet ein Begrüßungsschreiben an die Benutzer, um sie über Office 365 zu informieren und zu beschreiben, wie sie sich bei ihren neuen Postfächern anmelden müssen.

## Bereit zum Starten?

Wenn Ihnen das Einrichten einer Migration nach Office 365 vertraut ist, müssen Sie die folgenden Aufgaben erledigen:

- Richten Sie Exchange Server über das Exchange Admin Center ein.
- Ändern Sie den MX-Eintrag Ihrer Organisation so, dass er auf Office 365 verweist, wenn die Migration abgeschlossen ist. Ihr MX-Eintrag gibt an, wie andere E-Mail-Systeme den Speicherort Ihres E-Mail-Systems finden. Durch die Änderung Ihres MX-Eintrags können andere E-Mail-Systeme damit beginnen, E-Mails direkt an die neuen Postfächer in Office 365 zu senden. Wir stellen Anweisungen, wie dazu vorzugehen ist, für viele DNS-Anbieter bereit. Zum Einrichten der öffentlichen DNS-Server müssen Sie den MX-Eintrag Ihrer Organisation so ändern, dass er auf Office 365 verweist, wenn Sie auswählen, dass alle eingehenden Internet-E-Mails für Ihre lokale Exchange-Organisation über Office 365 weitergeleitet werden.

Wenn Sie mit einer Übernahmemigration beginnen möchten, wechseln Sie zu [Durchführen einer Übernahmemigration von E-Mails zu Office 365](#).

## Siehe auch

[Möglichkeiten zum Migrieren von E-Mail zu Office 365](#)

[Verwenden von PowerShell zum Durchführen einer Übernahmemigration nach Office 365](#)

# Migrieren der e-Mails mithilfe der Exchange-Ü-Methode

18.12.2018 • 31 minutes to read

Im Rahmen einer Office 365-Bereitstellung können Sie die Inhalte von Benutzerpostfächern aus einem Quell-E-Mail-System nach Office 365 migrieren. Wenn Sie dies alles auf einmal erledigen, handelt es sich um eine so genannte "Übernahmemigration". Die Wahl einer Übernahmemigration wird in folgenden Fällen empfohlen:

- Ihre aktuelle lokale Exchange-Organisation mit Microsoft Exchange Server 2003 oder höher ist.
- Ihre lokale Exchange-Organisation enthält weniger als 2.000 Postfächer.

## NOTE

Obwohl bei einer Übernahmemigration bis zu 2.000 Postfächer verschoben werden können, ist es angesichts der langen Zeit, die das Erstellen und Migrieren von 2.000 Benutzern dauert, sinnvoller, maximal 150 Benutzer zu migrieren.

## Planen der Migration

Das Einrichten einer E-Mail-Übernahmemigration nach Office 365 muss sorgfältig geplant werden.

Nachstehend finden Sie einige wichtige Hinweise, die Sie vor Beginn des Vorgangs berücksichtigen sollten:

- Sie können Ihre gesamte E-Mail-Organisation innerhalb weniger Tage in Office 365 verschieben und Benutzerkonten in Office 365 verwalten.
- Mit einer Exchange-Übernahmemigration können maximal 2.000 Postfächer nach Office 365 migriert werden. Es wird jedoch empfohlen, dass Sie nur 150 Postfächer migrieren.
- Der primäre Domänenname, der für Ihre lokale Exchange-Organisation verwendet wird, muss als eine Domäne akzeptiert sein, deren Besitzer Sie in Ihrer Office 365-Organisation sind.
- Nach Abschluss der Migration ist jeder Benutzer, der über ein lokales Exchange-Postfach verfügt, auch ein neuer Benutzer in Office 365. Sie müssen aber Benutzern, deren Postfächer migriert wurden, weiterhin Lizenzen zuweisen.

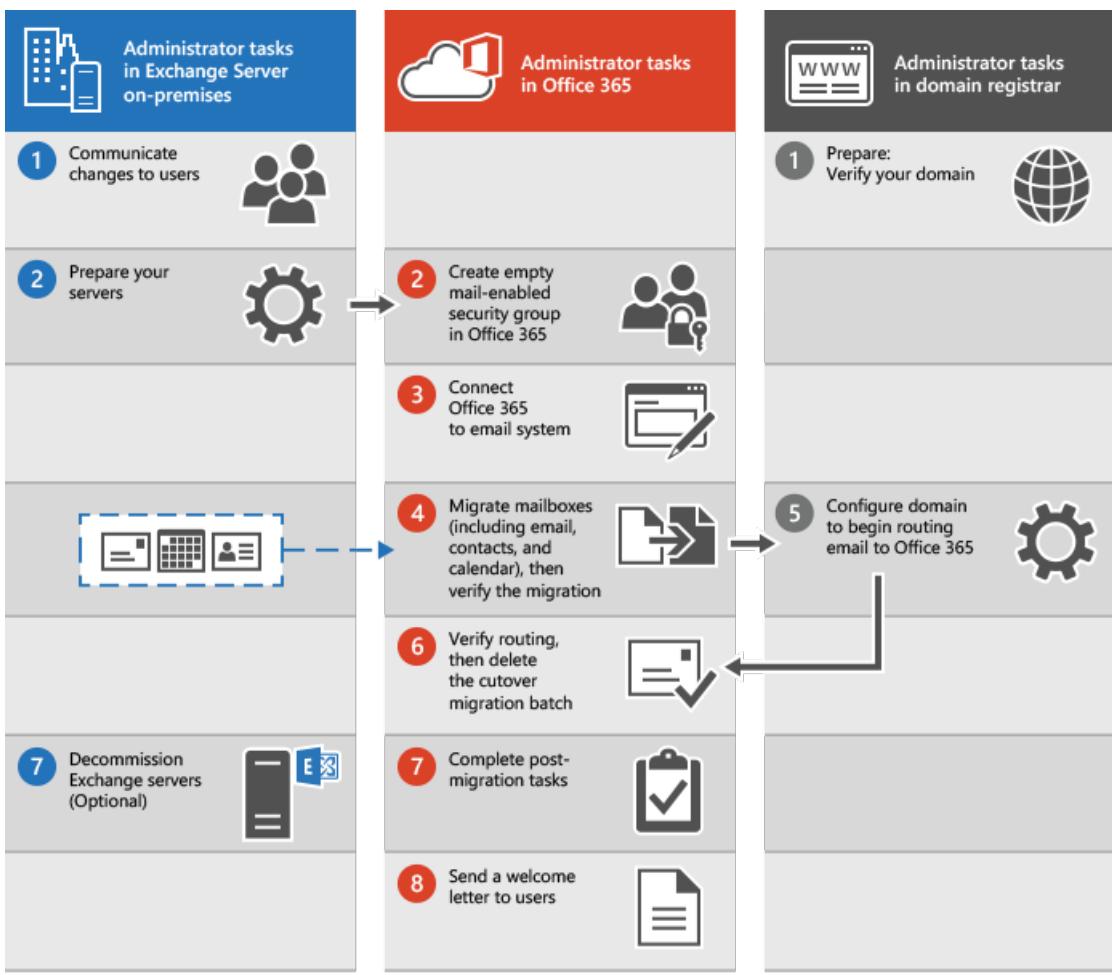
## Auswirkungen auf die Benutzer

Nachdem Ihre lokalen Organisationen und Office 365-Organisationen für eine Übernahmemigration eingerichtet wurden, könnten sich die nach dem Setup erforderlichen Aufgaben auf Ihre Benutzer auswirken.

- **Administratoren oder Benutzer müssen Desktopcomputer konfigurieren:** sicherstellen, dass Desktopcomputer aktualisierte und Set up für eine Verwendung mit Office 365 sind. Diese Aktionen können Benutzer mit lokalen Benutzeranmeldeinformationen über desktopanwendungen zu Office 365 anmelden. Benutzer mit Berechtigung zum Installieren können aktualisieren und ihren eigenen Desktop einrichten. Oder für diese Updates installiert werden können. Nach Updates vorgenommen wurde, können Benutzer von Outlook 2013, Outlook 2010 oder Outlook 2007 e-Mail senden.
- **Potenzial Verzögerung in e-Mail-routing:** an lokale Benutzer, deren Postfächer zu Office 365 migriert wurden, gesendeten E-Mails werden an ihre lokale Exchange-Postfächer weitergeleitet, bis der MX-Eintrag geändert wird.

## Wie funktioniert die Übernahmemigration?

Die wichtigsten Schritte, die Sie für eine Übernahmemigration ausführen, werden in der folgenden Abbildung gezeigt.



- Der Administrator benachrichtigt die Benutzer über anstehende Änderungen und überprüft den Domänenbesitz bei der Domänenregistrierungsstelle.
- Der Administrator bereitet die Server für eine Übernahmemigration vor und erstellt leere E-Mail-aktivierte Sicherheitsgruppen in Office 365.
- Der Administrator verbindet Office 365 mit dem lokalen E-Mail-System (dieser Vorgang wird als das "Erstellen eines Migrationsendpunkts" bezeichnet).
- Der Administrator migriert die Postfächer und überprüft dann die Migration.
- Weisen Sie Ihren Benutzern Office 365-Lizenzen zu.
- Der Administrator konfiguriert die Domäne, um mit der Weiterleitung von E-Mails direkt an Office 365 zu beginnen.
- Der Administrator überprüft, ob die Weiterleitung geändert wurde und löscht dann den Übernahmemigrationsbatch.
- Der Administrator führt die nach der Migration erforderlichen Aufgaben in Office 365 aus (Zuweisen von Lizenzen an Benutzer und Erstellen eines DNS-Eintrags für AutoErmittlung) und nimmt die lokalen Exchange-Server optional außer Betrieb.
- Der Administrator sendet ein Begrüßungsschreiben an die Benutzer, um sie über Office 365 zu informieren und zu beschreiben, wie sie sich bei ihren neuen Postfächern anmelden müssen.

Für die Ausführung einer einstufigen Migrations bereit?

Erweitern Sie in den folgenden Abschnitten aus, und führen Sie die Schritte aus.

## Vorbereiten auf eine Übernahmemigration

Bevor Sie mithilfe einer Übernahmemigration Postfächer zu Office 365 migrieren, müssen Sie einige Änderungen an Ihrer Exchange Server-Umgebung vornehmen.

### NOTE

Wenn Sie die Verzeichnissynchronisierung aktiviert haben, müssen Sie diese deaktivieren, bevor Sie eine Übernahmemigration durchführen können. Hierzu können Sie die PowerShell verwenden. Entsprechende Anweisungen finden Sie unter [Deaktivieren der Verzeichnissynchronisierung für Office 365](#).

1. **Konfigurieren von Outlook Anywhere auf Ihrem lokalen Exchange-Server:** der e-Mail-Migrationsservice Outlook Anywhere (auch bekannt als RPC über HTTP) für die Verbindung mit Ihrer lokalen Exchange-Server verwendet. Outlook Anywhere wird automatisch für Exchange 2013 konfiguriert. Informationen dazu, wie Outlook Anywhere für Exchange 2010, Exchange 2007 und Exchange 2003 einrichten finden Sie unter den folgenden:
  - [Exchange 2010: Aktivieren von Outlook Anywhere](#)
  - [Exchange 2007: Aktivieren von Outlook Anywhere](#)
  - [Konfigurieren von Outlook Anywhere mit Exchange 2003](#)
2. Sie müssen ein Zertifikat verwenden, das von einer vertrauenswürdigen Zertifizierungsstelle (CA) mit Ihrer Outlook Anywhere-Konfiguration ausgestellt wurde, um mit Office 365 eine Übernahmemigration durchführen zu können. Für die Übernahmemigration müssen Sie die Dienste Outlook Anywhere und AutoErmittlung zu Ihrem Zertifikat hinzufügen. Anweisungen zum Einrichten von Zertifikaten finden Sie unter:
  - [Hinzufügen eines SSL-Zertifikats zu Exchange 2013](#)
  - [Hinzufügen eines SSL-Zertifikats zu Exchange 2010](#)
  - [Hinzufügen eines SSL-Zertifikats zu Exchange 2007](#)
3. **Optional: Stellen Sie sicher, dass Sie Ihre Exchange-Organisation mit Outlook Anywhere eine Verbindung herstellen können:** Führen Sie eine der folgenden Methoden, um die Verbindungseinstellungen zu testen.
  - Verwenden Sie Outlook außerhalb Ihres Unternehmensnetzwerks zum Herstellen einer Verbindung mit dem lokalen Exchange-Postfach.
  - Verwenden Sie [Microsoft Exchange Remote Connectivity Analyzer](#) zum Testen der Verbindungseinstellungen. Verwenden Sie Tests von Outlook Anywhere (RPC über HTTP) oder Outlook-AutoErmittlung.
  - Warten Sie, bis die Verbindung automatisch getestet wird, wenn Sie die Aufgabe "Herstellen einer Verbindung zwischen Office 365 und dem E-Mail-System" weiter unten in diesem Verfahren ausführen.
4. **Festlegen von Berechtigungen:** das lokale Benutzerkonto, mit denen Sie Ihre lokalen Exchange-Organisation (auch als dem migrationsadministrator bezeichnet) herstellen, benötigen die erforderlichen Berechtigungen für die lokale Postfächer zugreifen, die Sie migrieren möchten zu Office 365. Dieses Benutzerkonto wird verwendet, wenn Sie mit Ihrem e-Mail-System weiter unten in diesem Verfahren Office 365 verbinden.

5. Um die Postfächer zu migrieren, muss der Administrator über eine der folgenden Berechtigungen verfügen:
  - Dem Migrationsadministrator muss die **FullAccess** -Berechtigung für jedes lokale Postfach zugeordnet sein.

oder

- Dem Migrationsadministrator muss die **Receive As** -Berechtigung für die lokale Postfachdatenbank zugeordnet sein, in der die Benutzerpostfächer gespeichert sind.

Anweisungen zum Festlegen dieser Berechtigungen finden Sie unter [Zuweisen von Exchange-Berechtigungen zum Migrieren von Postfächern zu Office 365](#).

6. **Deaktivieren von Unified Messaging (UM):** Wenn UM eingeschaltet ist und für die lokalen Postfächer, die Sie migrieren möchten, deaktivieren Sie UM vor der Migration. Schalten Sie UM oder die Postfächer nach der Migration abgeschlossen ist.

7. **Erstellen von Sicherheitsgruppen und Bereinigen von Stellvertretungen:** da der e-Mail-Migrationsservice nicht erkennen kann, ob der lokale Active Directory-Gruppen-Sicherheitsgruppen sind, kann nicht es alle migrierten Gruppen als Sicherheitsgruppen in Office 365 bereitstellen. Wenn Sie Sicherheitsgruppen in Office 365 haben möchten, müssen Sie zunächst eine leere e-Mail-aktivierte Sicherheitsgruppe in Office 365 vor dem Starten der einstufigen Migrations bereitstellen.

Darüber hinaus werden bei dieser Migrationsmethode nur Postfächer, E-Mail-Benutzer, E-Mail-Kontakte und E-Mail-aktivierte Gruppen verschoben. Wenn ein anderes Active Directory-Objekt, z. B. ein Benutzerpostfach, das nicht nach Office 365 migriert wird, einem Objekt, das migriert wird, als Manager oder Stellvertretung zugeordnet ist, müssen Sie diese Zuordnung vor der Migration aus dem Objekt entfernen.

## Schritt 1: Sicherstellen, dass Sie die Domäne besitzen

Während der Migration wird die SMTP-Adresse (Simple Mail Transfer Protocol) der einzelnen lokalen Postfächer verwendet, um die E-Mail-Adresse für ein neues Office 365-Postfach zu erstellen. Damit eine Übernahmemigration ausgeführt werden kann, muss die lokale Domäne eine überprüfte Domäne in Ihrer Office 365-Organisation sein.

1. Melden Sie sich bei Office 365 mit Ihrem Geschäfts-, Schul- oder Unikonto an.
2. Wählen Sie **Setup > Domänen** aus.
3. Klicken Sie auf der Seite **Domänen - auf Domäne hinzufügen**, um die Domäne-Assistenten zu starten.



4. Geben Sie auf der Seite **Domäne hinzufügen** den Domänennamen (z. B. "Contoso.com") ein, den Sie für die lokale Exchange-Organisation verwenden, und wählen Sie dann **Weiter** aus.
5. Wählen Sie auf der Seite **Domäne überprüfen** oder (sofern Ihre DNS-Datensätze durch GoDaddy verwaltet werden) **Melden Sie sich bei "GoDaddy" Hinzufügen ein TXT-Eintrags stattdessen** für alle anderen Registrierungsstellen > **Weiter**.
6. Folgen Sie den für Ihren DNS-Hostinganbieter zutreffenden Anweisungen. In der Regel wird der TXT-Eintrag ausgewählt, um den Besitz zu überprüfen.

Anweisungen hierzu finden Sie auch unter [Erstellen von DNS-Einträgen für Office 365, wenn Sie Ihre DNS-Einträge verwalten](#).

Nachdem Sie Ihren TXT- oder MX-Eintrag hinzugefügt haben, warten Sie etwa 15 Minuten, bevor Sie mit dem nächsten Schritt fortfahren.

7. Wählen Sie im Office 365-Assistenten für Domänen die Option **Fertig, jetzt überprüfen** aus. Daraufhin wird eine Überprüfungsseite angezeigt. Klicken Sie auf **Fertig stellen**.

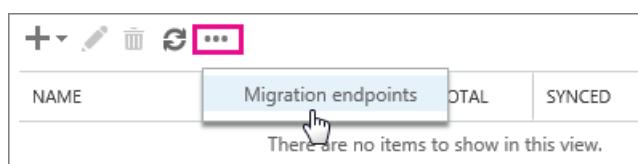
Wenn die Überprüfung zunächst fehlschlägt, warten Sie einen Moment, und versuchen Sie es erneut.

Fahren Sie nicht mit dem nächsten Schritt im Assistenten fort. Sie haben nun überprüft, dass Sie der Besitzer der lokalen Domäne der Exchange-Organisation sind, und können mit einer E-Mail-Migration fortfahren.

## Schritt 2: Herstellen einer Verbindung zwischen Office 365 und Ihrem E-Mail-System

Ein Migrationsendpunkt enthält die Einstellungen und Anmeldeinformationen, die erforderlich sind, um eine Verbindung mit dem lokalen Server herzustellen, der die Postfächer hostet, die Sie mit Office 365 migrieren. Der Migrationsendpunkt definiert auch die Anzahl der gleichzeitig zu migrierenden Postfächer. Für eine Übernahmemigration erstellen Sie einen Outlook Anywhere-Migrationsendpunkt.

1. Wechseln Sie zum Exchange Admin Center.
2. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.
3. Wählen Sie **Weitere ... > migrationsendpunkte**.



4. Wählen Sie auf der Seite **migrationsendpunkte neu +**.
5. Wählen Sie auf der Seite **Typ des Migrationsendpunkts auswählen** die Option **Outlook Anywhere > Weiter** aus.
6. Geben Sie auf der Seite **Anmeldeinformationen für lokales Konto eingeben** Informationen in die folgenden Felder ein:
  - **E-Mail-Adresse:** Geben Sie die e-Mail-Adresse eines Benutzers in der lokalen Exchange-Organisation, die migriert werden. Office 365 wird die Konnektivität für Postfach des Benutzers zu testen.
  - **Konto mit Berechtigungen:** Geben Sie den Benutzernamen (Format Domäne\Benutzername ein oder eine e-Mail-Adresse) für ein Konto, das in der lokalen Organisation die erforderlichen administrativen Berechtigungen verfügt. Office 365 wird dieses Konto verwenden, um den migrationsendpunkt zu erkennen und die Berechtigungen für dieses Konto durch den Versuch, Zugriff auf das Postfach mit der angegebenen e-Mail-Adresse zu testen.
  - **Das Kennwort des Kontos mit Berechtigungen:** Geben Sie das Kennwort für das Konto mit Berechtigungen, die das Administratorkonto handelt.
7. Wählen Sie **Weiter** aus, und führen Sie eine der folgenden Aktionen aus:
  - Wenn Office 365 erfolgreich eine Verbindung mit dem Quellserver herstellt, werden die Verbindungseinstellungen angezeigt. Wählen Sie **Weiter** aus.

new migration endpoint

Confirm the migration endpoint

The connection settings for this migration batch have been automatically selected based on the migration endpoints created in your organization. [Learn more](#)

\*Exchange server:  
exch-test5-01@contoso.com

\*RPC proxy server:  
mail.contoso.com

[More options...](#)

This is the FQDN of the Exchange server that hosts the mailboxes that you're migrating.

- Wenn die Testverbindung mit dem Quellserv er nicht erfolgreich ist, geben Sie die folgenden Informationen ein:
  - **Exchange Server:** Geben Sie den *vollqualifizierten Domänennamen* (FQDN) für den lokalen Exchange Server. Dies ist der Hostname für Ihre Postfachserver. Beispielsweise EXCH-SRV-01.corp.contoso.com.
  - **RPC-Proxyserver:** Geben Sie den *FQDN* für den RPC-Proxyserver für Outlook Anywhere. In der Regel ist der Proxyserver identisch mit der Outlook Web App-URL. Mail.contoso.com, also auch die URL für den Proxy-Server, die Outlook verwendet, um die Verbindung mit einem Exchange-Server
8. Geben Sie auf der Seite **Allgemeine Informationen eingeben** einen *migrationsendpunktnamen ein*, beispielsweise Test5-Endpunkt. Lassen Sie die beiden anderen Felder leer, verwenden Sie die Standardwerte.

new migration endpoint

Enter general information

Enter the value for the general information for the migration endpoint that'll be applied to the associated migrations. [Learn more](#)

\*Migration endpoint name:  
Test5-endpoint

Maximum concurrent migrations:

Maximum concurrent incremental syncs:

[back](#) [new](#) [cancel](#)

9. Wählen Sie **Neu** aus, um den Migrationsendpunkt zu erstellen.

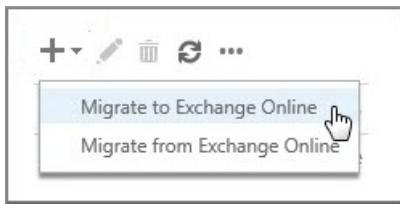
Zum Überprüfen, ob Ihr Exchange Online mit dem lokalen Server verbunden ist, führen Sie den Befehl in Beispiel 4 von [Test-MigrationServerAvailability](#) aus.

## Schritt 3: Erstellen des Übernahmemigrationsbatches

In einer Übernahmemigration werden lokale Postfächer in einem einzigen Migrationsbatch zu Office 365 migriert.

1. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.

2. Wählen Sie **neu + > zu Exchange Online migrieren**.



3. Wählen Sie auf der Seite **Migrationstyp auswählen** die Option **Übernahmemigration** > **Weiter** aus.

4. Wählen Sie auf der Seite **Migrationsendpunkt bestätigen** die aufgeführten Migrationsendpunktinformationen aus. Überprüfen Sie die Informationen, und wählen Sie dann **Weiter** aus.



5. Klicken Sie auf der Seite **Konfiguration verschieben** Geben Sie den *Namen* (darf keine Leerzeichen und Sonderzeichen enthalten) des migrationsbatches, und wählen Sie dann auf **Weiter**. Der Blattnamen wird angezeigt, in der Liste der migrationsbatches auf der Seite **Migration** nach dem Erstellen des migrationsbatches.

6. Wählen Sie auf der Seite **Batch starten** eine der folgenden Optionen aus:

- **Starten Sie den Batch automatisch:** der migrationsbatch gestartet ist, sobald Sie den neuen migrationsbatch mit dem Status der **Synchronisierung** gespeichert.
- **Starten Sie den Batch später manuell:** der migrationsbatch erstellt wurde, jedoch nicht gestartet wird. Der Status des Stapels wird auf **erstellt** festgelegt. Um einen migrationsbatch zu starten, wählen Sie sie im migrationsdashboard, und wählen Sie dann auf **Starten**.

7. Wählen Sie **Neu** aus, um den Migrationsbatch zu erstellen.

Der neue Migrationsbatch wird auf dem Migrationsdashboard angezeigt.

## Schritt 4: Starten des Übernahmemigrationsbatches

Wenn Sie einen Migrationsbatch erstellt und so konfiguriert haben, dass er manuell gestartet werden muss, können Sie ihn über das Exchange Admin Center starten.

1. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.

2. Wählen Sie auf dem Migrationsdashboard den Batch aus, und wählen Sie dann **Starten** aus.

3. Wurde ein Migrationsbatch erfolgreich gestartet, wird dessen Status auf dem Migrationsdashboard in **Wird synchronisiert** geändert.

Click to view the status for all current migration batches. <a href="#">Status for all batches</a>					
NAME	▲ STATUS	TOTAL	SYNCED	FINALIZED	FAILED
Test5-migration	Syncing	5	0	0	0
Status changes from Created to Syncing after the migration starts.					

## Überprüfen, ob die Synchronisierung erfolgreich war

- Sie können den Synchronisierungsstatus auf dem Migrationsdashboard verfolgen. Wenn Fehler vorhanden sind, können Sie eine Protokolldatei anzeigen, in der Sie weitere Informationen zu den Fehlern finden.
- Sie können im Office 365 Admin Center auch überprüfen, ob die Benutzer erstellt werden, während die Migration fortschreitet.

Nachdem die Migration abgeschlossen ist, ist der Synchronisierungsstatus gleich **Synchronisiert**.

## Optional: Verringern von E-Mail-Verzögerungen

Obwohl diese Aufgabe optional ist, lassen sich mit ihrer Ausführung Verzögerungen beim Empfangen von E-Mails in den neuen Office 365-Postfächern vermeiden.

Wenn Personen, die nicht zu Ihrer Organisation gehören, E-Mails an Sie senden, wird von den E-Mail-Systemen dieser Personen nicht jedes Mal geprüft, wohin die E-Mails gesendet werden sollen. Stattdessen speichern diese Systeme den Speicherort Ihres E-Mail-Systems anhand einer Einstellung in Ihrem DNS-Server, die als Gültigkeitsdauer (Time-to-live, TTL) bezeichnet wird. Wenn Sie den Speicherort Ihres E-Mail-Systems ändern, bevor die TTL abgelaufen ist, versucht das E-Mail-System des Absenders, E-Mails an den alten Speicherort zu senden, bevor es feststellt, dass sich der Speicherort geändert hat. Diese Speicherortänderung kann zu einer Verzögerung in der E-Mail-Zustellung führen. Eine Möglichkeit, dies zu vermeiden, besteht darin, den TTL-Wert zu verringern, den Ihr DNS-Server bereitstellt, die nicht zu Ihrer Organisation gehören. Dadurch werden die anderen Organisationen veranlasst, den Speicherort Ihres E-Mail-Systems häufiger zu aktualisieren.

Die meisten E-Mail-Systeme fordern jede Stunde eine Aktualisierung an, wenn ein kurzes Intervall, etwa 3.600 Sekunden (eine Stunde), festgelegt ist. Es wird empfohlen, dass Sie das Intervall mindestens auf diesen niedrigen Wert festlegen, bevor Sie die E-Mail-Migration starten. Diese Einstellung bietet allen Systemen, die E-Mails an Sie senden, genügend Zeit, die Änderung zu verarbeiten. Wenn Sie dann den endgültigen Umstieg auf Office 365 vorgenommen haben, können Sie den TTL-Wert wieder in ein längeres Intervall ändern.

Die TTL-Einstellung ändern Sie im MX-Eintrag Ihres E-Mail-Systems. Der MX-Eintrag befindet sich auf Ihrem öffentlichen DNS-System. Wenn Sie mehrere MX-Einträge haben, müssen Sie den Wert für jeden Eintrag auf 3.600 Sekunden oder weniger ändern.

Wenn Sie Unterstützung für das Konfigurieren Ihrer DNS-Einstellungen benötigen, sollten Sie zu [Erstellen von DNS-Einträgen für Office 365, wenn Sie Ihre DNS-Einträge verwalten](#) wechseln.

## Schritt 5: Direktes Weiterleiten von E-Mails an Office 365

E-Mail-Systeme verwenden einen als MX-Eintrag bezeichneten DNS-Eintrag, um zu ermitteln, wohin E-Mails gesendet werden sollen. Während der E-Mail-Migration hat Ihr MX-Eintrag auf Ihr Quell-E-Mail-System verwiesen. Nachdem die E-Mail-Migration zu Office 365 nun abgeschlossen ist, sollte Ihr MX-Eintrag auf Office 365 verweisen. Dadurch ist sichergestellt, dass E-Mails an Ihre Office 365-Postfächer gesendet werden. Das Verschieben des MX-Eintrags ermöglicht es Ihnen außerdem, das alte E-Mail-System zu deaktivieren, wenn Sie fertig sind.

Viele DNS-Anbieter stehen bestimmte Anweisungen zum Ändern des MX-Eintrags. Wenn es sich bei Ihrem DNS-Anbieter nicht vorhanden ist oder wenn Sie die allgemeinen Anweisungen einen Eindruck davon erhalten möchten, werden [Allgemeine MX-Eintrag Anweisungen](#) bereitgestellt sowie.

Es kann bis zu 72 Stunden dauern, bis die E-Mail-Systeme Ihrer Kunden und Partner den geänderten MX-Eintrag erkannt haben. Warten Sie mindestens 72 Stunden, bevor Sie beginnen, die nächste Aufgabe auszuführen: Löschen des Übernahmemigrationsbatches.

## Schritt 6: Löschen des Übernahmemigrationsbatches

Nachdem Sie den MX-Eintrag geändert und sich vergewissert haben, dass alle E-Mails an Office 365-Postfächer weitergeleitet werden, teilen Sie Ihren Benutzern mit, dass deren E-Mails an Office 365 gesendet werden. Danach können Sie den Übernahmemigrationsbatch löschen. Überprüfen Sie Folgendes, bevor Sie den Migrationsbatch löschen.

- Alle Benutzer verwenden Office 365-Postfächer. Nachdem der Batch gelöscht ist, werden E-Mails, die an Postfächer auf dem lokalen Exchange Server gesendet wurden, nicht in die entsprechenden Office 365-Postfächer kopiert.
- Office 365-Postfächer wurden mindestens einmal synchronisiert seit dem Zeitpunkt, ab dem E-Mails direkt an sie gesendet werden. Vergewissern Sie sich dazu, dass der Wert im Feld **Zeit der letzten Synchronisierung** für den Migrationsbatch einen neueren Zeitpunkt angibt als der Zeitpunkt, ab dem E-Mails direkt an Office 365-Postfächer weitergeleitet werden.

Wenn Sie einen Übernahmemigrationsbatch löschen, bereinigt der Migrationsdienst alle Einträge, die mit dem Migrationsbatch zu tun haben, und löscht dann den Migrationsbatch. Der Batch wird auf dem Migrationsdashboard aus der Liste der Migrationsbatches entfernt.

1. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.
2. Wählen Sie auf dem Migrationsdashboard den Batch aus, und wählen Sie dann **Löschen** aus.

### NOTE

Es kann einige Minuten dauern, bis der Batch entfernt ist.

3. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.
4. Vergewissern Sie sich, dass der Migrationsbatch nicht mehr auf dem Migrationsdashboard aufgeführt wird.

## Schritt 7: Zuweisen von Lizenzen zu Office 365-Benutzern

### Aktivieren von Office 365-Benutzerkonten für die migrierten Konten durch Zuweisen von Lizenzen:

Wenn Sie keine Lizenz zuweisen, wird das Postfach deaktiviert, wenn die Kulanzfrist (30 Tage) endet. Zuweisen, indem Sie eine Lizenz im Office 365 Administrationscenter finden Sie unter [Zuweisen von Lizenzen für Benutzer in Office 365 für Unternehmen](#).

## Ausführen der nach der Migration erforderlichen Aufgaben

Nach dem Migrieren von Postfächern zu Office 365 gibt es migrationsbezogene Aufgaben, die ausgeführt werden müssen.

1. **Erstellen Sie einen AutoErmittlung-DNS-Eintrag, sodass Benutzer auf einfache Weise auf ihre Postfächer zugreifen können:** Nachdem alle lokalen Postfächern zu Office 365 migriert wurden, können Sie einen Autodiscover DNS-Eintrag für Ihre Office 365-Organisation so aktivieren Sie Benutzer

für die Verbindung auf einfache Weise konfigurieren Ihre neuen Office 365-Postfächer mit Outlook und mobile Clients. Diese neuen Autodiscover DNS-Eintrag muss den gleichen Namespace verwendet, den Sie für Ihre Office 365-Organisation verwenden. Beispielsweise ist Ihre Cloud-basierten Namespace `cloud.contoso.com`, dem Autodiscover DNS-Eintrag, den Sie erstellen müssen `autodiscover.cloud.contoso.com`.

Wenn Sie Ihre Exchange-Server beibehalten haben, sollten Sie auch sicherstellen, dass AutoErmittlung DNS-CNAME-Eintrag muss, damit der Outlook-Client für die Verbindung mit dem richtigen Postfach wird zu Office 365 in interne und externe DNS nach der Migration zeigen. Ersetzen Sie `<ServerName>` mit dem Namen der Clientzugriffsserver und Ausführen den folgenden Befehl in der Exchange-Verwaltungsshell, Clientverbindungen mit dem Server zu verhindern. Sie müssen den Befehl auf jedem Client Access Server ausführen.

```
Set-ClientAccessServer -Identity <ServerName> AutoDiscoverServiceInternalUri $null
```

Office 365 wird ein CNAME-Eintrag für die Implementierung des AutoErmittlungsdiensts für Outlook und mobile Clients verwendet. Der CNAME-Eintrag für die AutoErmittlung muss folgende Informationen enthalten:

- **Alias:** autodiscover
- **Ziel:** autodiscover.outlook.com

Weitere Informationen finden Sie unter [Create DNS records for Office 365 when you manage your DNS records](#).

2. **Nehmen lokalen Exchange-Servern:** Nachdem Sie sichergestellt haben, dass alle e-Mails direkt an die Office 365-Postfächer weitergeleitet werden wird und müssen nicht mehr verwalten Ihre lokale e-Mail-Organisation oder nicht planen der Implementierung von einmaliges Anmelden -Lösung können Sie Deinstallieren von Exchange auf Ihren Servern und Ihrer lokalen Exchange-Organisation entfernen.

Weitere Informationen hierzu finden Sie in den folgenden Artikeln:

- [Ändern oder Entfernen von Exchange Server 2010](#)
- [Entfernen einer Exchange 2007-Organisation](#)
- [Deinstallieren von Exchange Server 2003](#)

#### NOTE

Eine Außerbetriebnahme von Exchange kann unerwartete Folgen haben. Vor der Außerbetriebnahme Ihrer lokalen Exchange-Organisation sollten Sie Kontakt mit dem Microsoft-Support aufnehmen.

## Siehe auch

[Möglichkeiten zum Migrieren von E-Mail zu Office 365](#)

[Auswählen eines Migrationspfads](#)

# Wichtige Informationen zur mehrstufigen E-Mail-Migration zu Office 365

18.12.2018 • 13 minutes to read

Im Rahmen einer Office 365-Bereitstellung können Sie die Inhalte von Benutzerpostfächern aus einem Quell-E-Mail-System nach Office 365 migrieren. Wenn Sie diesen Vorgang nach und nach ausführen, wird von "mehrstufiger Migration" gesprochen. Eine mehrstufige Migration wird in folgenden Fällen empfohlen:

- Ihr Quell-E-Mail-System ist Microsoft Exchange Server 2003 oder Microsoft Exchange Server 2007.

## NOTE

Sie können mithilfe einer mehrstufigen Migration keine Exchange 2013- oder Exchange Server 2010-Postfächer nach Office 365 migrieren. Erwägen Sie stattdessen eine Übernahmemigration oder eine hybride E-Mail-Migration.

- Sie haben mehr als 2.000 Postfächer.

Wenn eine mehrstufige Migration für Sie nicht funktioniert, lesen Sie [Möglichkeiten zum Migrieren von E-Mail nach Office 365](#), um Informationen zu weiteren Optionen zu erhalten.

## Zu berücksichtigende Faktoren

Es gibt einige Punkte, die Sie beachten müssen:

- Sie müssen Konten zwischen Ihrer lokalen Active Directory-Domäne und Office 365 mithilfe von Azure Active Directory-Synchronisierung synchronisieren, damit eine mehrstufige Migration funktioniert.
- Der primäre Domänenname, der für Ihre lokale Exchange-Organisation verwendet wird, muss für eine Domäne stehen, die für Ihre Office 365-Organisation überprüft wurde.
- Sie können nur Benutzerpostfächer und Ressourcenpostfächer migrieren. Andere Empfängertypen, beispielsweise Verteilergruppen, Kontakte und E-Mail-aktivierte Benutzer, werden durch die Verzeichnissynchronisierung nach Office 365 migriert.
- Abwesenheitsnachrichten werden nicht zusammen mit Benutzerpostfächern migriert. Wenn ein Benutzer das Feature "Abwesenheit" vor der Migration aktiviert, bleibt es im migrierten Postfach aktiviert, doch die Abwesenheitsnachricht ist leer. Personen, die Nachrichten an das Postfach senden, erhalten keine Abwesenheitsbenachrichtigung. Wenn Abwesenheitsbenachrichtigungen gesendet werden sollen, muss der Benutzer die Abwesenheitsnachricht nach der Migration des Postfachs erneut erstellen.
- Wenn Sie die Verbindungen mit Ihrem Quell-E-Mail-System beschränkt haben, ist es ratsam, sie zu erhöhen, um die Migrationsleistung zu verbessern. Zu den üblichen Verbindungsbeschränkungen gehören Gesamtanzahl der Client/Server-Verbindungen, Verbindungen pro Benutzer und IP-Adressenverbindungen auf dem Server oder in der Firewall. Wenn Sie diese Verbindungen nicht beschränkt haben, können Sie diese Aufgabe überspringen.

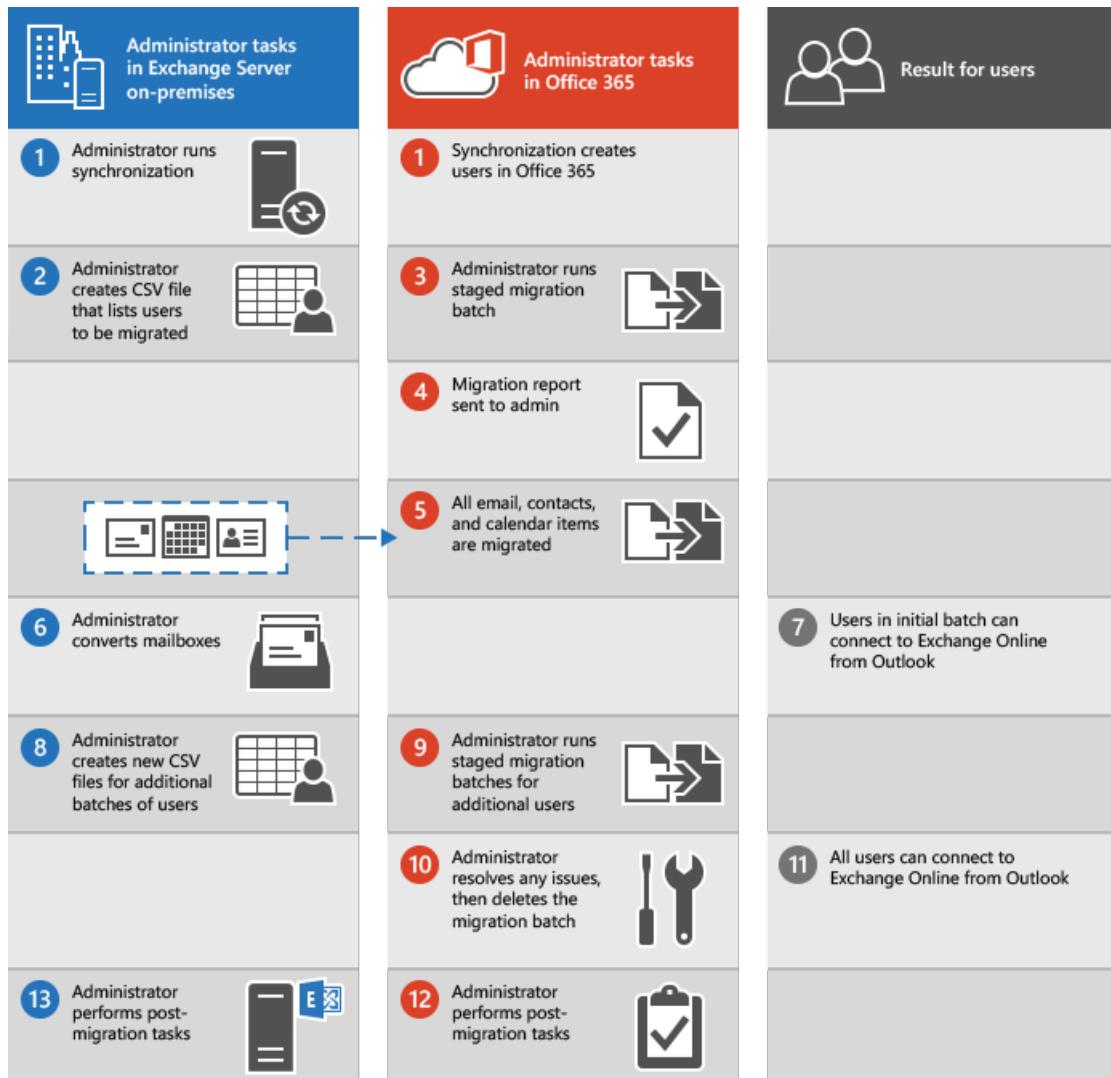
## Auswirkungen einer Migration auf Benutzer

- **Administratoren können e-Mails zugreifen:** zum Migrieren von e-Mail benötigen Sie Zugriff auf die Benutzerpostfächer in Ihrem e-Mail-System.

- **Benutzer müssen neuen Outlook-Profile erstellen:** Nachdem die Postfächer migriert werden und die lokalen Konten auf e-Mail-aktivierte Konten konvertiert werden, die Benutzer ein neues Office 365-Profil in Outlook erstellen müssen und dann Outlook automatisch eine Verbindung, Office herstellt 365.

## Wie funktioniert eine mehrstufige Migration?

Die wichtigsten Schritte, die Sie für eine mehrstufige Migration ausführen, und die Ergebnisse für die Benutzer werden in der nachstehenden Abbildung gezeigt.



Hier ist eine Beschreibung der mehrstufigen Migration aus der vorstehenden Abbildung.

- Der Administrator synchronisiert die Liste der Benutzer zwischen deren lokaler Umgebung und Office 365.  
Siehe die schrittweisen Anleitungen in [Vorbereiten auf eine mehrstufige Migration](#).
- Der Administrator erstellt eine CSV-Datei (Comma-Separated Values, durch Trennzeichen getrennte Werte), die jeweils eine Zeile für jeden Benutzer enthält, dessen lokales Postfach im Migrationsbatch migriert wird.  
Siehe die schrittweisen Anleitungen in [Erstellen einer Liste der zu migrierenden Postfächern](#).
- Der Administrator erstellt mithilfe des Migrationsdashboards im Exchange Admin Center eine mehrstufige Migration und führt sie durch.  
Siehe die schrittweisen Anleitungen in [Herstellen einer Verbindung zwischen Office 365 und Ihrem E-Mail-System](#), [Migrieren der Postfächer](#) und [Starten des mehrstufigen Migrationsbatches](#).

Nachdem der Administrator den Migrationsbatch gestartet hat, führt Exchange Online folgende Aktionen aus:

- Überprüft, ob die Verzeichnissynchronisierung aktiviert ist.
  - Überprüft, ob für jeden in der CSV-Datei aufgelisteten Benutzer ein E-Mail-aktivierter Benutzer in der Office 365-Organisation vorhanden ist. In Office 365 werden E-Mail-aktivierte Benutzer als Ergebnis der Verzeichnissynchronisierung erstellt.
  - Konvertiert den E-Mail-aktivierten Office 365-Benutzer in ein Exchange Online-Postfach für jeden Benutzer im Migrationsbatch.
  - Anfängliche Synchronisierung beginnt. Exchange Online-Prozesse bis zu migrationsanforderungen gleichzeitig  $N$ .  $N$  stellt die maximale Anzahl von gleichzeitigen Migrationen an, denen vom Administrator festgelegt, beim Erstellen des Endpunkts für den migrationsbatch verwendet. In der Standardeinstellung anfängliche Synchronisierung erfolgt auf 20 Postfächer zu einem Zeitpunkt, bis alle Postfächer im migrationsbatch migriert werden.
  - E-Mail-Weiterleitung konfiguriert. Die *TargetAddress*-Eigenschaft für das lokale Postfach wird mit der e-Mail-Adresse des Exchange Online-Postfach konfiguriert. Dies bedeutet, dass an den lokalen Postfach gesendete Nachrichten an das entsprechende Exchange Online-Postfach weitergeleitet wird.
4. Nachdem Exchange Online das Exchange Online-Postfach erstellt und die E-Mail-Weiterleitung für jeden Benutzer in der CSV-Datei konfiguriert hat, sendet es eine E-Mail-Nachricht mit dem aktuellen Status an den Administrator. In dieser Statusmeldung wird die Anzahl der erfolgreich migrierten Postfächer und die Anzahl der Postfächer aufgelistet, die nicht migriert werden konnten. Außerdem enthält die Meldung Links zu Migrationsstatistiken und Fehlerberichte mit detaillierteren Informationen. An diesem Punkt können die Benutzer mit der Verwendung ihrer Exchange Online-Postfächer beginnen.

5. Im Rahmen der Erstsynchronisierung migriert Exchange Online dann alle E-Mail-Nachrichten, Kontakte und Kalenderelemente aus den lokalen Postfächern in die Exchange Online-Postfächer. Nach Beendigung der Datenmigration sendet Exchange Online einen abschließenden Migrationsbericht.
6. Nachdem ein Migrationsbatch abgeschlossen wurde und der Administrator überprüft hat, dass alle Postfächer im Batch erfolgreich migriert wurden, kann er die lokalen Postfächer in E-Mail-aktivierte Benutzer konvertieren.

Siehe die schrittweisen Anleitungen in [Konvertieren lokaler Postfächer in E-Mail-aktivierte Benutzer, damit migrierte Benutzer auf ihre E-Mails zugreifen können](#).

7. Wenn ein Benutzer sein Postfach mit Outlook öffnet, versucht der AutoErmittlungsdienst, eine Verbindung mit dem lokalen Postfach herzustellen. Nachdem Sie lokale Postfächer in E-Mail-aktivierte Benutzer konvertiert haben, verwendet der AutoErmittlungsdienst den E-Mail-aktivierten Benutzer, um eine Verbindung zwischen Outlook und dem Exchange Online-Postfach herzustellen, nachdem der Benutzer ein neues Outlook-Profil erstellt hat.

8. Der Administrator erstellt zusätzliche Migrationsbatches und übermittelt eine CSV-Datei für jeden Batch.
9. Der Administrator führt zusätzliche Migrationsbatches aus.

10. Der Administrator löst eventuelle Probleme. Nachdem alle lokalen Postfächer in einem Migrationsbatch erfolgreich migriert wurden, löscht der Administrator den Batch.

Siehe die schrittweisen Anleitungen in [Löschen des mehrstufigen Migrationsbatches](#).

11. Die Benutzer können ihre Exchange Online-Postfächer verwenden.
12. Um den Übergang zu Exchange Online und Office 365 abzuschließen, führt der Administrator die erforderlichen Aufgaben nach der Konfiguration aus, wie beispielsweise:

- Er weist Office 365-Benutzern Lizenzen zu.
- Er konfiguriert den MX-Eintrag so, dass er auf Ihre Office 365-Organisation verweist, damit E-Mails direkt an Exchange Online-Postfächer übermittelt werden.
- Er erstellt für Ihre Office 365-Organisation einen DNS-Eintrag für AutoErmittlung.

Siehe die schrittweisen Anleitungen in [Direktes Weiterleiten von E-Mails an Office 365](#) und [Ausführen der nach der Migration erforderlichen Aufgaben](#).

Der Administrator kann die lokalen Exchange Server außer Betrieb nehmen (optional).

#### **NOTE**

Wenn Sie eine SSO-Lösung (Single Sign-on, einmaliges Anmelden) implementieren, wird dringend empfohlen, dass Sie mindestens einen Exchange Server beibehalten. Auf diese Weise können Sie auf den Exchange-System-Manager (Exchange 2003) oder die Exchange-Verwaltungskonsole/Exchange-Verwaltungsshell (Exchange 2007) zugreifen, um E-Mail-bezogene Attribute für die lokalen E-Mail-aktivierten Benutzer zu verwalten. Bei Exchange 2007 sollten auf dem Exchange Server, den Sie beibehalten, die Serverrollen "Hubtransport", "Clientzugriff" und "Postfach" installiert sein.

## Bereit zum Starten?

Wenn Sie mit dem Einrichten einer Migration nach Office 365 vertraut sind, müssen die folgenden Aufgaben ausgeführt werden:

- Synchronisieren und Erstellen Ihrer lokalen Benutzer in Office 365 mithilfe des Microsoft Azure Active Directory-Synchronisierungstools oder der Microsoft Azure Active Directory-Synchronisierungsdienste (AAD Sync)
- Konfigurieren von Exchange Server mithilfe des Exchange Admin Centers
- Ändern des MX-Eintrags Ihrer Organisation, damit nach Abschluss der Migration auf Office 365 verwiesen wird. Der MX-Eintrag gibt an, wie andere E-Mail-Systeme den Speicherort Ihres E-Mail-Systems finden können. Durch das Ändern Ihres MX-Eintrags können andere E-Mail-Systeme damit beginnen, E-Mails direkt an die neuen Postfächer in Office 365 zu senden.

Für den erfolgreichen Abschluss einer mehrstufigen E-Mail-Migration empfiehlt es sich, dass Sie mit den folgenden Aufgaben vertraut sind:

- Sie konfigurieren oder überprüfen, dass die Verzeichnissynchronisierung funktioniert.
- Sie konfigurieren Outlook Anywhere oder überprüfen, dass es funktioniert.
- Sie erstellen eine oder mehrere Listen von Postfächern zum Migrieren in Excel.
- Sie verwenden die schrittweisen Assistenten in Office 365 zum Konfigurieren und Starten des Migrationsprozesses.
- Sie fügen die DNS-Einträge Ihrer Organisation hinzu oder ändern sie, beispielsweise die AutoErmittlung- und MX-Einträge.
- Sie aktivieren lokale Postfächer für E-Mails.

Wenn Sie mit einer mehrstufigen E-Mail-Migration beginnen möchten, können Sie die Schritte ausführen, die in [Durchführen einer mehrstufigen Migration von E-Mails zu Office 365](#) angegeben sind.

## Siehe auch

Möglichkeiten zum Migrieren von E-Mail zu Office 365

Verwenden von PowerShell zum Durchführen einer mehrstufigen Migration nach Office 365

# Durchführen einer mehrstufigen Migration von E-Mails zu Office 365

18.12.2018 • 36 minutes to read

□ Sie können die Inhalte von Benutzerpostfächern aus einer Exchange 2003- oder Exchange 2007-E-Mail nach und nach anhand einer mehrstufigen Migration zu Office 365 migrieren.

Dieser Artikel führt Sie durch die Aufgaben, die mit einer mehrstufigen E-Mail-Migration in Zusammenhang stehen. [Wichtige Informationen zur mehrstufigen E-Mail-Migration zu Office 365](#) enthält eine Übersicht über den Migrationsprozess. Nachdem Sie diesen Artikel gelesen haben, können Sie anhand des vorliegenden Artikels damit beginnen, Postfächer von einem E-Mail-System zu einem anderen zu migrieren.

Windows PowerShell-Anweisungen finden Sie unter [Verwenden von PowerShell zum Durchführen einer mehrstufigen Migration zu Office 365](#).

## Migrationsaufgaben

Hier sind die Aufgaben, die Sie durchführen müssen, wenn Sie mit einer mehrstufigen Migration beginnen möchten.

1. [Vorbereiten auf eine mehrstufige Migration](#)
2. [Sicherstellen, dass Sie die Domäne besitzen](#)
3. [Verwenden der Verzeichnissynchronisierung zum Erstellen von Benutzern in Office 365](#)
4. [Erstellen einer Liste der zu migrierenden Postfächern](#)
5. [Herstellen einer Verbindung zwischen Office 365 und Ihrem E-Mail-System.](#)
6. [Migrieren der Postfächer](#)
7. [Starten des mehrstufigen Migrationsbatches](#)
8. [Konvertieren lokaler Postfächer in E-Mail-aktivierte Benutzer, damit migrierte Benutzer auf ihre E-Mails zugreifen können](#)
9. [Direktes Weiterleiten von E-Mails an Office 365](#)
10. [Löschen des mehrstufigen Migrationsbatches](#)
11. [Ausführen der nach der Migration erforderlichen Aufgaben](#)

## Vorbereiten auf eine mehrstufige Migration

Bevor Sie mithilfe einer mehrstufigen Migration Postfächer zu Office 365 migrieren, müssen Sie einige Änderungen an Ihrer Exchange Server-Umgebung vornehmen.

### So bereiten Sie eine mehrstufige Migration vor

1. **Konfigurieren von Outlook Anywhere auf Ihrem lokalen Exchange-Server:** der e-Mail-Migrationsservice Outlook Anywhere (auch bekannt als RPC über HTTP) für die Verbindung mit Ihrer lokalen Exchange-Server verwendet. Informationen dazu, wie Outlook Anywhere für Exchange 2003 und Exchange 2007 einrichten finden Sie unter den folgenden:

- Exchange 2007: Aktivieren von Outlook Anywhere
- Konfigurieren von Outlook Anywhere mit Exchange 2003

**IMPORTANT**

Sie müssen für Ihre Outlook Anywhere-Konfiguration ein Zertifikat verwenden, das von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt wurde. Outlook Anywhere kann nicht mit einem selbstsignierten Zertifikat konfiguriert werden. Weitere Informationen finden Sie unter [Konfigurieren von SSL für Outlook Anywhere](#).

2. **(Optional) überprüfen, die Sie mit der Exchange-Organisation verbinden können mithilfe von Outlook Anywhere:** Führen Sie eine der folgenden Methoden, um die Verbindungseinstellungen zu testen.
  - Verwenden Sie Outlook außerhalb Ihres Unternehmensnetzwerks zum Herstellen einer Verbindung mit dem lokalen Exchange-Postfach.
  - Verwenden Sie [Microsoft Exchange Remote Connectivity Analyzer](#) zum Testen der Verbindungseinstellungen. Verwenden Sie Tests von Outlook Anywhere (RPC über HTTP) oder Outlook-AutoErmittlung.
  - Warten Sie, bis die Verbindung automatisch getestet wird, wenn Sie die Aufgabe [Herstellen einer Verbindung zwischen Office 365 und Ihrem E-Mail-System](#) weiter unten in diesem Verfahren ausführen.
3. **Festlegen von Berechtigungen:** das lokale Benutzerkonto, mit denen Sie Ihre lokalen Exchange-Organisation (auch als dem migrationsadministrator bezeichnet) herstellen, benötigen die erforderlichen Berechtigungen für die lokale Postfächer zugreifen, die Sie migrieren möchten zu Office 365. Dieses Benutzerkonto wird verwendet, wenn Sie [eine Verbindung herstellen Office 365 auf Ihr e-Mail-System](#) weiter unten in diesem Verfahren.
4. Um die Postfächer zu migrieren, muss der Administrator über eine der folgenden Berechtigungsgruppen verfügen:
  - Ihm muss die Berechtigung " **FullAccess** " für jedes lokale Postfach und die Berechtigung " **WriteProperty** " zum Ändern der Eigenschaft " **TargetAddress** " für die lokalen Benutzerkonten zugewiesen sein.  
oder
  - Ihm muss die Berechtigung " **Receive As** " für die lokale Postfachdatenbank, in der Benutzerpostfächer gespeichert werden, und die Berechtigung " **WriteProperty** " zum Ändern der Eigenschaft " **TargetAddress** " für die lokalen Benutzerkonten zugewiesen sein.

Anweisungen zum Festlegen dieser Berechtigungen finden Sie unter [Zuweisen von Exchange-Berechtigungen zum Migrieren von Postfächern zu Office 365](#).
5. **Deaktivieren von Unified Messaging (UM):** Wenn UM eingeschaltet ist und für die lokalen Postfächer, die Sie migrieren möchten, deaktivieren Sie UM vor der Migration. Schalten Sie UM für die Postfächer nach der Migration abgeschlossen ist. Weitere Anleitungen finden Sie unter [Deaktivieren von unified messaging](#).

## Sicherstellen, dass Sie die Domäne besitzen

Während der Migration wird die SMTP-Adresse (Simple Mail Transfer Protocol) der einzelnen lokalen Postfächer verwendet, um die E-Mail-Adresse für ein neues Office 365-Postfach zu erstellen. Zum Ausführen einer mehrstufigen Migration muss überprüft werden, dass Sie der Besitzer der lokalen Domäne in Ihrer Office 365-Organisation sind.

**Verwenden des Assistenten für Domänen zum Überprüfen, dass Sie der Besitzer der lokalen Domäne**

## sind

1. Melden Sie sich bei Office 365 mit Ihrem Geschäfts, Schul- oder Unikonto an.

### NOTE

Zum Ausführen dieser Schritte müssen Sie ein globaler Administrator in Office 365 sein.

2. Wählen Sie **Setup > Domänen** aus.
3. Klicken Sie auf der Seite **Domänen verwalten** auf **Domäne hinzufügen +** um die Domäne-Assistenten zu starten.
4. Wählen Sie auf der Seite **Hinzufügen einer Domäne zu Office 365** die Option **Domänenname angeben und Besitz bestätigen** aus.
5. Geben Sie den *Domänennamen* (z. B.: Contoso.com) Sie für Ihre lokale Exchange-Organisation verwenden, und wählen Sie dann auf **Weiter**.
6. Wählen Sie auf der Seite **Bestätigen, dass Sie der rechtmäßige Besitzer von <Ihr Domänenname> sind** Ihren DNS-Hostinganbieter (Domain Name System) aus der Liste aus, oder wählen Sie **Allgemeine Anweisungen** aus (falls zutreffend).
7. Folgen Sie den Anweisungen für Ihren DNS-Hostinganbieter. In der Regel wird der TXT-Eintrag ausgewählt, um den Domänenbesitz zu überprüfen.  
Sie können auch den Anweisungen unter [Sammeln der zum Erstellen von Office 365-DNS-Einträgen erforderlichen Informationen](#) folgen, um nach dem spezifischen TXT- oder MX-Wert für Ihren Office 365-Mandanten zu suchen.  
Nachdem Sie Ihren TXT- oder MX-Eintrag hinzugefügt haben, warten Sie etwa 15 Minuten, bevor Sie mit dem nächsten Schritt fortfahren.
8. Wählen Sie im Office 365-Assistenten für Domänen die Option **Fertig, jetzt überprüfen** aus. Daraufhin sollte eine Überprüfungsseite angezeigt werden. Klicken Sie auf **Fertig stellen**.  
Wenn die Überprüfungsseite nicht angezeigt wird, warten Sie einen Moment, und versuchen Sie es dann erneut.  
Fahren Sie nicht mit dem nächsten Schritt im Assistenten für Domänen fort. Sie haben nun überprüft, dass Sie der Besitzer der lokalen Domäne der Exchange-Organisation sind, und können mit einer E-Mail-Migration fortfahren.

## Verwenden der Verzeichnissynchronisierung zum Erstellen von Benutzern in Office 365

Mit der Verzeichnissynchronisierung erstellen Sie alle lokalen Benutzer in Ihrer Office 365-Organisation.

Sie müssen den Benutzern nach dem Erstellen eine Lizenz zuweisen. Nach dem Erstellen der Benutzer haben Sie 30 Tage Zeit zum Hinzufügen von Lizenz. Schritte zum Hinzufügen von Lizenz finden Sie unter [Ausführen der nach der Migration erforderlichen Aufgaben](#).

### Erstellen neuer Benutzer

- Sie können entweder das Microsoft Azure Active Directory-Synchronisierungstool oder die Microsoft Azure Active Directory-Synchronisierungsdienste (AAD Sync) zum Synchronisieren und Erstellen der lokalen Benutzer in Office 365 verwenden. Nach der Migration von Postfächern zu Office 365, verwalten Sie Benutzerkonten in Ihrer lokalen Organisation, und diese werden mit Ihrer Office 365-Organisation

synchronisiert. Weitere Informationen finden Sie unter [Verzeichnisintegration](#).

## Erstellen einer Liste der zu migrierenden Postfächern

Nachdem Sie die Benutzer ermittelt haben, deren lokale Postfächer Sie zu Office 365 migrieren möchten, verwenden Sie eine Datei mit kommagetrennten Werten (CSV), um einen Migrationsbatch zu erstellen. Jede Zeile in der CSV-Datei (die von Office 365 zum Ausführen der Migration verwendet wird) enthält Informationen zu einem lokalen Postfach.

### NOTE

Es gibt keine Beschränkung der Anzahl von Postfächern, die Sie mit einer mehrstufigen Migration zu Office 365 migrieren können. Die CSV-Datei für einen Migrationsbatch kann maximal 2.000 Zeilen enthalten. Erstellen Sie zum Migrieren von mehr als 2.000 Postfächern zusätzliche CSV-Dateien und verwenden Sie jede Datei, um einen neuen Migrationsbatch zu erstellen.

### Unterstützte Attribute

Die CSV-Datei für eine mehrstufige Migration unterstützt die folgenden drei Attribute. Jede Zeile der CSV-Datei entspricht einem Postfach und muss einen Wert für jedes dieser Attribute enthalten.

ATTRIBUT	BESCHREIBUNG	ERFORDERLICH?
EmailAddress	Gibt die primäre SMTP-E-Mail-Adresse, z. B. "laurab@contoso.com", für lokale Postfächer an. Verwenden Sie die primäre SMTP-Adresse für lokale Postfächer und keine Benutzer-IDs aus der Office 365. Wenn die lokale Domäne beispielsweise "contoso.com" lautet, aber die Office 365-E-Mail-Domäne "service.contoso.com" benannt wurde, verwenden Sie den Domänenamen "contoso.com" für E-Mail-Adressen in der CSV-Datei.	Erforderlich
Password	Das festzulegende Kennwort für das neue Office 365 Postfach. Alle Kennworteinschränkungen, die auf die Office 365-Organisation angewendet wurden, gelten auch für die in der CSV-Datei enthaltenen Kennwörter.	Optional
ForceChangePassword	Gibt an, ob ein Benutzer das Kennwort beim ersten ändern muss, die Anmeldung bei ihren neuen Office 365-Postfach. Verwenden Sie für den Wert dieses Parameters <b>True</b> oder <b>False</b> . Beachten Sie, dass, wenn Sie eine Lösung für einmaliges Anmelden implementiert haben, durch die Bereitstellung von Active Directory-Verbunddienste (AD FS) 2.0 (AD FS 2.0) oder höher in Ihrer lokalen Organisation müssen Sie <b>False</b> für den Wert der <b>ForceChangePassword</b> verwenden Attribut.	Optional

## CSV-Dateiformat

Das folgende Beispiel zeigt das Format der CSV-Datei. In diesem Beispiel werden drei lokale Postfächer zu Office 365 migriert.

In der ersten Zeile (auch als Kopfzeile bezeichnet) der CSV-Datei sind die Namen der Attribute oder Felder aufgelistet, die in den folgenden Zeilen angegeben werden. Die einzelnen Attributnamen werden jeweils durch ein Komma getrennt.

```
EmailAddress,Password,ForceChangePassword  
pilarp@contoso.com,Pa$$w0rd,False  
tobyn@contoso.com,Pa$$w0rd,False  
briant@contoso.com,Pa$$w0rd,False
```

Die Zeilen unter der Kopfzeile stellen einen Benutzer dar und enthalten die Informationen, die zum Migrieren des Postfachs des Benutzers verwendet werden. Die Attributwerte in jeder einzelnen Zeile müssen die gleiche Reihenfolge aufweisen wie die Attributnamen in der Kopfzeile.

Verwenden Sie einen beliebigen Texteditor oder eine Anwendung wie Excel, um die CSV-Datei zu erstellen. Speichern Sie die Datei als CSV- oder TXT-Datei.

### NOTE

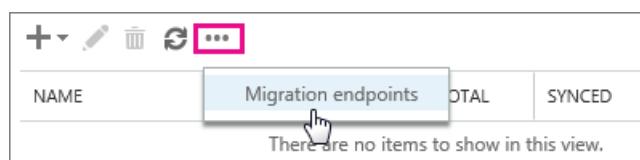
Wenn die CSV-Datei ASCII-fremde Zeichen oder Sonderzeichen enthält, speichern Sie die CSV-Datei mit UTF-8 oder einer anderen Unicode-Codierung. Je nach Anwendung kann es einfacher sein, die CSV-Datei mit UTF-8 oder einer anderen Unicode-Codierung zu speichern, wenn das Systemgebietsschema des Computers mit der in der CSV-Datei verwendeten Sprache übereinstimmt.

## Herstellen einer Verbindung zwischen Office 365 und Ihrem E-Mail-System.

Ein Migrationsendpunkt enthält die Einstellungen und Anmeldeinformationen, die erforderlich sind, um eine Verbindung mit dem lokalen Server herzustellen, der die Postfächer hostet, Sie sind mit Office 365 migrieren. Für eine mehrstufige Migration erstellen Sie einen Outlook Anywhere-Migrationsendpunkt. Es wird ein einzelner Migrationsendpunkt für alle Ihre Migrationsbatches erstellt.

### So erstellen Sie einen Migrationsendpunkt

1. Wechseln Sie zum Exchange Admin Center.
2. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.
3. Wählen Sie **Weitere ... > migrationsendpunkte**.

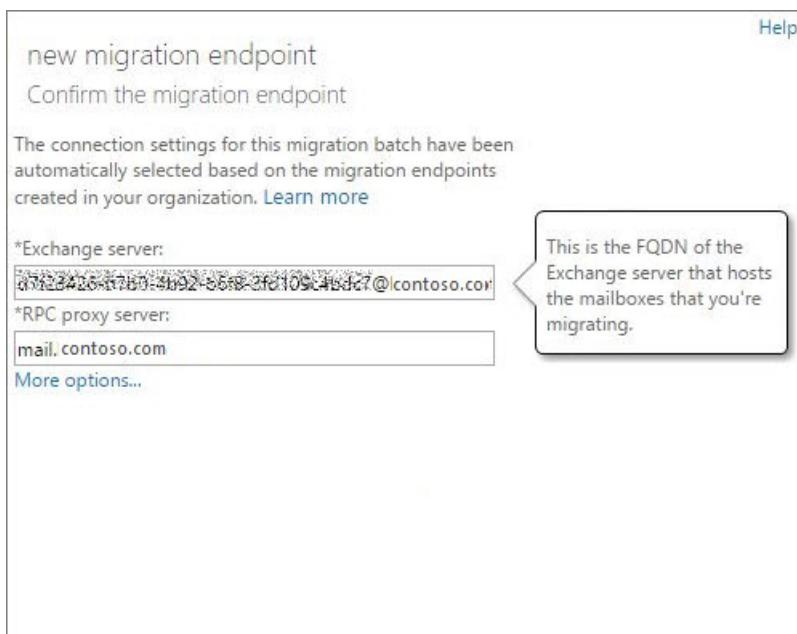


4. Wählen Sie auf der Seite **migrationsendpunkte neu +**.
5. Wählen Sie auf der Seite **Typ des Migrationsendpunkts auswählen** die Option **Outlook Anywhere > Weiter** aus.
6. Geben Sie auf der Seite **Anmeldeinformationen für lokales Konto eingeben** folgende Informationen ein:

- **E-Mail-Adresse:** Geben Sie die *e-Mail-Adresse* eines Benutzers in der lokalen Exchange-Organisation, die migriert werden. Office 365 wird die Konnektivität für Postfach des Benutzers zu testen.
- **Konto mit Berechtigungen:** Geben Sie den *Benutzernamen* (Format Domäne\Benutzername ein oder eine e-Mail-Adresse) für ein Konto, das in der lokalen Organisation die erforderlichen administrativen Berechtigungen verfügt. Office 365 wird dieses Konto verwenden, um den migrationsendpunkt zu erkennen und die Berechtigungen für dieses Konto durch den Versuch, Zugriff auf das Postfach mit der angegebenen e-Mail-Adresse zu testen.
- **Das Kennwort des Kontos mit Berechtigungen:** Geben Sie das *Kennwort* für das Konto mit Berechtigungen, die das Administratorkonto handelt.

7. Wählen Sie **Weiter** aus, und führen Sie dann eine der folgenden Aktionen aus:

- Wenn Office 365 erfolgreich eine Verbindung mit dem Quellserver herstellt, werden die Verbindungseinstellungen angezeigt. Wählen Sie **Weiter** aus.



- Wenn die Testverbindung mit dem Quellserver nicht erfolgreich ist, geben Sie die folgenden Informationen ein:
- **Exchange Server:** Geben Sie den *vollqualifizierten Domänennamen* (FQDN) für den lokalen Exchange-Server. Dies ist der Hostname für Ihre Postfachserver, beispielsweise EXCH-SRV-01.corp.contoso.com.
- **RPC-Proxyserver:** Geben Sie den *FQDN* für den RPC-Proxyserver für Outlook Anywhere. In der Regel ist der Proxyserver identisch mit der Outlook Web App-URL. Mail.contoso.com, also auch die URL für den Proxy-Server, die Outlook verwendet, um die Verbindung mit einem Exchange-Server

8. Geben Sie auf der Seite **Allgemeine Informationen eingeben** einen *migrationsendpunktnamen ein*, beispielsweise Test5-Endpunkt. Lassen Sie die beiden anderen Felder leer, verwenden Sie die Standardwerte.

Help

**new migration endpoint**

Enter general information

Enter the value for the general information for the migration endpoint that'll be applied to the associated migrations. [Learn more](#)

\*Migration endpoint name:

Maximum concurrent migrations:

Maximum concurrent incremental syncs:

[back](#) [new](#) [cancel](#)

9. Wählen Sie **Neu** aus, um den Migrationsendpunkt zu erstellen.

Zum Überprüfen, ob Ihr Exchange Online mit dem lokalen Server verbunden ist, führen Sie den Befehl in Beispiel 4 von [Test-MigrationServerAvailability](#) aus.

## Migrieren der Postfächer

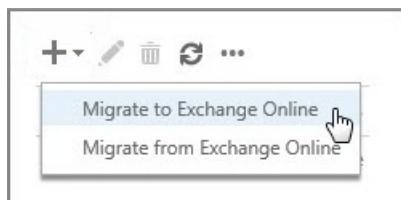
Sie erstellen einen Migrationsbatch und führen diesen dann aus, um Postfächer zu Office 365 zu migrieren.

### Erstellen eines mehrstufigen Migrationsbatches

Bei einer mehrstufigen Migration migrieren Sie Postfächer in Batches - einen Batch für jede von Ihnen erstellte CSV-Datei.

### So erstellen Sie einen mehrstufigen Migrationsbatch

1. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.
2. Wählen Sie **neu + > zu Exchange Online migrieren**.



3. Wählen Sie auf der Seite **Wählen Sie eine Migration Mehrstufige Migration > Weiter**.

4. Wählen Sie auf der Seite **Benutzer auswählen** die Option **Durchsuchen** aus, und wählen Sie dann die CSV-Datei aus, die für diesen Migrationsbatch verwendet werden soll.

Nachdem Sie eine CSV-Datei ausgewählt haben, prüft Office 365 die Datei, um Folgendes sicherzustellen:

- Die Datei ist nicht leer.
- Sie ist mit Kommas als Trennzeichen formatiert.
- Sie enthält nicht mehr als 2.000 Zeilen.
- Sie enthält die erforderliche Spalte "**EmailAddress**" in der Überschriftenzeile.
- Alle Zeilen weisen dieselbe Anzahl von Spalten wie die Überschriftenzeile auf.

Tritt bei einer dieser Prüfungen ein Fehler auf, wird eine Fehlermeldung angezeigt, in der der Grund für

den Fehler beschrieben ist. An diesem Punkt müssen Sie alle Fehler in der CSV-Datei beheben und sie erneut übermitteln, um einen Migrationsbatch zu erstellen. Nach der Überprüfung der CSV-Datei wird die Anzahl der Benutzer, die in der CSV-Datei aufgelistet sind, als die Anzahl der zu migrierenden Postfächer angezeigt.

5. Wählen Sie **Weiter** aus.
6. Prüfen Sie auf der Seite **Migrationsendpunkt bestätigen** die aufgeführten Migrationsendpunktinformationen, und wählen Sie dann **Weiter** aus.



7. Geben Sie auf der Seite **Konfiguration verschieben** den Namen (keine Leerzeichen oder Sonderzeichen) des Migrationsbatches ein, und wählen Sie dann **Weiter** aus. Dieser Name wird in der Liste der Migrationsbatches auf der Seite **Migration** angezeigt, nachdem Sie den Migrationsbatch erstellt haben.
8. Wählen Sie auf der Seite **Batch starten** eine der folgenden Optionen aus:
  - **Starten Sie den Batch automatisch:** der migrationsbatch gestartet wird, sobald Sie den neuen migrationsbatch gespeichert. Der Batch beginnt mit dem Status **synchronisiert**.
  - **Starten Sie den Batch später manuell:** der migrationsbatch erstellt, jedoch noch nicht gestartet. Der Status des Stapels wird auf **erstellt** festgelegt. Um einen migrationsbatch zu starten, wählen Sie sie im migrationsdashboard, und wählen Sie dann auf **Starten**.

#### 9. Wählen Sie **Neu** aus, um den Migrationsbatch zu erstellen.

Der neue Migrationsbatch wird auf dem Migrationsdashboard angezeigt.

#### **Starten des mehrstufigen Migrationsbatches**

Wenn Sie einen Migrationsbatch erstellt und so konfiguriert haben, dass er manuell gestartet werden muss, können Sie ihn über das Exchange Admin Center starten.

#### **So starten Sie einen mehrstufigen Migrationsbatch**

1. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.
2. Wählen Sie auf dem Migrationsdashboard den Batch aus, und wählen Sie dann **Starten** aus.
3. Wurde ein Migrationsbatch erfolgreich gestartet, wird dessen Status auf dem Migrationsdashboard in **Synchronisierung** geändert.

Click to view the status for all current migration batches. <a href="#">Status for all batches</a>					
NAME	▲ STATUS	TOTAL	SYNCED	FINALIZED	FAILED
Test5-migration	Syncing	5	0	0	0
Status changes from Created to Syncing after the migration starts.					

## Überprüfen, ob der Migrationsschritt erfolgreich war

Sie können den Synchronisationsstatus auf dem Migrationsdashboard verfolgen. Wenn ein Problem auftritt, können Sie eine Protokolldatei anzeigen, in der Sie weitere Informationen zu den Fehlern finden.

Sie können im Office 365 Admin Center auch überprüfen, ob die Benutzer erstellt werden, während die Migration fortschreitet.

## Konvertieren lokaler Postfächer in E-Mail-aktivierte Benutzer, damit migrierte Benutzer auf ihre E-Mails zugreifen können

Nachdem Sie einen Batch Postfächer erfolgreich migriert haben, benötigen Sie eine Methode, damit die Benutzer auf ihre E-Mail zugreifen können. Ein Benutzer, dessen Postfach migriert wurden, hat jetzt sowohl ein lokales Postfach als auch eins in Office 365. Benutzer mit einem Postfach in Office 365, werden keine neuen E-Mail-Nachrichten in ihrem lokalen Postfach empfangen.

Da die Migration noch nicht abgeschlossen ist, können Sie noch nicht alle Benutzer für ihre E-Mails an Office 365 weiterleiten. Was also tun Sie für diese Personen, die beide haben? Sie können die lokalen Postfächer ändern, die Sie bereits zu E-Mail-aktivierte Benutzer migriert haben. Wenn Sie von einem Postfach zu einem E-Mail-aktivierten Benutzer wechseln, können Sie den Benutzer für seine E-Mails anstatt zu seinem lokalen Postfach an Office 365 weiterleiten.

Ein weiterer wichtiger Grund dafür, lokale Postfächer in E-Mail-aktivierte Benutzer zu konvertieren, ist die Beibehaltung von Proxyadressen der Exchange Online-Postfächer, indem Proxyadressen in die E-Mail-aktivierten Benutzer kopiert werden. Auf diese Weise können Sie cloudbasierte Benutzer aus Ihrer lokalen Organisation mithilfe von Active Directory verwalten. Wenn Sie sich entscheiden, Ihre lokale Exchange-Organisation, außer Betrieb zu nehmen, nachdem alle Postfächer zu Exchange Online migriert wurden, verbleiben die Proxyadressen, die Sie in die E-Mail-aktivierten Benutzer kopiert haben, in Ihrem lokalen Active Directory.

Weitere Informationen finden Sie unter den folgenden Themen. Dort stehen auch Skripts zum Download bereit, die Sie zum Konvertieren von Postfächern in E-Mail-aktivierte Benutzer ausführen können:

- [Konvertieren von Exchange 2007-Postfächern in E-Mail-aktivierte Benutzer](#)
- [Konvertieren von Exchange 2003-Postfächern in E-Mail-aktivierte Benutzer](#)

## Optional: Wiederholen der Migrationsschritte

Sie können Batches gleichzeitig oder einzeln nacheinander ausführen. Gehen Sie so vor, dass es Ihrem Zeitplan entspricht und Sie Personen beim Durchführen der Migration unterstützen können. Beachten Sie, dass jeder Migrationsbatch maximal 2.000 Postfächer umfassen kann.

Nachdem Sie alle Benutzer zu Office 365 migriert haben, können E-Mails direkt an Office 365 gesendet werden, und Sie können Ihr altes E-Mail-System außer Betrieb nehmen.

## Optional: Verringern von E-Mail-Verzögerungen

Diese Aufgabe müssen Sie nicht durchführen, doch wenn Sie sie überspringen, kann es etwas länger dauern, bis E-Mails in den neuen Office 365-Postfächern angezeigt werden.

Wenn Personen, die nicht zu Ihrer Organisation gehören, E-Mails an Sie senden, wird von den E-Mail-Systemen dieser Personen nicht jedes Mal geprüft, wohin die E-Mails gesendet werden sollen. Stattdessen speichern diese Systeme den Speicherort Ihres E-Mail-Systems anhand einer Einstellung in Ihrem DNS-Server, die als Gültigkeitsdauer (Time-to-live, TTL) bezeichnet wird. Wenn Sie den Speicherort Ihres E-Mail-Systems ändern, bevor die TTL abgelaufen ist, wird zuerst versucht, Ihnen E-Mails an den alten Speicherort zu senden, bevor festgestellt wird, dass sich der Speicherort geändert hat. Dies kann zu einer Verzögerung in der E-Mail-Zustellung führen. Eine Möglichkeit, dies zu vermeiden, besteht darin, den TTL-Wert zu verringern, den Ihr DNS-Server bereitstellt, der nicht zu Ihrer Organisation gehören. Dadurch werden die anderen Organisationen veranlasst, den Speicherort Ihres E-Mail-Systems häufiger zu aktualisieren.

Die Verwendung eines kurzen Intervalls, z. B. 3.600 Sekunden (eine Stunde) oder weniger, bedeutet, dass die meisten E-Mail-Systeme jede Stunde einen aktualisierten Speicherort anfordern. Es wird empfohlen, dass Sie das Intervall mindestens auf diesen niedrigen Wert festlegen, bevor Sie die E-Mail-Migration starten. Dies bietet allen Systemen, die E-Mails an Sie senden, genügend Zeit, die Änderung zu verarbeiten. Wenn Sie dann den endgültigen Umstieg auf Office 365 vorgenommen haben, können Sie den TTL-Wert wieder in ein längeres Intervall ändern.

*So ändern Sie die Einstellung TTL die Stelle auf Ihr e-Mail-System Mail Exchanger-Eintrag, auch als einen MX-Eintrag bezeichnet wird.* Dies befindet sich in Ihrem öffentlichen internetbasierte DNS-System. Wenn Sie mehr als einen MX-Datensatz verfügen, müssen Sie den Wert für jeden Datensatz auf 3.600 oder weniger zu ändern.

Wenn Sie einige Hilfe benötigen Ihre DNS-Einstellungen konfigurieren, lesen Sie unsere [Erstellen von DNS-Datensätze an alle DNS-Hostinganbieter für Office 365](#).

## Direktes Weiterleiten von E-Mails an Office 365

E-Mail-Systeme verwenden einen als MX-Eintrag bezeichneten DNS-Eintrag, um zu ermitteln, wohin E-Mails gesendet werden sollen. Während der E-Mail-Migration hat Ihr MX-Eintrag auf Ihr lokales E-Mail-System verwiesen. Nachdem die E-Mail-Migration zu Office 365 nun für alle Benutzer abgeschlossen ist, sollte Ihr MX-Eintrag auf Office 365 verweisen. Dadurch kann sichergestellt werden, dass eingehende E-Mails an Ihre Office 365-Postfächer gesendet werden. Das Verschieben des MX-Eintrags ermöglicht es Ihnen außerdem, das alte E-Mail-System zu deaktivieren, wenn Sie fertig sind.

Für viele DNS-Anbieter haben wir [Erstellen von DNS-Datensätze an alle DNS-Hostinganbieter für Office 365](#). Wenn es sich bei Ihrem DNS-Anbieter nicht mit inbegriffen, oder Sie die allgemeinen Anweisungen einen Eindruck davon erhalten möchten, haben wir sowie [Allgemeine MX-Eintrag Anweisungen](#) bereitgestellt.

Es kann bis zu 72 Stunden dauern, bis die E-Mail-Systeme Ihrer Kunden und Partner den geänderten MX-Eintrag erkannt haben. Warten Sie mindestens 72 Stunden, bevor Sie beginnen, die nächste Aufgabe auszuführen.

## Löschen des mehrstufigen Migrationsbatches

Nachdem Sie den MX-Eintrag geändert und sich vergewissert haben, dass alle E-Mails an Office 365-Postfächer weitergeleitet werden, können Sie die mehrstufigen Migrationsbatches löschen. Überprüfen Sie Folgendes, bevor Sie einen Migrationsbatch löschen:

- Alle Benutzer im Batch verwenden ihre Office 365-Postfächer. Nachdem der Batch gelöscht ist, werden E-Mails, die an Postfächer auf dem lokalen Exchange Server gesendet wurden, nicht in die entsprechenden Office 365-Postfächer kopiert.
- Office 365-Postfächer wurden mindestens einmal synchronisiert seit dem Zeitpunkt, ab dem E-Mails direkt an sie gesendet werden. Vergewissern Sie sich dazu, dass der Wert im Feld **Zeit der letzten**

**Synchronisierung** für den Migrationsbatch einen neueren Zeitpunkt angibt als der Zeitpunkt, ab dem E-Mails direkt an Office 365-Postfächer weitergeleitet werden.

Wenn Sie einen mehrstufigen Migrationsbatch löschen, bereinigt der Migrationsdienst alle Einträge, die mit dem Migrationsbatch zu tun haben, und löscht dann den Migrationsbatch. Der Batch wird auf dem Migrationsdashboard aus der Liste der Migrationsbatches entfernt.

### **So löschen Sie den mehrstufigen Migrationsbatch**

1. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.
2. Wählen Sie auf dem Migrationsdashboard den Batch aus, und wählen Sie dann **Löschen** aus.  
Es kann einige Minuten dauern, bis der Batch gelöscht wurde.
3. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.
4. Vergewissern Sie sich, dass der Migrationsbatch nicht mehr auf dem Migrationsdashboard aufgeführt wird.

## Ausführen der nach der Migration erforderlichen Aufgaben

Nach dem Migrieren von Postfächern zu Office 365 gibt es migrationsbezogene Aufgaben, die ausgeführt werden müssen.

### **So führen Sie die nach der Migration erforderlichen Aufgaben aus**

1. **Aktivieren von Office 365-Benutzerkonten für die migrierten Konten durch Zuweisen von Lizenzen:** Wenn Sie keine Lizenz zuweisen, wird das Postfach deaktiviert, wenn die Kulanzfrist (30 Tage) endet. Zuweisen, indem Sie eine Lizenz im Office 365 Administrationscenter finden Sie unter [Zuweisen von Lizenzen für Benutzer in Office 365 für Unternehmen](#).
2. **Erstellen Sie einen AutoErmittlung-DNS-Eintrag, sodass Benutzer auf einfache Weise auf ihre Postfächer zugreifen können:** Nachdem alle lokalen Postfächern zu Office 365 migriert wurden, können Sie einen Autodiscover DNS-Eintrag für Ihre Office 365-Organisation so aktivieren Sie Benutzer für die Verbindung auf einfache Weise konfigurieren Ihre neuen Office 365-Postfächer mit Outlook und mobile Clients. Diese neuen Autodiscover DNS-Eintrag muss den gleichen Namespace verwendet, den Sie für Ihre Office 365-Organisation verwenden. Beispielsweise ist Ihre Cloud-basierten Namespace `cloud.contoso.com`, dem Autodiscover DNS-Eintrag, den Sie erstellen müssen `autodiscover.cloud.contoso.com`.

Office 365 verwendet einen CNAME-Eintrag, um den AutoErmittlungsdienst für Outlook und mobile Clients zu implementieren. Der AutoErmittlung-CNAME-Eintrag muss die folgenden Informationen enthalten:

- **Alias:**autodiscover
- **Ziel:** autodiscover.outlook.com

Weitere Informationen finden Sie unter [Create DNS records for Office 365 when you manage your DNS records](#).

3. **Nehmen lokalen Exchange-Servers:** Nachdem Sie sichergestellt haben, dass alle e-Mails direkt an die Office 365-Postfächer weitergeleitet werden, die Migration ausgeführt haben, und verwalten Sie Ihre lokale e-Mail-Organisation, die Sie deinstallieren können nicht mehr benötigen. Exchange.

Weitere Informationen hierzu finden Sie unter folgenden Themen:

- [Entfernen einer Exchange 2007-Organisation](#)

- Deinstallieren von Exchange Server 2003

**NOTE**

Eine Außerbetriebnahme von Exchange kann unerwartete Folgen haben. Vor der Außerbetriebnahme Ihrer lokalen Exchange-Organisation sollten Sie Kontakt mit dem Microsoft-Support aufnehmen.

## Siehe auch

[Wichtige Informationen zur mehrstufigen E-Mail-Migration zu Office 365](#)

[Möglichkeiten zum Migrieren von E-Mail zu Office 365](#)

# Konvertieren von Exchange 2007-Postfächern in E-Mail-aktivierte Benutzer

18.12.2018 • 11 minutes to read

[] Nachdem Sie eine mehrstufige Migration abgeschlossen haben, konvertieren Sie die Postfächer in E-Mail-aktivierte Benutzer, damit die Postfächer automatisch eine Verbindung mit dem Cloudpostfach herstellen können.

## Gründe zum Konvertieren von Postfächern in E-Mail-aktivierte Benutzer

Wenn Sie eine mehrstufige Exchange-Migration zum Migrieren Ihrer lokalen Exchange 2007-Postfächer Ihrer Organisation zu Office 365 abgeschlossen haben, und Sie cloudbasierte Benutzer der lokalen Organisation mithilfe von Active Directory verwalten möchten, sollten Sie die lokalen Postfächer in E-Mail-aktivierte Benutzer konvertieren. Warum? Zwei Dinge geschehen, nachdem ein Postfach bei einer mehrstufigen Exchange-Migration in die Cloud migriert wurde:

- Ein Benutzer verfügt über ein lokales Postfach und ein Cloudpostfach.
- An das lokale Postfach des Benutzers gesendete E-Mails werden an sein Cloudpostfach weitergeleitet. Dies geschieht, da während der Migration die **TargetAddress** -Eigenschaft für das lokale Postfach mit der Remoteroutingadresse des Cloudpostfachs gefüllt wird. Dies bedeutet, dass Benutzer eine Verbindung mit ihren Cloudpostfächern herstellen müssen, um auf ihre E-Mails zugreifen zu können.

Dieses Verhalten führt zu zwei Problemen:

- Wenn eine Person Microsoft Outlook zum Öffnen ihres Postfachs verwendet, versucht der AutoErmittlungsdienst weiterhin, eine Verbindung mit dem lokalen Postfach herzustellen. Der Benutzer ist dann nicht in der Lage, eine Verbindung mit seinem Cloudpostfach herzustellen. Wenn Benutzer vorhanden sind, die noch nicht in die Cloud migriert wurden, können Sie mit dem CNAME-Eintrag der AutoErmittlung nicht auf die Cloud verweisen, bis alle Benutzer migriert werden.
- Wenn eine Organisation Exchange nach der Migration aller lokalen Postfächer in die Cloud außer Betrieb setzt, gehen nachrichtenbezogene Benutzerinformationen für das Cloudpostfach verloren. Das Microsoft Online Services-Verzeichnissynchronisierungstool (DirSync) entfernt Daten (z. B. Proxyadressen) aus dem Cloudpostfachobjekt, da das lokale Postfach nicht mehr vorhanden ist und es von DirSync nicht mit dem entsprechenden Cloudpostfach verglichen werden kann.

Die Lösung besteht darin, das lokale Postfach in einen E-Mail-aktivierten Benutzer in Ihrer lokalen Organisation zu konvertieren, nachdem das Postfach des Benutzers in die Cloud migriert wurde. Wenn Sie ein lokales Postfach in einen E-Mail-aktivierten Benutzer konvertieren:

- Die Proxyadressen eines cloudbasierten Postfachs werden in den neuen E-Mail-aktivierten Benutzer kopiert. Wenn Sie Exchange außer Betrieb nehmen, bleiben diese Proxyadressen in Active Directory weiterhin erhalten.
- Die Eigenschaften des E-Mail-aktivierten Benutzers ermöglichen es DirSync, den E-Mail-aktivierten Benutzer mit seinem entsprechenden Cloudpostfach zu vergleichen.
- Der AutoErmittlungsdienst verwendet den E-Mail-aktivierten Benutzer, um Outlook mit dem Cloudpostfach zu verbinden, nachdem der Benutzer ein neues Outlook-Profil erstellt hat.

# PowerShell-Skripts zum Erstellen E-Mail-aktivierter Benutzer

Sie können die nachfolgenden Skripts zum Erfassen von Informationen zu den cloudbasierten Postfächern und zum Konvertieren der Exchange 2007-Postfächer in E-Mail-aktivierte Benutzer verwenden.

Das folgende Skript erfasst Informationen aus Ihren Cloudpostfächern und speichert sie in einer CSV-Datei. Führen Sie dieses Skript zuerst aus.

Kopieren Sie das nachfolgende Skript, und weisen Sie ihm den Dateinamen "ExportO365UserInfo.ps1" zu.

```
Param($migrationCSVFileName = "migration.csv")
function O365Logon
{
    #Check for current open 0365 sessions and allow the admin to either use the existing session or create a new one
    $session = Get-PSSession | ?{$_.ConfigurationName -eq 'Microsoft.Exchange'}
    if($session -ne $null)
    {
        $a = Read-Host "An open session to Office 365 already exists. Do you want to use this session? Enter y to use the open session, anything else to close and open a fresh session."
        if($a.ToLower() -eq 'y')
        {
            Write-Host "Using existing Office 365 Powershell Session." -ForegroundColor Green
            return
        }
        $session | Remove-PSSession
    }
    Write-Host "Please enter your Office 365 credentials" -ForegroundColor Green
    $cred = Get-Credential
    $s = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com/powershell -Credential $cred -Authentication Basic -AllowRedirection
    $importresults = Import-PSSession -Prefix "Cloud" $s
}
function Main
{
    #Verify the migration CSV file exists
    if(!(Test-Path $migrationCSVFileName))
    {
        Write-Host "File $migrationCSVFileName does not exist." -ForegroundColor Red
        Exit
    }

    #Import user list from migration.csv file
    $MigrationCSV = Import-Csv $migrationCSVFileName

    #Get mailbox list based on email addresses from CSV file
    $MailBoxList = $MigrationCSV | %{$_.EmailAddress} | Get-CloudMailbox
    $Users = @()
    #Get LegacyDN, Tenant, and On-Premise Email addresses for the users
    foreach($user in $MailBoxList)
    {
        $UserInfo = New-Object System.Object

        $CloudEmailAddress = $user.EmailAddresses | ?{($_ -match 'onmicrosoft') -and ($_. -cmatch 'smtp:')}
        if ($CloudEmailAddress.Count -gt 1)
        {
            $CloudEmailAddress = $CloudEmailAddress[0].ToString().ToLower().Replace('smtp:', '')
            Write-Host "$user returned more than one cloud email address. Using $CloudEmailAddress" -ForegroundColor Yellow
        }
        else
        {
            $CloudEmailAddress = $CloudEmailAddress.ToString().ToLower().Replace('smtp:', '')
        }

        $UserInfo | Add-Member -Type NoteProperty -Name LegacyExchangeDN -Value $user.LegacyExchangeDN
        $UserInfo | Add-Member -Type NoteProperty -Name CloudEmailAddress -Value $CloudEmailAddress
    }
}
```

```

$UserInfo | Add-Member -Type NoteProperty -Name CloudEmailAddress -Value $CloudEmailAddress
$UserInfo | Add-Member -Type NoteProperty -Name OnPremiseEmailAddress -Value $user.PrimarySMTPAddress.ToString()
$UserInfo | Add-Member -Type NoteProperty -Name MailboxGUID -Value $user.ExchangeGUID
$Users += $UserInfo
}
#Check for existing csv file and overwrite if needed
if(Test-Path ".\cloud.csv")
{
    $delete = Read-Host "The file cloud.csv already exists in the current directory. Do you want to delete it? Enter y to delete, anything else to exit this script."
    if($delete.ToString().ToLower() -eq 'y')
    {
        Write-Host "Deleting existing cloud.csv file" -ForegroundColor Red
        Remove-Item ".\cloud.csv"
    }
    else
    {
        Write-Host "Will NOT delete current cloud.csv file. Exiting script." -ForegroundColor Green
        Exit
    }
}
$Users | Export-Csv -Path ".\cloud.csv" -notype
(Get-Content ".\cloud.csv") | %{$_.Replace("'", '')} | Set-Content ".\cloud.csv" -Encoding Unicode
Write-Host "CSV File Successfully Exported to cloud.csv" -ForegroundColor Green
}
0365Logon
Main

```

Das folgende Skript konvertiert lokale Exchange 2007-Postfächer in E-Mail-aktivierte Benutzer. Führen Sie dieses Skript aus, nachdem Sie das Skript zum Erfassen von Informationen aus den Cloudbenutzern ausgeführt haben.

Kopieren Sie das folgende Skript in eine TXT-Datei, und speichern Sie die Datei dann unter "Exchange2007MBtoMEU.ps1".

```

param($DomainController = [String]::Empty)
function Main
{
    #Script Logic flow
    #1. Pull User Info from cloud.csv file in the current directory
    #2. Lookup AD Info (DN, mail, proxyAddresses, and legacyExchangeDN) using the SMTP address from the CSV file
    #3. Save existing proxyAddresses
    #4. Add existing legacyExchangeDN's to proxyAddresses
    #5. Delete Mailbox
    #6. Mail-Enable the user using the cloud email address as the targetAddress
    #7. Disable RUS processing
    #8. Add proxyAddresses and mail attribute back to the object
    #9. Add msExchMailboxGUID from cloud.csv to the user object (for offboarding support)

    if($DomainController -eq [String]::Empty)
    {
        Write-Host "You must supply a value for the -DomainController switch" -ForegroundColor Red
        Exit
    }

    $CSVInfo = Import-Csv ".\cloud.csv"
    foreach($User in $CSVInfo)
    {
        Write-Host "Processing user" $User.OnPremiseEmailAddress -ForegroundColor Green
        Write-Host "Calling LookupADInformationFromSMTPAddress" -ForegroundColor Green
        $UserInfo = LookupADInformationFromSMTPAddress($User)

        #Check existing proxies for On-Premise and Cloud Legacy DN's as x500 proxies. If not present add them.
        $CloudLegacyDNPresent = $false
        $LegacyDNPresent = $false
    }
}

```

```

foreach($Proxy in $UserInfo.ProxyAddresses)
{
    if(("x500:$UserInfo.CloudLegacyDN") -ieq $Proxy)
    {
        $CloudLegacyDNPresent = $true
    }
    if(("x500:$UserInfo.LegacyDN") -ieq $Proxy)
    {
        $LegacyDNPresent = $true
    }
}
if(-not $CloudLegacyDNPresent)
{
    $X500Proxy = "x500:" + $UserInfo.CloudLegacyDN
    Write-Host "Adding $X500Proxy to EmailAddresses" -ForegroundColor Green
    $UserInfo.ProxyAddresses += $X500Proxy
}
if(-not $LegacyDNPresent)
{
    $X500Proxy = "x500:" + $UserInfo.LegacyDN
    Write-Host "Adding $X500Proxy to EmailAddresses" -ForegroundColor Green
    $UserInfo.ProxyAddresses += $X500Proxy
}

#Disable Mailbox
Write-Host "Disabling Mailbox" -ForegroundColor Green
Disable-Mailbox -Identity $UserInfo.OnPremiseEmailAddress -DomainController $DomainController -Confirm:$false

#Mail Enable
Write-Host "Enabling Mailbox" -ForegroundColor Green
Enable-MailUser -Identity $UserInfo.Identity -ExternalEmailAddress $UserInfo.CloudEmailAddress -DomainController $DomainController

#Disable RUS
Write-Host "Disabling RUS" -ForegroundColor Green
Set-MailUser -Identity $UserInfo.Identity -EmailAddressPolicyEnabled $false -DomainController $DomainController

#Add Proxies and Mail
Write-Host "Adding EmailAddresses and WindowsEmailAddress" -ForegroundColor Green
Set-MailUser -Identity $UserInfo.Identity -EmailAddresses $UserInfo.ProxyAddresses -WindowsEmailAddress $UserInfo.Mail -DomainController $DomainController

#Set Mailbox GUID. Need to do this via S.DS as Set-MailUser doesn't expose this property.
$ADPath = "LDAP://" + $DomainController + "/" + $UserInfo.DistinguishedName
$ADUser = New-Object -TypeName System.DirectoryServices.DirectoryEntry -ArgumentList $ADPath
$MailboxGUID = New-Object -TypeName System.Guid -ArgumentList $UserInfo.MailboxGUID
[Void]$ADUser.psbase.invokeSet('msExchMailboxGUID',$MailboxGUID.ToByteArray())
Write-Host "Setting Mailbox GUID" $UserInfo.MailboxGUID -ForegroundColor Green
$ADUser.psbase.CommitChanges()

Write-Host "Migration Complete for" $UserInfo.OnPremiseEmailAddress -ForegroundColor Green
Write-Host ""
Write-Host ""
}

}

function LookupADInformationFromSMTPAddress($CSV)
{
    $Mailbox = Get-Mailbox $CSV.OnPremiseEmailAddress -ErrorAction SilentlyContinue

    if($Mailbox -eq $null)
    {
        Write-Host "Get-Mailbox failed for" $CSV.OnPremiseEmailAddress -ForegroundColor Red
        continue
    }

    $UserInfo = New-Object System.Object

```

```

$UserInfo | Add-Member -Type NoteProperty -Name OnPremiseEmailAddress -Value $CSV.OnPremiseEmailAddress
$UserInfo | Add-Member -Type NoteProperty -Name CloudEmailAddress -Value $CSV.CloudEmailAddress
$UserInfo | Add-Member -Type NoteProperty -Name CloudLegacyDN -Value $CSV.LegacyExchangeDN
$UserInfo | Add-Member -Type NoteProperty -Name LegacyDN -Value $Mailbox.LegacyExchangeDN
$ProxyAddresses = @()
foreach($Address in $Mailbox.EmailAddresses)
{
    $ProxyAddresses += $Address
}
$UserInfo | Add-Member -Type NoteProperty -Name ProxyAddresses -Value $ProxyAddresses
$UserInfo | Add-Member -Type NoteProperty -Name Mail -Value $Mailbox.WindowsEmailAddress
$UserInfo | Add-Member -Type NoteProperty -Name MailboxGUID -Value $CSV.MailboxGUID
$UserInfo | Add-Member -Type NoteProperty -Name Identity -Value $Mailbox.Identity
$UserInfo | Add-Member -Type NoteProperty -Name DistinguishedName -Value (Get-User
$Mailbox.Identity).DistinguishedName

$UserInfo
}
Main

```

## Einrichten von Schritten zum Konvertieren lokaler Postfächer in E-Mail-aktivierte Benutzer

Gehen Sie wie folgt vor, um den Vorgang abzuschließen.

1. Kopieren Sie "ExportO365UserInfo.ps1", "Exchange2007MBtoMEU.ps1" und die zum Ausführen des Migrationsbatches verwendete CSV-Datei auf Ihrem lokalen Server in dasselbe Verzeichnis.
2. Benennen Sie die CSV-Migrationsdatei in "migration.csv" um.
3. Führen Sie in der Exchange-Verwaltungsshell den folgenden Befehl ein. Das Skript wird davon ausgegangen, dass die CSV-Datei befindet sich in demselben Verzeichnis und migration.csv heißt.

```
.\ExportO365UserInfo.ps1
```

<span data-ttu-id="d9f37-137">Sie werden aufgefordert, die vorhandene Sitzung zu verwenden oder eine neue Sitzung zu öffnen.</span><span class="sxs-lookup"><span data-stu-id="d9f37-137">You will be prompted to use the existing session or open a new session.</span></span>

4. Geben Sie n ein, und drücken Sie **EINGABE**, um eine neue Sitzung zu öffnen.

Das Skript wird ausgeführt, das die Datei "Cloud.csv" im aktuellen Arbeitsverzeichnis speichert.

5. Geben Sie die Anmeldeinformationen eines Administrators für Ihre cloudbasierte Organisation ein, und klicken Sie dann auf **OK**.
6. Führen Sie in einer neuen Sitzung der Exchange-Verwaltungsshell den folgenden Befehl aus. Bei diesem Befehl wird davon ausgegangen, dass sich "ExportO365UserInfo.ps1" und "Cloud.csv" in demselben Verzeichnis befinden.

```
.\Exchange2007MBtoMEU.ps1 <FQDN of on-premises domain controller>
```

<span data-ttu-id="d9f37-143">Beispiel:</span><span class="sxs-lookup"><span data-stu-id="d9f37-143">For example:</span></span>

```
.\\Exchange2007MBtoMEU.ps1 DC1.contoso.com
```

<span data-ttu-id="d9f37-144">Das Skript konvertiert lokale Postfächer für alle in "Cloud.csv" enthaltenen Benutzer in E-Mail-aktivierte Benutzer.</span><span class="sxs-lookup"><span data-stu-id="d9f37-144">The script converts on-premises mailboxes to MEUs for all users included in the Cloud.csv.</span></span>

7. Überprüfen Sie, ob die neuen E-Mail-aktivierten Benutzer erstellt wurden. Führen Sie in Active Directory-Benutzer und -Computer folgende Schritte aus:
8. Klicken Sie auf "Aktion" > "Suchen".
9. Klicken Sie auf die Registerkarte "Exchange".
10. Wählen Sie **Nur Exchange-Empfänger anzeigen** und dann **Benutzer mit externer E-Mail-Adresse** aus.
11. Klicken Sie auf **Jetzt suchen**.

Die Postfächer, die in E-Mail-aktivierte Benutzer konvertiert wurden, werden unter **Suchergebnisse** aufgelistet.

12. Überprüfen Sie mithilfe von "Active Directory-Benutzer und -Computer", "ADSI Edit" oder "Ldp.exe", ob die folgenden Eigenschaften der E-Mail-aktivierten Benutzer mit den richtigen Informationen ausgefüllt werden.
  - legacyExchangeDN
  - mail
  - msExchMailboxGuid
  - proxyAddresses
  - targetAddress

# Konvertieren von Exchange 2003-Postfächern in E-Mail-aktivierte Benutzer

18.12.2018 • 17 minutes to read

[] Nachdem Sie eine mehrstufige Migration abgeschlossen haben, konvertieren Sie die Postfächer in E-Mail-aktivierte Benutzer, damit die Postfächer automatisch eine Verbindung mit dem Cloudpostfach herstellen können.

## Gründe zum Konvertieren von Postfächern in E-Mail-aktivierte Benutzer

Wenn Sie eine mehrstufige Exchange-Migration zum Migrieren Ihrer lokalen Exchange 2003-Postfächer Ihrer Organisation zu Office 365 abgeschlossen haben, und Sie cloudbasierte Benutzer der lokalen Organisation mithilfe von Active Directory verwalten möchten, sollten Sie die lokalen Postfächer in E-Mail-aktivierte Benutzer konvertieren.

Dieser Artikel enthält ein Windows PowerShell-Skript, mit dem Informationen aus den cloudbasierten Postfächern erfasst werden, und ein Visual Basic-Skript (VB), das Sie zum Konvertieren von Exchange 2003-Postfächern in E-Mail-aktivierte Benutzer ausführen können. Wenn Sie dieses Skript ausführen, werden die Proxyadressen aus dem cloudbasierten Postfach in den E-Mail-aktivierten Benutzer kopiert, der sich in Active Directory befindet. Darüber hinaus ermöglichen es die Eigenschaften des E-Mail-aktivierten Benutzers dem Microsoft Online Services-Verzeichnissynchronisierungstool (DirSync), die E-Mail-aktivierten Benutzer mit den entsprechenden Cloudpostfächern zu vergleichen.

Es wird empfohlen, dass Sie lokale Postfächer für einen Migrationsbatch in E-Mail-aktivierte Benutzer konvertieren. Nach Abschluss eines mehrstufigen Exchange-Migrationsbatches und nachdem Sie überprüft haben, dass alle Postfächer im Batch erfolgreich migriert wurden und die erste Synchronisierung von Postfachelementen mit der Cloud abgeschlossen ist, konvertieren Sie die Postfächer im Migrationsbatch in E-Mail-aktivierte Benutzer.

## PowerShell-Skript zum Erfassen von Daten aus Cloudpostfächern

Sie können die nachfolgenden Skripts zum Erfassen von Informationen zu den cloudbasierten Postfächern und zum Konvertieren der Exchange 2007-Postfächer in E-Mail-aktivierte Benutzer verwenden.

Das folgende Skript erfasst Informationen aus Ihren Cloudpostfächern und speichert sie in einer CSV-Datei. Führen Sie dieses Skript zuerst aus.

Kopieren Sie das folgende Skript in eine TXT-Datei, und speichern Sie die Datei dann unter "ExportO365UserInfo.ps1".

```
Param($migrationCSVFileName = "migration.csv")
function O365Logon
{
    #Check for current open 0365 sessions and allow the admin to either use the existing session or create a new one
    $session = Get-PSSession | ?{$_.ConfigurationName -eq 'Microsoft.Exchange'}
    if($session -ne $null)
    {
        $a = Read-Host "An open session to Office 365 already exists. Do you want to use this session? Enter y to use the open session, anything else to close and open a fresh session."
        if($a.ToLower() -eq 'y')
        {
            Write-Host "Using existing Office 365 Powershell Session." -ForegroundColor Green
            return
        }
    }
}
```

```

        }
        $session | Remove-PSSession
    }
    Write-Host "Please enter your Office 365 credentials" -ForegroundColor Green
    $cred = Get-Credential
    $s = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.outlook.com/powershell
    -Credential $cred -Authentication Basic -AllowRedirection
    $importresults = Import-PSSession $s
}
function Main
{
    #Verify the migration CSV file exists
    if(!(Test-Path $migrationCSVFileName))
    {
        Write-Host "File $migrationCSVFileName does not exist." -ForegroundColor Red
        Exit
    }
    #Import user list from migration.csv file
    $MigrationCSV = Import-Csv $migrationCSVFileName
    #Get mailbox list based on email addresses from CSV file
    $MailBoxList = $MigrationCSV | %{$_.EmailAddress} | Get-Mailbox
    $Users = @()
    #Get LegacyDN, Tenant, and On-Premise Email addresses for the users
    foreach($user in $MailBoxList)
    {
        $UserInfo = New-Object System.Object
        $CloudEmailAddress = $user.EmailAddresses | ?{($_ -match 'onmicrosoft') -and ($_. -cmatch 'smtp:')})
        if ($CloudEmailAddress.Count -gt 1)
        {
            $CloudEmailAddress = $CloudEmailAddress[0].ToString().ToLower().Replace('smtp:', '')
            Write-Host "$user returned more than one cloud email address. Using $CloudEmailAddress" -
ForegroundColor Yellow
        }
        else
        {
            $CloudEmailAddress = $CloudEmailAddress.ToString().ToLower().Replace('smtp:', '')
        }
        $UserInfo | Add-Member -Type NoteProperty -Name LegacyExchangeDN -Value $user.LegacyExchangeDN
        $UserInfo | Add-Member -Type NoteProperty -Name CloudEmailAddress -Value $CloudEmailAddress
        $UserInfo | Add-Member -Type NoteProperty -Name OnPremiseEmailAddress -Value
$user.PrimarySMTPAddress.ToString()
        $Users += $UserInfo
    }
    #Check for existing csv file and overwrite if needed
    if(Test-Path ".\cloud.csv")
    {
        $delete = Read-Host "The file cloud.csv already exists in the current directory. Do you want to
delete it? Enter y to delete, anything else to exit this script."
        if($delete.ToString().ToLower() -eq 'y')
        {
            Write-Host "Deleting existing cloud.csv file" -ForegroundColor Red
            Remove-Item ".\cloud.csv"
        }
        else
        {
            Write-Host "Will NOT delete current cloud.csv file. Exiting script." -ForegroundColor Green
            Exit
        }
    }
    $Users | Export-Csv -Path ".\cloud.csv" -notype
    (Get-Content ".\cloud.csv") | %{$_. -replace "'", ''} | Set-Content ".\cloud.csv" -Encoding Unicode
    Write-Host "CSV File Successfully Exported to cloud.csv" -ForegroundColor Green
}
0365Logon
Main

```

Das folgende Visual Basic-Skript konvertiert lokalen Exchange 2003-Postfächer in MEUs. Führen Sie dieses Skript

nach der Ausführung des Skripts zum Sammeln von Informationen aus der Cloud-Postfächer verfügen.

Kopieren Sie das folgende Skript in eine TXT-Datei, und speichern Sie die Datei dann unter "Exchange2003MBtoMEU.vbs".

```
'Globals/Constants
Const ADS_PROPERTY_APPEND = 3
Dim UserDN
Dim remoteSMTPAddress
Dim remoteLegacyDN
Dim domainController
Dim csvMode
csvMode = FALSE
Dim csvFileName
Dim lastADLookupFailed
Class UserInfo
    public OnPremiseEmailAddress
    public CloudEmailAddress
    public CloudLegacyDN
    public LegacyDN
    public ProxyAddresses
    public Mail
    public MailboxGUID
    public DistinguishedName
    Public Sub Class_Initialize()
        Set ProxyAddresses = CreateObject("Scripting.Dictionary")
    End Sub
End Class
'Command Line Parameters
If WScript.Arguments.Count = 0 Then
    'No parameters passed
    WScript.Echo("No parameters were passed.")
    ShowHelp()
ElseIf StrComp(WScript.Arguments(0), "-c", vbTextCompare) = 0 And WScript.Arguments.Count = 2 Then
    WScript.Echo("Missing DC Name.")
    ShowHelp()
ElseIf StrComp(WScript.Arguments(0), "-c", vbTextCompare) = 0 Then
    'CSV Mode
    csvFileName = WScript.Arguments(1)
    domainController = WScript.Arguments(2)
    csvMode = TRUE
    WScript.Echo("CSV mode detected.  Filename: " & WScript.Arguments(1) & vbCrLf)
ElseIf wscript.Arguments.Count <> 4 Then
    'Invalid Arguments
    WScript.Echo WScript.Arguments.Count
    Call ShowHelp()
Else
    'Manual Mode
    UserDN = wscript.Arguments(0)
    remoteSMTPAddress = wscript.Arguments(1)
    remoteLegacyDN = wscript.Arguments(2)
    domainController = wscript.Arguments(3)
End If
Main()
>Main entry point
Sub Main
    'Check for CSV Mode
    If csvMode = TRUE Then
        UserInfoArray = GetUserInfoFromCSVFile()
    Else
        WScript.Echo "Manual Mode Detected" & vbCrLf
        Set info = New UserInfo
        info.CloudEmailAddress = remoteSMTPAddress
        info.DistinguishedName = UserDN
        info.CloudLegacyDN = remoteLegacyDN
        ProcessSingleUser(info)
    End If
End Sub
```

```

'Process a single user (manual mode)
Sub ProcessSingleUser(ByRef UserInfo)
    userADSPPath = "LDAP://" & domainController & "/" & UserInfo.DistinguishedName
    WScript.Echo "Processing user " & userADSPPath
    Set MyUser = GetObject(userADSPPath)
    proxyCounter = 1
    For Each address in MyUser.Get("proxyAddresses")
        UserInfo.ProxyAddresses.Add proxyCounter, address
        proxyCounter = proxyCounter + 1
    Next
    UserInfo.OnPremiseEmailAddress = GetPrimarySMTPAddress(UserInfo.ProxyAddresses)
    UserInfo.Mail = MyUser.Get("mail")
    UserInfo.MailboxGUID = MyUser.Get("msExchMailboxGUID")
    UserInfo.LegacyDN = MyUser.Get("legacyExchangeDN")
    ProcessMailbox(UserInfo)
End Sub

'Populate user info from CSV data
Function GetUserInfoFromCSVFile()
    CSVInfo = ReadCSVFile()
    For i = 0 To (UBound(CSVInfo)-1)
        lastADLookupFailed = false
        Set info = New UserInfo
        info.CloudLegacyDN = Split(CSVInfo(i+1), ",")(0)
        info.CloudEmailAddress = Split(CSVInfo(i+1), ",")(1)
        info.OnPremiseEmailAddress = Split(CSVInfo(i+1), ",")(2)
        WScript.Echo "Processing user " & info.OnPremiseEmailAddress
        WScript.Echo "Calling LookupADInformationFromSMTPAddress"
        LookupADInformationFromSMTPAddress(info)
        If lastADLookupFailed = false Then
            WScript.Echo "Calling ProcessMailbox"
            ProcessMailbox(info)
        End If
        set info = nothing
    Next
End Function

'Populate user info from AD
Sub LookupADInformationFromSMTPAddress(ByRef info)
    'Lookup the rest of the info in AD using the SMTP address
    Set objRootDSE = GetObject("LDAP://RootDSE")
    strDomain = objRootDSE.Get("DefaultNamingContext")
    Set objRootDSE = nothing
    Set objConnection = CreateObject("ADODB.Connection")
    objConnection.Provider = "ADsDSOObject"
    objConnection.Open "Active Directory Provider"
    Set objCommand = CreateObject("ADODB.Command")
    BaseDN = "<LDAP://" & domainController & "/" & strDomain & ">"
    adFilter = "(&(proxyAddresses=SMTP:" & info.OnPremiseEmailAddress & "))"
    Attributes = "distinguishedName,msExchMailboxGUID,mail,proxyAddresses,legacyExchangeDN"
    Query = BaseDN & ";" & adFilter & ";" & Attributes & ";subtree"
    objCommand.CommandText = Query
    Set objCommand.ActiveConnection = objConnection
    On Error Resume Next
    Set objRecordSet = objCommand.Execute
    'Handle any errors that result from the query
    If Err.Number <> 0 Then
        WScript.Echo "Error encountered on query " & Query & ". Skipping user."
        lastADLookupFailed = true
        return
    End If
    'Handle zero or ambiguous search results
    If objRecordSet.RecordCount = 0 Then
        WScript.Echo "No users found for address " & info.OnPremiseEmailAddress
        lastADLookupFailed = true
        return
    ElseIf objRecordSet.RecordCount > 1 Then
        WScript.Echo "Ambiguous search results for email address " & info.OnPremiseEmailAddress
        lastADLookupFailed = true
        return
    End If
End Sub

```

```

ElseIf Not objRecordSet.EOF Then
    info.LegacyDN = objRecordSet.Fields("legacyExchangeDN").Value
    info.Mail = objRecordSet.Fields("mail").Value
    info.MailboxGUID = objRecordSet.Fields("msExchMailboxGUID").Value
    proxyCounter = 1
    For Each address in objRecordSet.Fields("proxyAddresses").Value
        info.ProxyAddresses.Add proxyCounter, address
        proxyCounter = proxyCounter + 1
    Next
    info.DistinguishedName = objRecordSet.Fields("distinguishedName").Value
    objRecordSet.MoveNext
End If
objConnection = nothing
objCommand = nothing
objRecordSet = nothing
On Error Goto 0
End Sub
'Populate data from the CSV file
Function ReadCSVFile()
    'Open file
    Set objFS = CreateObject("Scripting.FileSystemObject")
    Set objTextFile = objFS.OpenTextFile(csvFileName, 1, false, -1)
    'Loop through each line, putting each line of the CSV file into an array to be returned to the caller
    counter = 0
    Dim CSVArray()
    Do While NOT objTextFile.AtEndOfStream
        ReDim Preserve CSVArray(counter)
        CSVArray(counter) = objTextFile.ReadLine
        counter = counter + 1
    Loop
    'Close and return
    objTextFile.Close
    Set objTextFile = nothing
    Set objFS = nothing
    ReadCSVFile = CSVArray
End Function
'Process the migration
Sub ProcessMailbox(User)
    'Get user properties
    userADSIPath = "LDAP://" & domainController & "/" & User.DistinguishedName
    Set MyUser = GetObject(userADSIPath)
    'Add x.500 address to list of existing proxies
    existingLegDnFound = FALSE
    newLegDnFound = FALSE
    'Loop through each address in User.ProxyAddresses
    For i = 1 To User.ProxyAddresses.Count
        If StrComp(address, "x500:" & User.LegacyDN, vbTextCompare) = 0 Then
            WScript.Echo "x500 proxy " & User.LegacyDN & " already exists"
            existingLegDnFound = true
        End If
        If StrComp(address, "x500:" & User.CloudLegacyDN, vbTextCompare) = 0 Then
            WScript.Echo "x500 proxy " & User.CloudLegacyDN & " already exists"
            newLegDnFound = true
        End If
    Next
    'Add existing leg DN to proxy list
    If existingLegDnFound = FALSE Then
        WScript.Echo "Adding existing legacy DN " & User.LegacyDN & " to proxy addresses"
        User.ProxyAddresses.Add (User.ProxyAddresses.Count+1),("x500:" & User.LegacyDN)
    End If
    'Add new leg DN to proxy list
    If newLegDnFound = FALSE Then
        'Add new leg DN to proxy addresses
        WScript.Echo "Adding new legacy DN " & User.CloudLegacyDN & " to existing proxy addresses"
        User.ProxyAddresses.Add (User.ProxyAddresses.Count+1),("x500:" & User.CloudLegacyDN)
    End If
    'Dump out new list of addresses
    WScript.Echo "Original proxy addresses updated count: " & User.ProxyAddresses.Count
    For i = 1 to User.ProxyAddresses.Count

```

```

WScript.Echo " proxyAddress " & i & ":" & User.ProxyAddresses(i)
Next
'Delete the Mailbox
WScript.Echo "Opening " & userADSIPath & " as CDOEXM::IMailboxStore object"
Set Mailbox = MyUser
Wscript.Echo "Deleting Mailbox"
On Error Resume Next
Mailbox.DeleteMailbox
'Handle any errors deleting the mailbox
If Err.Number <> 0 Then
    WScript.Echo "Error " & Err.number & ". Skipping User." & vbCrLf & "Description: "
& Err.Description & vbCrLf
    Exit Sub
End If
On Error Goto 0
'Save and continue
WScript.Echo "Saving Changes"
MyUser.SetInfo
WScript.Echo "Refeshing ADSI Cache"
MyUser.GetInfo
Set Mailbox = nothing
'Mail Enable the User
WScript.Echo "Opening " & userADSIPath & " as CDOEXM::IMailRecipient"
Set MailUser = MyUser
WScript.Echo "Mail Enabling user using targetAddress " & User.CloudEmailAddress
MailUser.MailEnable User.CloudEmailAddress
WScript.Echo "Disabling Recipient Update Service for user"
MyUser.PutEx ADS_PROPERTY_APPEND, "msExchPoliciesExcluded", Array("{26491CFC-9E50-4857-861B-
0CB8DF22B5D7}")
WScript.Echo "Saving Changes"
MyUser.SetInfo
WScript.Echo "Refreshing ADSI Cache"
MyUser.GetInfo
'Add Legacy DN back on to the user
WScript.Echo "Writing legacyExchangeDN as " & User.LegacyDN
MyUser.Put "legacyExchangeDN", User.LegacyDN
'Add old proxies list back on to the MEU
WScript.Echo "Writing proxyAddresses back to the user"
For j=1 To User.ProxyAddresses.Count
    MyUser.PutEx ADS_PROPERTY_APPEND, "proxyAddresses", Array(User.ProxyAddresses(j))
    MyUser.SetInfo
    MyUser.GetInfo
Next
'Add mail attribute back on to the MEU
WScript.Echo "Writing mail attribute as " & User.Mail
MyUser.Put "mail", User.Mail
'Add msExchMailboxGUID back on to the MEU
WScript.Echo "Converting mailbox GUID to writable format"
Dim mbxGUIDByteArray
Call ConvertHexStringToByteArray(OctetToString(User.MailboxGUID), mbxGUIDByteArray)
WScript.Echo "Writing property msExchMailboxGUID to user object with value " &
OctetToString(User.MailboxGUID)
MyUser.Put "msExchMailboxGUID", mbxGUIDByteArray
WScript.Echo "Saving Changes"
MyUser.SetInfo
WScript.Echo "Migration Complete!" & vbCrLf
End Sub
'Returns the primary SMTP address of a user
Function GetPrimarySMTPAddress(Addresses)
    For Each address in Addresses
        If Left(address, 4) = "SMTP" Then GetPrimarySMTPAddress = address
    Next
End Function
'Converts Hex string to byte array for writing to AD
Sub ConvertHexStringToByteArray(ByVal strHexString, ByRef pByteArray)
    Set FSO = CreateObject("Scripting.FileSystemObject")
    Set Stream = CreateObject("ADODB.Stream")
    Temp = FSO.GetTempName()
    Set TS = FSO.CreateTextFile(Temp)

```

```

For i = 1 To (Len (strHexString) -1) Step 2
    TS.Write Chr("&h" & Mid (strHexString, i, 2))
Next
TS.Close
Stream.Type = 1
Stream.Open
Stream.LoadFromFile Temp
pByteArray = Stream.Read
Stream.Close
FSO.DeleteFile Temp
Set Stream = nothing
Set FSO = Nothing
End Sub
'Converts raw bytes from AD GUID to readable string
Function OctetToHexString (arrbytOctet)
    OctetToHexStr = ""
    For k = 1 To Lenb (arrbytOctet)
        OctetToHexString = OctetToHexString & Right("0" & Hex(AscB(MidB(arrbytOctet, k, 1))), 2)
    Next
End Function
Sub ShowHelp()
    WScript.Echo("This script runs in two modes, CSV Mode and Manual Mode." & vbCrLf & "CSV Mode
allows you to specify a CSV file from which to pull usernames." & vbCrLf&"Manual mode allows you to
run the script against a single user.")
    WScript.Echo("Both modes require you to specify the name of a DC to use in the local domain." & vbCrLf
& "To run the script in CSV Mode, use the following syntax:")
    WScript.Echo(" cscript Exchange2003MBtoMEU.vbs -c x:\csv\csvfilename.csv dc.domain.com")
    WScript.Echo("To run the script in Manual Mode, you must specify the users AD Distinguished Name, Remote
SMTP Address, Remote Legacy Exchange DN, and Domain Controller Name.")
    WScript.Echo(" cscript Exchange2003MBtoMEU.vbs " & chr(34) &
"CN=UserName,CN=Users,DC=domain,DC=com" & chr(34) & " " & chr(34) & "user@cloudaddress.com"
& chr(34) & " " & chr(34) & "/o=Cloud Org/ou=Cloud Site/ou=Recipients/cn=CloudUser" &
chr(34) & " dc.domain.com")
    WScript.Quit
End Sub

```

## Was tun die Skripts?

### **ExportO365UserInfo.ps1**

Dies ist ein Windows PowerShell-Skript, das Sie in Ihrer cloudbasierten Organisation ausführen, um Informationen zu den Cloudpostfächern zu erfassen, die Sie bei der mehrstufigen Exchange-Migration migriert haben. Es verwendet eine CSV-Datei, um den Umfang des Batches von Benutzern festzulegen. Es wird empfohlen, dass Sie dieselbe CSV-Migrationsdatei verwenden, die Sie zum Migrieren eines Benutzerbatches verwendet haben.

Wenn Sie das Skript "ExportO365UserInfo" ausführen:

- Die folgenden Eigenschaften werden aus den Cloudpostfächern für die in der CSV-Datei aufgelisteten Benutzer erfasst:
  - Primäre SMTP-Adresse
  - Primäre SMTP-Adresse des entsprechenden lokalen Postfachs
  - Andere Proxyadressen für das Cloudpostfach
  - LegacyExchangeDN
- Die erfassten Eigenschaften werden in einer CSV-Datei namens "Cloud.csv" gespeichert.

### **Exchange2003MBtoMEU.vbs**

Dies ist ein VB-Skript, das Sie in Ihrer lokalen Exchange 2003-Organisation zum Konvertieren von Postfächern in E-Mail-aktivierte Benutzer ausführen. Es verwendet die Datei "Cloud.csv", die vom Skript "ExportO365UserInfo"

ausgegeben wird.

Wenn Sie das Skript "Exchange2003MBtoMEU.vbs" ausführen, führt es die folgenden Schritte für jedes Postfach aus, das in der CSV-Datei aufgelistet ist:

- Erfasst Informationen aus der CSV-Datei und aus dem lokalen Postfach.
- Erstellt eine Liste von Proxyadressen aus dem lokalen und dem Cloudpostfach, die zum E-Mail-aktivierten Benutzer hinzugefügt werden.
- Löscht das lokale Postfach.
- Erstellt einen E-Mail-aktivierten Benutzer und füllt die folgenden Eigenschaften aus:
  - **LegacyExchangeDN**: Wert aus dem lokalen Postfach.
  - **e-Mail**: die primäre SMTP des Postfachs Cloud.
  - **MsExchMailboxGuid**: Wert aus dem lokalen Postfach.
  - **ProxyAddresses**: Werte aus dem lokalen Postfach und das cloudbasierten Postfach.
  - **TargetAddress**: Lesen aus dem lokalen Postfach; der Wert ist die primäre SMTP des Postfachs Cloud.

#### IMPORTANT

Zum Aktivieren des Offboardings von Office 365 zu Exchange 2003 müssen Sie den Wert von "msExchMailboxGuid" für den E-Mail-aktivierten Benutzer durch die GUID des cloudbasierten Postfachs ersetzen. Führen Sie den folgenden PowerShell-Befehl aus, um die GUIDs für die Postfächer in Ihrer Cloudorganisation abzurufen und in einer CSV-Datei zu speichern:

```
Get-Mailbox | Select PrimarySmtpAddress, Guid | Export-csv -Path .\guid.csv
```

Dieser Befehl extrahiert die primäre SMTP-Adresse und GUID für alle Cloudpostfächer in die Datei "guid.csv". Anschließend wird diese Datei im aktuellen Verzeichnis gespeichert.

Anstatt mithilfe der CSV-Eingabedatei eine Gruppe von Postfächern zu konvertieren, können Sie das Skript "Exchange2003MBtoMEU.vbs" im manuellen Modus ausführen, um die Postfächer nacheinander zu konvertieren. Dazu müssen Sie die folgenden Eingabeparameter bereitstellen:

- Distinguished Name (DN) des lokalen Postfachs
- Primäre SMTP-Adresse des Cloudpostfachs
- Exchange-Legacy-DN für das Cloudpostfach
- Domänencontrollername in Ihrer Exchange 2003-Organisation

## Schritte zum Konvertieren lokaler Postfächer in E-Mail-aktivierte Benutzer

1. Führen Sie "die ExportO365UserInfo" in Ihrer Cloudorganisation aus. Verwenden Sie die CSV-Datei als Eingabedatei für den Migrationsbatch. Das Skript erstellt eine CSV-Datei namens "Cloud.csv".

```
.\ExportO365UserInfo.ps1 <CSV input file>
```

Beispiel:

```
.\Export0365UserInfo.ps1 .\MigrationBatch1.csv
```

In diesem Beispiel wird davon ausgegangen, dass sich das Skript und die CSV-Eingabedatei in demselben Verzeichnis befinden.

2. Kopieren Sie "Exchange2003MBtoMEU.vbs" und "Cloud.csv" in dasselbe Verzeichnis in Ihrer lokalen Organisation.
3. Führen Sie den folgenden Befehl in Ihrer lokalen Organisation aus:

```
cscript Exchange2003MBtoMEU.vbs -c .\Cloud.csv <FQDN of on-premises domain controller>
```

Beispiel:

```
cscript Exchange2003MBtoMEU.vbs -c .\Cloud.csv DC1.contoso.com
```

Geben Sie den folgenden Befehl ein, um das Skript im manuellen Modus auszuführen. Verwenden Sie Leerzeichen zwischen den einzelnen Werten.

```
cscript Exchange2003MBtoMEU.vbs "<DN of on-premises mailbox>" "<Primary SMTP of cloud mailbox>" "<ExchangeLegacyDN of cloud mailbox>" <FQDN of on-premises domain controller>
```

Beispiel:

```
cscript Exchange2003MBtoMEU.vbs "CN=Ann Beebe,CN=Users,DC=contoso,DC=com" "annb@contoso.onmicrosoft.com" "/o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d808d014cec5411ea6de1f70cc116e7b-annb" DC1.contoso.com
```

4. Überprüfen Sie, ob die neuen E-Mail-aktivierten Benutzer erstellt wurden. Führen Sie in Active Directory-Benutzer und -Computer folgende Schritte aus:
5. Klicken Sie auf **Aktion > Suchen**.
6. Klicken Sie auf die Registerkarte **Exchange**.
7. Wählen Sie **Nur Exchange-Empfänger anzeigen** und dann **Benutzer mit externer E-Mail-Adresse** aus.
8. Klicken Sie auf **Jetzt suchen**.

```
<span data-ttu-id="4bc5d-172">Die Postfächer, die in E-Mail-aktivierte Benutzer konvertiert wurden, werden unter **Suchergebnisse** aufgelistet.</span><span class="sxs-lookup"><span data-stu-id="4bc5d-172">The mailboxes that were converted to MEUs are listed under **Search results**.</span></span>
```

5. Überprüfen Sie mithilfe von "Active Directory-Benutzer und -Computer", "ADSI Edit" oder "Ldp.exe", ob die folgenden Eigenschaften der E-Mail-aktivierten Benutzer mit den richtigen Informationen ausgefüllt werden.
  - legacyExchangeDN
  - mail
  - msExchMailboxGuid\*

- proxyAddresses
- targetAddress

\*Wie bereits erklärt behält das Skript Exchange2003MBtoMEU.vbs den **MsExchMailboxGuid**-Wert aus dem lokalen Postfach. Zum aktivieren müssen Sie Verschiebens von Office 365 zu Exchange 2003, um den Wert für die **MsExchMailboxGuid**-Eigenschaft auf den MEU mit der Guid aus dem Postfach Cloud-basierten ersetzen.

# Was Sie zum Migrieren von IMAP-Postfächern zu Office 365 wissen müssen

18.12.2018 • 10 minutes to read

[] Sie können die Inhalte von Benutzerpostfächern aus Ihrem Quell-E-Mail-System zu Office 365 migrieren. Verwenden Sie IMAP (Internet Message Access Protocol), um Ihre E-Mails zu migrieren, wenn Folgendes zutrifft:

- Ihr Quell-E-Mail-System unterstützt IMAP.

Wenn diese Option für Sie nicht funktioniert, lesen Sie [Möglichkeiten zum Migrieren von E-Mail zu Office 365](#), um Informationen zu weiteren Optionen zu erhalten.

Informationen zu den Windows PowerShell-Schritten finden Sie unter [Verwenden von PowerShell zum Durchführen einer IMAP-Migration zu Office 365](#).

## Zu berücksichtigende Faktoren

Es gibt einige Beschränkungen, die Sie beachten müssen:

- Sie können nur Elemente migrieren, die sich im Posteingang oder in anderen E-Mail-Ordnern eines Benutzers befinden. Bei diesem Typ von Migration werden keine Kontakte, Kalenderelemente oder Aufgaben migriert.
- Sie können maximal 500.000 Elemente aus dem Postfach eines Benutzers migrieren (E-Mails werden von den neuesten zu den ältesten E-Mails migriert).
- Eine E-Mail kann nur migriert werden, wenn sie nicht größer ist als 35 MB.
- Wenn Sie die Verbindungen mit Ihrem Quell-E-Mail-System beschränkt haben, ist es ratsam, diese Beschränkungen so zu ändern, dass die Migrationsleistung verbessert wird. Zu den üblichen Verbindungsbeschränkungen gehören Gesamtanzahl der Client/Server-Verbindungen, Verbindungen pro Benutzer und IP-Adressenverbindungen auf dem Server oder in der Firewall.

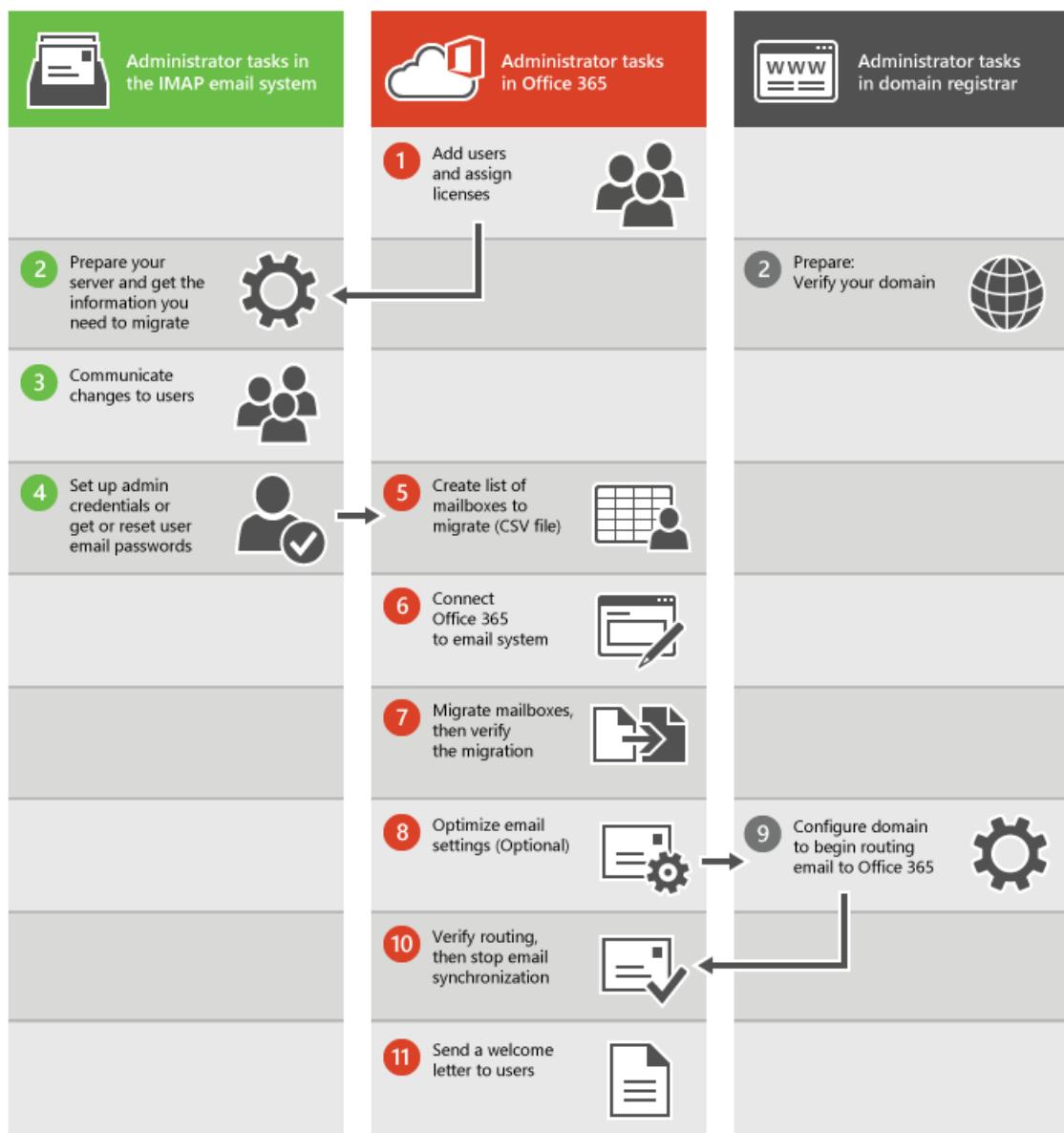
## Auswirkungen einer Migration auf Benutzer

Damit Sie E-Mail migrieren können, benötigen Sie Zugriff auf die Benutzerpostfächer in Ihrem Quell-E-Mail-System. Wenn Sie die Benutzerkennwörter wissen oder mit Administrator-Anmeldeinformationen auf die Benutzerpostfächer zugreifen können, gibt es keine Auswirkungen für die Benutzer, bis Sie Ihr Quell-E-Mail-System herunterfahren.

Wenn Sie nicht auf die Benutzerpostfächer zugreifen können, müssen Sie die Kennwörter zurücksetzen. Auf diese Weise können Sie auf die Benutzerpostfächer zugreifen, indem Sie neue Kennwörter verwenden, die Sie wissen. Wenn Benutzer die neuen Kennwörter nicht wissen, haben sie während oder nach der E-Mail-Migration keinen Zugriff mehr auf ihre alten Postfächer. Sie können die neuen Kennwörter nach der Migration verteilen, wenn Sie möchten, dass die Benutzer ihre alten Postfächer erhalten.

## Wie funktioniert die IMAP-Migration?

Die wichtigsten Schritte, die Sie für eine IMAP-E-Mail-Migration ausführen, sind in der folgenden Abbildung gezeigt.



Diese allgemeinen Schritte gelten, wenn Sie von Gmail oder einem anderen IMAP-System migrieren.

1. Zuerst müssen Sie Ihre Benutzer in Office 365 erstellen und ihnen Lizenzen zuweisen. Die Postfächer müssen in Office 365 vorhanden sein, um die IMAP-Migration zu verwenden.
2. Bereiten Sie Ihr IMAP-Quell-E-Mail-System vor, und rufen Sie die Informationen ab, die Sie zum Migrieren benötigen. Wenn Sie planen, Ihre Domäne zu Office 365 zu migrieren, überprüfen Sie bei Ihrer Domänenregistrierungsstelle, ob Sie die Domäne besitzen.

Je nachdem, von welcher Art von E-Mail-Dienst Sie migrieren, müssen Sie möglicherweise einige Einstellungen konfigurieren oder einfach den Namen Ihres E-Mail-Servers oder -Diensts für die spätere Verwendung notieren. Sie müssen Ihre Domäne auch in Ihrem Domänenregistrierungssystem überprüfen, wenn Sie eine benutzerdefinierte Domäne haben.

3. Teilen Sie den Benutzern die Änderungen mit.

Es wird empfohlen, die Benutzer über die E-Mail-Migration und deren Auswirkungen zu benachrichtigen. Informieren Sie die Benutzer über die Aufgaben, die vor, während und nach der Migration ausgeführt werden müssen.

4. Richten Sie Administratoranmeldeberechtigungen ein, oder rufen Sie die E-Mail-Benutzerkennwörter ab, oder setzen Sie diese zurück.

Zum Durchführen der Migration benötigen Sie ein Administratorkonto, das die Berechtigungen hat, oder den Benutzernamen und das Kennwort für jedes Postfach.

5. Wenn Sie die Schritte in [Migrieren von Google Apps zu Office 365 Postfächer](#) oder [andere Arten von IMAP-Postfächern zu Office 365 migrieren](#) verwenden, erstellen Sie eine Liste der Postfächer zu migrieren (CSV-Datei). Diese Anweisungen Migrationen aus der Exchange-Verwaltungskonsole starten, und Sie müssen eine CSV-Datei erstellen, in der aufgelistet, die e-Mail-Adressen, Benutzernamen und Kennwörter für die Postfächer, den, die Sie migrieren möchten.

Sie können auch die Seite "Migrationen" oder die Setupsanweisungen aus der [Admin Center Preview verwenden, um IMAP-Systeme zu migrieren](#) (wie Gmail, Hotmail.com oder Outlook.com). Diese Schritte eignen sich am besten, wenn Sie nur einige wenige Benutzer (weniger als 50) migrieren möchten. Wenn Sie die E-Mails für mehr Benutzer migrieren möchten, ist es einfacher, eine CSV-Datei zu verwenden, um alle Daten für die Konten einzugeben.

6. Verbinden Sie Office 365 mit dem E-Mail-System.

Damit Gmail-Postfächer erfolgreich migriert werden können, muss Office 365 mit dem Quell-E-Mail-System verbunden werden und mit diesem System kommunizieren können. Zu diesem Zweck verwendet Office 365 einen Migrationsendpunkt, die Einstellungen, die verwendet werden, um die Verbindung zu erstellen.

7. Migrieren Sie die Postfächer, und überprüfen Sie dann die Migration.

Zum Migrieren von Postfächern erstellen Sie einen Migrationsbatch, und starten Sie dann die Migration. Nach dem Ausführen des Migrationbatch vergewissern Sie sich, dass die E-Mail-Konten erfolgreich migriert wurden.

8. Optimieren Sie die E-Mail-Einstellungen (optional).

Es gibt einige Einstellungen, die Sie konfigurieren können, sodass es für die E-Mail-Adressen nicht so lange dauert, bis sie in den neuen Office 365-Postfächern angezeigt werden. Weitere Informationen finden Sie unter: [Tipps zum Optimieren von IMAP-Migrationen](#).

9. Beginnen Sie mit dem Routing von E-Mails an Office 365.

Sie müssen einen DNS-Eintrag, der als MX-Eintrag bezeichnet wird, so ändern, dass Ihr E-Mail-System damit beginnen kann, E-Mails an Office 365 weiterzuleiten.

10. Überprüfen Sie das Routing, und stoppen Sie dann die E-Mail-Synchronisierung.

Nachdem Sie überprüft haben, dass alle E-Mail-Nachrichten Office 365 weitergeleitet werden, können Sie den Migrationsbatch löschen, damit die Synchronisierung zwischen Ihrem Quell-E-Mail-System und Office 365 beendet wird.

11. Senden Sie eine Begrüßungsschreiben an die Benutzer.

Geben Sie Ihren Benutzer Informationen zu Office 365, und teilen Sie ihnen mit, wie sie sich bei ihren neuen Postfächern anmelden.

## Bereit zum Starten?

Um eine E-Mail-Migration erfolgreich abzuschließen, ist es ratsam, die folgenden Aufgaben auszuführen:

- Sie erstellen eine Liste der Postfächer in Excel zu migrieren. Sie fügen der Benutzer e-Mail-Adressen, Benutzernamen und Kennwörter dieser Datei finden Sie.
- Sie verwenden die schrittweisen Assistenten in Office 365 zum Konfigurieren und Starten des Migrationsprozesses.
- Nachdem die E-Mails migriert wurden, ändern Sie den MX-Eintrag Ihrer Organisation so, dass er auf Office 365 verweist, wenn die Migration abgeschlossen ist. Ihr MX-Eintrag gibt an, ist wie andere E-Mail-

Systeme den Speicherort Ihres E-Mail-Systems finden. Ein Ändern Ihres MX-Eintrags ermöglicht es anderen E-Mail-Systemen, damit zu beginnen, E-Mails direkt an die neuen Postfächer in Office 365 zu senden. Informationen zum Aktualisieren Ihres MX-Eintrags finden Sie auch unter [Erstellen von DNS-Einträgen bei einem beliebigen DNS-Hostinganbieter für Office 365](#).

Wenn Sie genau wissen, welche Schritte zum Migrieren von Postfächern nach Office 365 erforderlich sind, können Sie sofort beginnen. Der erste Schritt besteht darin festzustellen, aus welchem Quell-E-Mail-System Sie migrieren:

- [Gmail](#)

Dieses Verfahren verwendet die Schritte von Exchange Admin Center für die IMAP-Migration.

- [Ein anderes IMAP-aktiviertes E-Mail-System](#)

Dieses Verfahren verwendet die Schritte von Exchange Admin Center für die IMAP-Migration.

- [IMAP-Migration im Admin Center](#)

- [Verwenden von PowerShell zum Durchführen einer IMAP-Migration zu Office 365](#)

## Siehe auch

[Tipps zum Optimieren von IMAP-Migrationen](#)

[Weitere Informationen zum Einrichten Ihrer IMAP-Serververbindung](#)

# Migrieren von G Suite-Postfächern zu Office 365

18.12.2018 • 28 minutes to read

Unter [Migrieren von IMAP-Postfächern zu Office 365](#) erhalten Sie einen Überblick über den Migrationsprozess. Lesen Sie diesen Artikel zuerst. Nachdem Sie sich mit den Inhalten vertraut gemacht haben, kehren Sie zu diesem Thema zurück, um sich über die Schritte zum Migrieren von Postfächern von G Suite (vormals Google Apps) Gmail zu Office 365 zu informieren. Zum Ausführen der Schritte für die IMAP-Migration müssen Sie ein globaler Administrator in Office 365 sein.

Suchen Sie nach Windows PowerShell-Befehlen? Dann lesen Sie [Verwenden von PowerShell zum Durchführen einer IMAP-Migration zu Office 365](#).

Möchten Sie andere Typen von IMAP-Postfächern migrieren? Dann lesen Sie [Migrieren anderer Typen von IMAP-Postfächern zu Office 365](#).

## Migration von G Suite-Postfächern über das Office 365 Admin Center

Sie können den Setup-Assistenten im Office 365 Admin Center für eine IMAP-Migration verwenden. Weitere Anweisungen finden Sie unter [IMAP-Migration im Office 365 Admin Center](#).

**Wichtig:** IMAP-Migration wird nur e-Mails migrieren, nicht Kalender und Kontaktinformationen enthalten. Benutzer können ihre eigenen e-Mail, Kontakte und andere Postfachinformationen zu Office 365 importieren. Finden Sie unter [Migrate e-Mails und Kontakte zu Office 365](#) Hier erfahren, wie.

Bevor Office 365 die Verbindung mit Gmail oder G Suite herstellen kann, müssen alle Kontobesitzer ein App-Kennwort für den Zugriff auf ihr Konto erstellen. Der Grund hierfür ist, dass Google Outlook als eine weniger sichere App betrachtet und die Verbindung nur mit einem Kennwort nicht zulässt. Anweisungen finden Sie unter [Vorbereiten Ihres G Suite-Kontos für die Verbindung mit Outlook und Office 365](#). Darüber hinaus müssen Sie sicherstellen, dass [G Suite-Benutzer die Prüfung in zwei Schritten aktivieren können](#).

### Gmail-Migrationsaufgaben

Die folgende Liste enthält die Migrationsaufgaben in der Reihenfolge, in der Sie sie ausführen sollten.

#### Schritt 1: Sicherstellen, dass Sie die Domäne besitzen

In dieser Aufgabe stellen Sie zunächst gegenüber Office 365 sicher, dass Sie die Domäne besitzen, die Sie für Ihre G Suite-Konten verwendet haben.

##### NOTE

Eine andere Option besteht darin, den *Namen Ihres Unternehmens* verwenden. Domäne "onmicrosoft.com", die mit Ihrem Office 365-Abonnement, anstatt Ihre eigene benutzerdefinierte Domäne enthalten ist. In diesem Fall können Sie nur Benutzer hinzufügen, wie [Benutzer einzeln oder in einer Sammeloperation zu Office 365 - Admin Hilfe hinzufügen](#) unter und ausgelassen werden, diese Aufgabe. Die meisten Personen jedoch ihrer eigenen Domäne verwenden möchten.

Domänenüberprüfung ist eine Aufgabe, die Sie als Setup Office 365 durchlaufen werden. Während des Setups von Office 365 Setup enthält Assistenten TXT-Eintrag, den Sie an Ihre Domäne Hostanbieter hinzufügen möchten. Finden Sie unter [Hinzufügen einer Domäne zu Office 365](#) für die Schritte in Office 365 Administrationscenter ausführen, und wählen eine domänenregistrierungsstelle aus den folgenden zwei Optionen zu sehen, wie für die Durchführung der TXT-Eintrag hinzufügen zum Hosten von Ihrem DNS-Anbieter.

- **Ihre aktuelle DNS-Host-Anbieter ist Google:** Wenn Sie Ihre Domäne von Google erworben haben,

und sie die DNS-Hostinganbieter sind, befolgen Sie diese Anweisungen: [Erstellen von DNS-Einträge bei Ihrer Domäne von Google \(Go Daddy\) verwaltet wird.](#)

- **Sie Ihre Domäne aus einer anderen domänenregistrierungsstelle erworben:** Wenn Sie Ihre Domäne in einem anderen Unternehmen erworben haben, bieten wir [Anweisungen](#) für viele häufig verwendete Domäne Hostinganbieter.

## Schritt 2: Hinzufügen von Benutzern zu Office 365

Sie können die Benutzer entweder [einzelnen hinzufügen](#) oder [mehrere Benutzer gleichzeitig hinzufügen](#). Beim Hinzufügen von Benutzern weisen Sie diesen auch Lizenzen zu. Jeder Benutzer muss über ein Postfach in Office 365 verfügen, bevor Sie die E-Mails dorthin migrieren können. Darüber hinaus benötigt auch jeder Benutzer eine Lizenz, die einen Exchange Online-Plan umfasst, um sein Postfach nutzen zu können.

### IMPORTANT

An diesem Punkt haben Sie sichergestellt, dass Sie der Besitzer der Domäne sind, und Ihre G Suite-Benutzer und die Postfächer in Office 365 mit Ihrer benutzerdefinierten Domäne erstellt. Schließen Sie hier den Assistenten. Fahren Sie erst mit dem Schritt **Einrichten der Domäne** fort, nachdem Sie die Gmail-Postfächer zu Office 365 migriert haben. Die Einrichtung schließen Sie in Aufgabe 7 [Schritt 6: Aktualisieren Ihrer DNS-Einträge, um Gmail direkt an Office 365 weiterzuleiten](#) ab.

## Schritt 3: Erstellen einer Liste der zu migrierenden Gmail-Postfächer

Für diese Aufgabe erstellen Sie eine Migrationsdatei, die eine Liste der Gmail-Postfächer enthält, die nach Office 365 migriert werden sollen. Am einfachsten lässt sich die Migrationsdatei mit Excel erstellen, weshalb Excel in diesen Anleitungen verwendet wird. Sie können Excel 2013, Excel 2010 oder Excel 2007 verwenden.

Wenn Sie die Migrationsdatei erstellen, müssen Sie das app-Kennwort jedes Gmail-Postfachs zu kennen, die Sie migrieren möchten. Es wird davon ausgegangen, dass die Benutzerkennwörter nicht kennen, damit Sie wahrscheinlich benötigen temporären Kennwörter zuweisen (durch die Kennwörter zurücksetzen) auf alle Postfächer während der Migration. Sie müssen ein Administrator in G Suite zum Zurücksetzen von Kennwörtern sein.

Sie müssen nicht alle Gmail-Postfächer gleichzeitig migrieren. Sie können die Migration nach Zweckmäßigkeits in Batches vornehmen. Sie können bis zu 50.000 Postfächer (eine Zeile für jeden Benutzer) in die Migrationsdatei einfügen. Die Datei darf bis zu 10 MB groß sein.

1. Melden Sie sich mit Ihrem Administratorbenutzernamen und -kennwort bei der [G Suite-Verwaltungskonsole](#) an.
2. Nachdem Sie angemeldet sind, wählen Sie **Benutzer** aus.

Name	Last signed in
Alberta Greene	Jan 6
Alex Darrow	3:29 PM PST
Bobby Overby	Jan 6

3. Wählen Sie jeden Benutzer aus, um die E-Mail-Adresse des Benutzers zu sehen. Notieren Sie sich die jeweilige Adresse.

The screenshot shows the Office 365 Admin Center interface. On the left is a red circular profile picture with a white letter 'A' in the center. To its right, the user's name 'Alberta Greene' is displayed in bold black text. Below it, the email address 'albertag@contoso.com' is shown in a smaller box with a pink border. Underneath that, the status 'User · Active' and the last login date 'Last login Jan 6' are listed. At the top right of the card are several small icons: a lock, a person, a plus sign, and three dots.

4. Melden Sie sich bei der [Office 365-Verwaltungskonsole](#), und navigieren Sie zur **Benutzer > aktive Benutzer**. Achten Sie auf der Spalte **Benutzername**. Verwenden Sie diese Informationen in einer Minute. Lassen Sie das Office 365 Admin Center-Fenster geöffnet, zu.

The screenshot shows a table titled 'Select a view: All users'. The columns are labeled 'DISPLAY NAME', 'USER NAME', and 'STATUS'. There are five rows of data:

DISPLAY NAME	USER NAME	STATUS
Alberta Greene	alberta@Contoso.com	In cloud
Bobby Overby	bobby@Contoso.com	In cloud
Irwin Hume	irwin@Contoso.com	In cloud
Katrina Hernandez	katrina@Contoso.com	In cloud
Mathew Slattery	mathew@Contoso.com	In cloud

5. Starten Sie Excel.
6. Verwenden Sie das folgende Bildschirmfoto als Vorlage zum Erstellen der Migrationsdatei in Excel. Beginnen Sie mit den Überschriften in Zeile 1. Achten Sie darauf, dass die Überschriften genau mit denen in der Abbildung übereinstimmen und keine Leerzeichen enthalten. Die genauen Überschriften lauten:

- **EmailAddress** in Zelle A1
- **UserName** in Zelle B1
- **Password** in Zelle C1

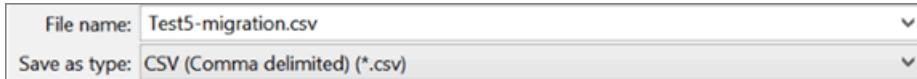
The screenshot shows a simple Excel spreadsheet with three columns labeled A, B, and C. The first row (row 1) contains the headers 'EmailAddress', 'UserName', and 'Password' respectively. Rows 2 through 6 are empty, representing where data will be input.

	A	B	C
1	EmailAddress	UserName	Password
2			
3			
4			
5			
6			

7. Geben Sie den e-Mail-Adresse, Username und app-Kennwort für jedes Postfach, den Sie migrieren möchten. Geben Sie ein Postfach pro Zeile ein.
- **Spalte A** ist die e-Mail-Adresse des Postfachs an Office 365. Dies ist was angezeigt wird, in der Spalte **Benutzername** in **Benutzer > aktive Benutzer** in Office 365 Administrationscenter.
  - **Spalte B** enthält jeweils den Anmeldenamen für das Gmail-Postfach des Benutzers, beispielsweise "alberta@contoso.com".
  - **Spalte C** enthält das App-Kennwort für das Gmail-Postfach des Benutzers. Die Erstellung des App-Kennworts wird unter [Migration von G Suite-Postfächern über das Office 365 Admin Center](#) beschrieben.

	A	B	C
1	EmailAddress	UserName	Password
2	alberta@Contoso.com	alberta@Contoso.com	Password1
3	mathew@Contoso.com	mathew@Contoso.com	Password2
4	bobby@Contoso.com	bobby@Contoso.com	Password3
5	katrina@Contoso.com	katrina@Contoso.com	Password4
6	irwin@Contoso.com	irwin@Contoso.com	Password5

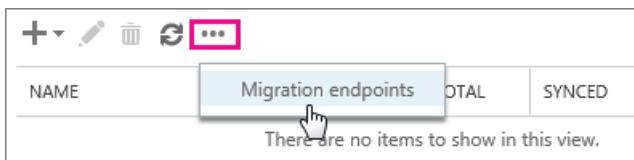
8. Speichern Sie die Datei als CSV-Datei, und schließen Sie Excel dann.



#### Schritt 4: Verbinden von Office 365 mit Gmail

Damit Gmail-Postfächer erfolgreich migriert werden können, muss Office 365 mit Gmail verbunden werden und mit Gmail kommunizieren können. Dazu verwendet Office 365 einen Migrationsendpunkt. Migrationsendpunkt ist ein technischer Begriff, der die Einstellungen beschreibt, mit denen die Verbindung hergestellt wird, damit Sie die Postfächer migrieren können. Sie erstellen den Migrationsendpunkt in dieser Aufgabe.

1. Wechseln Sie zum Exchange Admin Center.
2. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Migration > Weitere ... > migrationsendpunkte**.



3. Klicken Sie auf **neu +** um einen neuen migrationsendpunkt zu erstellen.
4. Wählen Sie auf der Seite **Typ des Migrationsendpunkts auswählen** die Option **IMAP** aus.
5. Legen Sie auf der Seite **IMAP-Migrationskonfiguration** das Feld **IMAP-Server** auf imap.gmail.com fest, und übernehmen Sie die Standardeinstellungen.
6. Klicken Sie auf **Weiter**. Der Migrationsdienst verwendet die Einstellungen, um die Verbindung mit dem Gmail-System zu testen. Wenn die Verbindung funktioniert, wird die Seite **Allgemeine Informationen eingeben** geöffnet.
7. Geben Sie auf der Seite **Allgemeine Informationen eingeben** einen *migrationsendpunktnamen* ein, beispielsweise Test5-Endpunkt. Lassen Sie die beiden anderen Felder leer, verwenden Sie die Standardwerte.

Help

### new migration endpoint

Enter general information

Enter the value for the general information for the migration endpoint that'll be applied to the associated migrations. [Learn more](#)

\*Migration endpoint name:

Maximum concurrent migrations:

Maximum concurrent incremental syncs:

[back](#) [new](#) [cancel](#)

8. Klicken Sie auf **Neu**, um den Migrationsendpunkt zu erstellen.

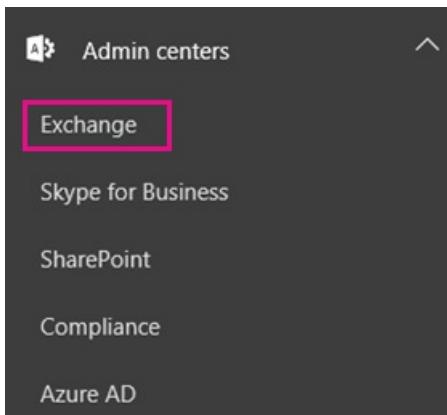
#### Schritt 5: Erstellen eines Migrationsbatchs und Starten des Migrierens von Gmail-Postfächern

Sie verwenden einen Migrationsbatch, um Gruppen von Gmail-Postfächern gleichzeitig nach Office 365 zu migrieren. Der Batch besteht aus den Gmail-Postfächern, die Sie in der Migrationsdatei in der vorherigen [Schritt 4: Verbinden von Office 365 mit Gmail](#) aufgelistet haben.

##### TIP

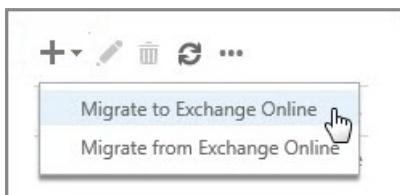
Es ist ratsam, einen Testmigrationsbatch mit einer kleinen Anzahl von Postfächern zu erstellen, um den Prozess zunächst zu testen. > Verwenden Sie die Migrationsdateien mit identischer Anzahl von Zeilen, und führen Sie die Batches zu ähnlichen Zeiten während des Tages aus. Vergleichen Sie dann die Gesamtausführungszeiten aller Testbatches. Dies erleichtert Ihnen die Abschätzung, wie lange ein Migrieren aller Postfächer dauern könnte, wie umfangreich jeder Migrationsbatch sein sollte und wie viele gleichzeitige Verbindungen mit dem Quell-E-Mail-System verwendet werden sollten, um einen sinnvollen Kompromiss zwischen Migrationsgeschwindigkeit und Internetbandbreite zu erzielen.

1. Navigieren Sie im Office 365 Admin Center zu **Admin Center > Exchange**.

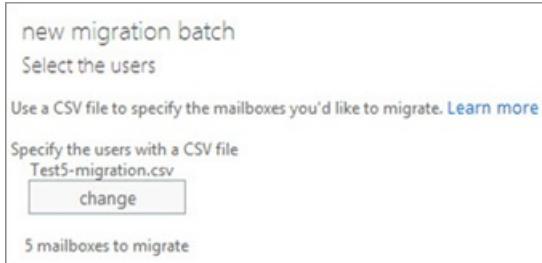


2. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.

3. Klicken Sie auf **neu + > zu Exchange Online migrieren**.

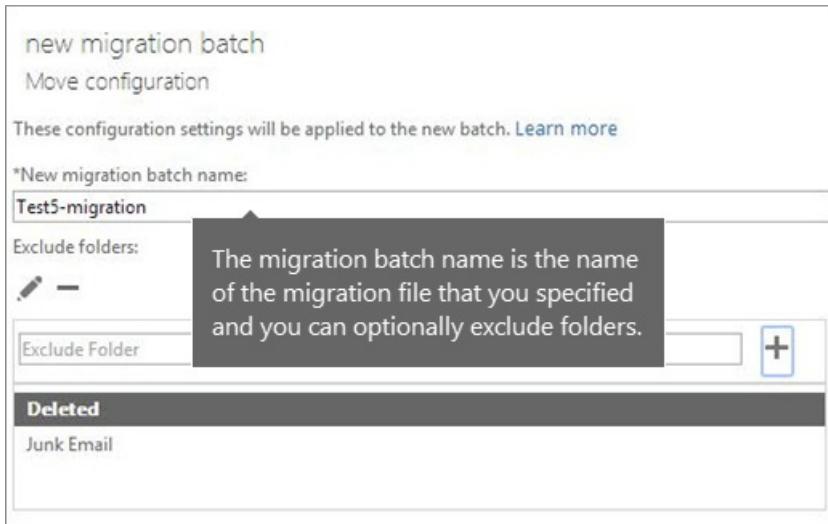


4. Wählen Sie **IMAP-Migration** > **Weiter** aus.
5. Klicken Sie auf der Seite **Benutzer auswählen** auf die Schaltfläche **Durchsuchen**, um die Migrationsdatei anzugeben, die Sie erstellt haben. Nachdem Sie Ihre Migrationsdatei ausgewählt haben, wird diese von Office 365 geprüft, um Folgendes sicherzustellen:
  - Die Datei ist nicht leer.
  - Sie ist mit Kommas als Trennzeichen formatiert.
  - Sie enthält nicht mehr als 50.000 Zeilen.
  - Sie enthält die erforderlichen Attribute in der Überschriftenzeile.
  - Sie enthält Zeilen mit derselben Anzahl von Spalten wie die Überschriftenzeile.Tritt bei einer dieser Prüfungen ein Fehler auf, wird eine Fehlermeldung angezeigt, in der der Grund für den Fehler beschrieben ist. Wird eine Fehlermeldung angezeigt, müssen Sie die Migrationsdatei korrigieren und erneut senden, damit ein Migrationsbatch erstellt wird.
6. Nachdem Office 365 die Migrationsdatei geprüft hat, wird die Anzahl von Benutzern, die in der Datei aufgeführt sind, als Anzahl der zu migrierenden Gmail-Postfächer angezeigt.



7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Migrationsendpunkt festlegen** den Migrationsendpunkt aus, den Sie im vorherigen Schritt erstellt haben, und klicken Sie auf **Weiter**.
9. Übernehmen Sie auf der Seite **IMAP-Migrationskonfiguration** die Standardwerte, und klicken Sie auf **Weiter**.
10. Geben Sie auf der Seite **Konfiguration verschieben** den *Namen* (ohne Leerzeichen oder Sonderzeichen) des migrationsbatches im ein – beispielsweise Test5-Migration. Die Migration Batch Standardname, die angezeigt wird, ist der Name der Migrationsdatei, die Sie angegeben. Der Blattname Migration wird in der Liste migrationsdashboard angezeigt, nach dem Erstellen des migrationsbatches.

Sie können auch die Namen der Ordner eingeben, den, die Sie von der Migration ausschließen möchten. Beispielsweise Shared, Junk-e-Mail und gelöscht. Klicken Sie auf **Hinzufügen +** So fügen sie der Liste der ausgeschlossenen hinzu. Sie können auch auf **Bearbeiten** klicken + so ändern Sie einen Ordnernamen und **Löschen** – auf den Namen des Ordners löschen.



11. Klicken Sie auf **Weiter**.

12. Führen Sie auf der Seite **Batch starten** die folgenden Aktionen aus:

- Wählen Sie **Durchsuchen** aus, um eine Kopie der Migrationsberichte an andere Benutzer zu senden. Standardmäßig werden Migrationsberichte per E-Mail an Sie gesendet. Sie können auch über die Eigenschaftenseite des Migrationsbatches auf die Migrationsberichte zugreifen.
- Wählen Sie **Batch automatisch starten** > **Neu** aus. Die Migration beginnt sofort mit dem Status **Synchronisierung**.

Click to view the status for all current migration batches. <a href="#">Status for all batches</a>					
NAME	▲ STATUS	TOTAL	SYNCED	FINALIZED	FAILED
Test5-migration	Syncing	5	0	0	0

Status changes from Created to Syncing after the migration starts.

#### NOTE

Wenn der Status **Synchronisierung** längere Zeit angezeigt wird, wurden von Google möglicherweise Bandbreitenbeschränkungen festgelegt. Weitere Informationen hierzu finden Sie unter [Bandbreitenbeschränkungen](#).

### Überprüfen, ob die Migration erfolgreich war

- Navigieren Sie im Exchange Admin Center zu **Empfänger** > **Migration**. Vergewissern Sie sich, dass der Batch auf dem Migrationsdashboard angezeigt wird. Wenn die Migration erfolgreich abgeschlossen wurde, ist der Status gleich **Synchronisiert**.
- Wenn diese Aufgabe fehlschlägt, überprüfen Sie den zugeordneten Postfachstatusbericht auf bestimmte Fehler, und vergewissern Sie sich, dass Ihre Migrationsdatei die richtige Office 365-E-Mail-Adresse in der Spalte **EmailAddress** enthält.

### Überprüfen einer erfolgreichen Migration von Postfächern zu Office 365

- Bitten Sie die migrierten Benutzer, die folgenden Aufgaben auszuführen:
  - Besuchen Sie die [Office 365 - Anmeldeseite](#), und melden Sie sich mit Ihrem Benutzernamen und dem temporären Kennwort.
  - Aktualisieren Sie Ihr Kennwort, und legen Sie die Zeitzone fest. Es ist wichtig, dass Sie die richtige

Zeitzone auswählen, um sicherzustellen, dass Ihre Kalender- und E-Mail-Einstellungen korrekt sind.

- Wenn Outlook Web App geöffnet ist, senden Sie eine E-Mail-Nachricht an einen anderen Office 365-Benutzer, um zu überprüfen, ob Sie E-Mails senden können.
- Wählen Sie **Outlook** aus, und vergewissern Sie sich, dass Ihre E-Mail-Nachrichten und Ordner vollständig vorhanden sind.

### **Optional: Verringern von E-Mail-Verzögerungen**

Obwohl diese Aufgabe optional ist, lassen sich mit ihrer Ausführung Verzögerungen beim Empfangen von E-Mails in den neuen Office 365-Postfächern vermeiden.

Wenn Personen, die nicht zu Ihrer Organisation gehören, E-Mails an Sie senden, wird von den E-Mail-Systemen dieser Personen nicht jedes Mal geprüft, wohin die E-Mails gesendet werden sollen. Stattdessen speichern diese Systeme den Speicherort Ihres E-Mail-Systems anhand einer Einstellung in Ihrem DNS-Server, die als Gültigkeitsdauer (Time-to-live, TTL) bezeichnet wird. Wenn Sie den Speicherort Ihres E-Mail-Systems ändern, bevor die TTL abgelaufen ist, versucht das E-Mail-System des Absenders, E-Mails an den alten Speicherort zu senden, bevor es feststellt, dass sich der Speicherort geändert hat. Dies kann zu einer Verzögerung in der E-Mail-Zustellung führen. Eine Möglichkeit, dies zu vermeiden, besteht darin, den TTL-Wert zu verringern, den Ihr DNS-Server bereitstellt, die nicht zu Ihrer Organisation gehören. Dadurch werden die anderen Organisationen veranlasst, den Speicherort Ihres E-Mail-Systems häufiger zu aktualisieren.

Die meisten E-Mail-Systeme fordern jede Stunde eine Aktualisierung an, wenn ein kurzes Intervall, etwa 3.600 Sekunden (eine Stunde), festgelegt ist. Es wird empfohlen, dass Sie das Intervall mindestens auf diesen niedrigen Wert festlegen, bevor Sie die E-Mail-Migration starten. Diese Einstellung bietet allen Systemen, die E-Mails an Sie senden, genügend Zeit, die Änderung zu verarbeiten. Wenn Sie dann den endgültigen Umstieg auf Office 365 vorgenommen haben, können Sie den TTL-Wert wieder in ein längeres Intervall ändern.

Die TTL-Einstellung ändern Sie im Mail-Exchanger-Eintrag Ihres E-Mail-Systems, der auch als MX-Eintrag bezeichnet wird. Dieser Eintrag befindet sich in Ihrem öffentlichen DNS. Wenn Sie mehrere MX-Einträge haben, müssen Sie den Wert für jeden Eintrag auf 3.600 Sekunden oder weniger ändern.

Machen Sie sich keine Gedanken Sie, wenn Sie diese Aufgabe überspringen. Möglicherweise dauert es etwas länger, bis Sie E-Mails in Ihren neuen Office 365-Postfächern sehen, aber die E-Mails gelangen dorthin.

Wenn Sie Unterstützung für das Konfigurieren Ihrer DNS-Einstellungen benötigen, sollten Sie zu [Erstellen von DNS-Einträgen für Office 365, wenn Sie Ihre DNS-Einträge verwalten](#) wechseln.

### **Schritt 6: Aktualisieren Ihrer DNS-Einträge, um Gmail direkt an Office 365 weiterzuleiten**

E-Mail-Systeme verwenden einen als MX-Eintrag bezeichneten DNS-Eintrag, um zu ermitteln, wohin E-Mails gesendet werden sollen. Während der E-Mail-Migration hat Ihr MX-Eintrag auf Ihr Gmail-System verwiesen. Nachdem Sie die E-Mail-Migration zu Office 365 nun abgeschlossen haben, sollte Ihr MX-Eintrag auf Office 365 verweisen. Nachdem Sie Ihren MX-Eintrag durch Ausführen dieser Schritte geändert haben, werden E-Mails, die an Benutzer in Ihrer benutzerdefinierten Domäne gesendet werden, an Office 365-Postfächer übermittelt.

Für viele DNS-Anbieter gibt es spezielle Anweisungen zum Ändern des MX-Eintrags. Sie finden diese Anweisungen unter [Erstellen von DNS-Einträgen für Office 365, wenn Sie Ihre DNS-Einträge verwalten](#). Für den Fall, dass Ihr DNS-Anbieter nicht aufgeführt ist oder Sie eine Vorstellung von den allgemeinen Anweisungen erhalten möchten, stehen auch allgemeine Anweisungen für MX-Einträge bereit. Sie finden diese Anweisungen unter [Erstellen von DNS-Einträgen bei einem beliebigen DNS-Hostinganbieter für Office 365](#).

1. Melden Sie sich bei Office 365 mit Ihrem Geschäfts-, Schul- oder Unikonto an.
2. Wählen Sie **Setup > Domänen** aus.
3. Wählen Sie Ihre Domäne aus, und klicken Sie dann auf **Probleme beheben**.

Als Status wird **Probleme beheben** angezeigt, weil Sie den Assistenten auf halbem Weg gestoppt haben, sodass Sie Ihre Gmail-E-Mails zu Office 365 migrieren konnten, bevor Sie Ihren MX-Eintrag ändern.

DOMAIN NAME	STATUS	ACTION
Cohocafe.com	Setup not started	<a href="#">Start setup</a>
contoso.com (Default)	Possible service issues	<a href="#">Fix issues</a>

4. Wählen Sie für jeden DNS-Eintragstyp, den Sie hinzufügen müssen, **Was korrigiere ich?** aus, und folgen Sie den Anweisungen, um die Einträge für Office 365-Dienste hinzuzufügen.
5. Nachdem Sie alle Einträge hinzugefügt haben, wird in einer Meldung angezeigt, dass Ihre Domäne ordnungsgemäß eingerichtet wurde: **Contoso.com ist ordnungsgemäß eingerichtet. Es ist keine Aktion erforderlich.**

Es kann bis zu 72 Stunden dauern, bis die E-Mail-Systeme Ihrer Kunden und Partner den geänderten MX-Eintrag erkannt haben. Warten Sie mindestens 72 Stunden, bevor Sie die Schritte ausführen, in denen die Synchronisierung mit Gmail beendet wird.

### Schritt 7: Beenden der Synchronisierung mit Gmail

In der letzten Aufgabe haben Sie den MX-Eintrag für Ihre Domäne aktualisiert. Nun sollten Sie überprüfen, ob alle E-Mails an Office 365 weitergeleitet werden. Nach der Überprüfung können Sie den Migrationsbatch löschen und die Synchronisierung zwischen Gmail und Office 365 beenden. Bevor Sie diesen Schritt ausführen:

- Vergewissern Sie sich, dass die Benutzer für ihre E-Mails ausschließlich Office 365 verwenden. Nachdem Sie den Migrationsbatch gelöscht haben, werden E-Mails, die an Gmail-Postfächer gesendet wurden, nicht nach Office 365 kopiert. Das bedeutet, dass die Benutzer diese E-Mails nicht erhalten, also sollten Sie sicherstellen, dass sich alle Benutzer im neuen System befinden.
- Löschen Sie den Migrationsbatch erst, nachdem er mindestens 72 Stunden ausgeführt wurde. Dadurch werden die beiden folgenden Punkte wahrscheinlicher:
  - Ihre Gmail-Postfächer und Office 365-Postfächer wurden mindestens einmal synchronisiert (sie werden einmal pro Tag synchronisiert).
  - Die E-Mail-Systeme Ihrer Kunden und Partner haben die Änderungen an den MX-Einträgen erkannt und senden jetzt ordnungsgemäß E-Mails an Ihre Office 365-Postfächer.

Wenn Sie den Migrationsbatch löschen, bereinigt der Migrationsdienst alle Einträge, die mit dem Migrationsbatch zu tun haben, und entfernt den Batch dann aus dem Migrationsdashboard.

### Löschen eines Migrationsbatches

1. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.
2. Wählen Sie auf dem Migrationsdashboard den Batch aus, und klicken Sie dann auf **Löschen**.

### Woher wissen Sie, ob dieser Vorgang erfolgreich war?

- Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**. Vergewissern Sie sich, dass der Migrationsbatch nicht mehr auf dem Migrationsdashboard aufgelistet wird.

### Schritt 8: Migrieren der Kalender und Kontakte durch die Benutzer

Nachdem Sie die E-Mails der Benutzer migriert haben, können diese ihre Gmail-Kalender und Kontakte in

Outlook importieren:

- [Importieren von Kontakten in Outlook](#)
- [Importieren des Google-Kalenders in Outlook](#)

## Bitte geben Sie uns Feedback

Waren diese Schritte hilfreich? Wenn das der Fall ist, lassen Sie uns dies bitte am Ende des Themas wissen. Wenn die Schritte nicht hilfreich waren und Sie weiterhin Probleme mit dem Migrieren Ihrer E-Mails haben, sagen Sie uns Bescheid. Wir verwenden Ihr Feedback, um unsere Verfahrensschritte noch einem zu überprüfen.

## Verwandte Themen

[IMAP-Migration im Office 365 Admin Center](#)

[Migrieren von IMAP-Postfächern zu Office 365](#)

[Möglichkeiten zum Migrieren von E-Mail zu Office 365](#)

[Tipps für die Optimierung von IMAP-Migrationen](#)

# Migrieren anderer Typen von IMAP-Postfächern zu Office 365

18.12.2018 • 36 minutes to read

Als Teil des Prozesses der Bereitstellung von Office 365 können Sie wählen, dass die Inhalte von Benutzerpostfächern von einem IMAP-E-Mail-Dienst (Internet Mail Access Protocol) nach Office 365 migriert werden.

Suchen Sie nach Windows PowerShell-Befehlen für allgemeine IMAP-Migrationen? Informationen finden Sie unter [Verwenden von PowerShell zum Durchführen einer IMAP-Migration nach Office 365](#).

## Migrationsaufgaben für IMAP-Postfächer

### NOTE

Sie müssen die Benutzer in Office 365 erstellen, bevor Sie ihre IMAP-Postfächer aus dem Quellsystem migrieren. Jeder Benutzer verfügt über ein vorhandenes Office 365-Postfach haben, dem Sie Ihre e-Mail-Nachrichten zu importieren. Wenn Sie eine Domäne mit Ihrem IMAP-System verwenden und auch mit Office 365 verwenden möchten, müssen Sie zu Office 365 als Hinzufügen einer akzeptierten Domäne, bevor Sie Benutzer in Office 365 erstellen. Anweisungen finden Sie unter [Hinzufügen einer Domäne zu Office 365](#). Wenn Sie Office 365 von 21Vianet in China betrieben verwenden, finden Sie unter [Hinzufügen Ihrer Domäne und Benutzer zu Office 365](#) handelt, das von 21Vianet. Zum Hinzufügen von Benutzern finden Sie unter [Benutzer einzeln oder in einer Sammeloperation zu Office 365 - Admin Hilfe hinzufügen](#) oder Office 365 handelt, das von 21Vianet finden Sie unter [Hinzufügen, bearbeiten, löschen oder Wiederherstellen von Benutzerkonten in Office 365](#) handelt, das von 21Vianet - Admin-Hilfe.

Hier sind die Aufgaben, die Sie durchführen müssen, wenn Sie mit einer Migration Ihrer IMAP-Postfächer beginnen möchten.

### Schritt 1: Suchen des vollständigen Namens Ihres aktuellen E-Mail-Servers

Office 365 benötigt den Namen des Quell-E-Mail-Systems, manchmal als Server bezeichnet, aus dem Sie Postfächer migrieren möchten. Es gibt viele Möglichkeiten, den Namen Ihres E-Mail-Systems zu ermitteln. Die einfachste Möglichkeit ist, einen E-Mail-Client zu verwenden, der mit Ihrem E-Mail-System verbunden ist. In dieser Aufgabe wird erläutert, wie Sie den Namen des Systems mit Outlook Web App ermitteln. Wenn Ihr E-Mail-Client hier nicht beschrieben ist, wenden Sie sich an den Support Ihres Quell-E-Mail-Systems.

### Abrufen des Namens Ihres E-Mail-Quellsystems mithilfe von TE102821288

1. Klicken Sie in Outlook Web App auf der Symbolleiste auf **Einstellungen** > **Optionen** > **Mail** > **Konten** > **POP und IMAP**. Unten Ihre Kontoinformationen sehen Sie eine Verknüpfung mit der Meldung von **Einstellungen für POP- und IMAP-Zugriff**. Name des IMAP-Servers wird unter IMAP-Einstellung aufgeführt.

## POP and IMAP settings

Use the information on this page if you need to use POP or IMAP to connect your mailbox.

### POP setting

Server name: outlook.office365.com  
Port: 995  
Encryption method: SSL

### IMAP setting

Server name: outlook.office365.com  
Port: 993  
Encryption method: SSL

Your IMAP server name, if enabled,  
is listed under IMAP setting.

### SMTP setting

Server name: smtp.office365.com  
Port: 587  
Encryption method: TLS

Weitere Informationen zu IMAP-Verbindungen in Office 365 finden Sie unter [Verwenden von POP oder IMAP für die Herstellung der Verbindung zu Office 365 Business- oder Microsoft Exchange-Konten](#).

## Schritt 2: Erstellen der Liste der zu migrierenden Postfächer

Die Schritte, die zum Erstellen der Liste der Postfächer auszuführen sind, hängen davon ab, wie Sie auf die Postfächer zugreifen. Sie benötigen Zugriff auf die Benutzerpostfächer, bevor Sie diese zu Office 365 migrieren können. Es gibt zwei Möglichkeiten, wie Sie Zugriff auf die Postfächer erhalten können:

- Entweder Sie wissen die Kennwörter für die Postfächer der Benutzer, oder Sie setzen die Kennwörter auf neue Kennwörter zurück, die Sie wissen. Führen Sie Schritte aus, die unter [Erstellen der Liste der Benutzerpostfächer, wenn Sie die Benutzerkennwörter wissen, oder Zurücksetzen der Kennwörter](#) aufgeführt sind.
- Ihr Quell-E-Mail-System ermöglicht es Ihnen, über die Anmeldeberechtigungen eines Postfachadministrators auf die Benutzerpostfächer zuzugreifen, was bedeutet, dass Sie die Kennwörter weder wissen noch zurücksetzen müssen. Führen Sie die Schritte unter [Erstellen einer Liste von Benutzerpostfächern mithilfe von Administratoranmeldeberechtigungen für den Zugriff](#), um zu erfahren, wie Sie auf Benutzerpostfächer zugreifen.

### Erstellen der Liste der Benutzerpostfächer, wenn Sie die Benutzerkennwörter wissen, oder Zurücksetzen der Kennwörter

Für diese Aufgabe erstellen Sie eine Migrationsdatei, die eine Liste der Postfächer enthält, die nach Office 365 migriert werden sollen. Hier wird Excel in den Anweisungen verwendet, da dies die einfachste Möglichkeit ist, die Migrationsdatei zu erstellen. Sie können Excel 2013, Excel 2010 oder Excel 2007 verwenden.

Wenn Sie die Migrationsdatei erstellen, müssen Sie das Kennwort für jedes Postfach wissen, das migriert werden soll. Da Sie die Benutzerkennwörter vermutlich nicht wissen, müssen Sie wahrscheinlich allen Postfächern während der Migration temporäre Kennwörter zuweisen (durch Zurücksetzen der Kennwörter).

Sie müssen nicht alle Postfächer gleichzeitig migrieren. Sie können die Migration nach Zweckmäßigkeit in Batches vornehmen. Sie können bis zu 50.000 Postfächer (eine Zeile für jeden Benutzer) in die Migrationsdatei einfügen, deren maximale Größe 10 MB beträgt.

Weitere Informationen finden Sie unter [CSV-Dateien für IMAP-Migrationsbatches](#).

1. Wechseln Sie zu Ihrem E-Mail-System (dasjenige, aus dem Sie migrieren), und navigieren Sie zu der Liste der Postfächer, die Sie migrieren möchten.

Wir würden Ihnen die genauen Schritte mitteilen, wenn wir könnten, aber es gibt so viele verschiedene E-Mail-Systeme, dass Sie diese Schritte selbst in Erfahrung bringen müssen. Wenn Sie die Liste der Postfächer gefunden haben, belassen Sie dieses Fenster geöffnet.

- Navigieren Sie zum Office 365 Admin Center.
- Navigieren Sie zu **Benutzern** > **aktive Benutzer**. Achten Sie auf der Spalte **Benutzername**. Verwenden Sie diese Informationen in einer Minute. Lassen Sie das Office 365 Administrationscenter geöffnet, zu.

Select a view: All users

DISPLAY NAME    USER NAME    STATUS

	DISPLAY NAME	USER NAME	STATUS
<input type="checkbox"/>	Albert	Albert@Contoso.com	In cloud
<input type="checkbox"/>	Bobby	Bobby@Contoso.com	In cloud
<input type="checkbox"/>	Irwin Hume	irwin@Contoso.com	In cloud
<input type="checkbox"/>	Katrina Hernandez	katrina@Contoso.com	In cloud
<input type="checkbox"/>	Mathew Slattery	mathew@Contoso.com	In cloud

**Note:** Navigate to **Users > Active users** to keep track of the USER NAME column.

- Starten Sie Excel.
- Verwenden Sie das folgende Bildschirmfoto als Vorlage zum Erstellen der Migrationsdatei in Excel. Beginnen Sie mit den Überschriften in Zeile 1. Achten Sie darauf, dass die Überschriften genau mit denen in der Abbildung übereinstimmen und keine Leerzeichen enthalten. Die genauen Überschriften lauten:

- EmailAddress** in Zelle A1
- UserName** in Zelle B1
- Password** in Zelle C1

	A	B	C
1	EmailAddress	UserName	Password
2			
3		Make sure your spreadsheet matches this picture exactly and doesn't contain spaces.	
4			
5			
6			

- Geben Sie im nächsten Schritt die e-Mail-Adresse, Benutzername und Kennwort für jedes Postfach, das Sie migrieren möchten. Geben Sie ein Postfach pro Zeile ein:
- Spalte A** ist die e-Mail-Adresse des Postfachs an Office 365. Dies ist was angezeigt wird, in der Spalte **Benutzername** unter **Benutzer > aktive Benutzer** in Office 365 Administrationscenter.
  - Spalte B** enthält jeweils den Anmeldenamen - beispielsweise "albertha" oder häufig "albertha@contoso.com" - für das Postfach des Benutzers im Quell-E-Mail-System.

#### NOTE

Viele E-Mail-Systeme verwenden die vollständige E-Mail-Adresse als Anmeldenamen. Beachten Sie auch, dass die Spalten A und B identisch sein können, wenn Sie in Office 365 und Ihrem Quell-E-Mail-System dieselbe Domäne verwenden.

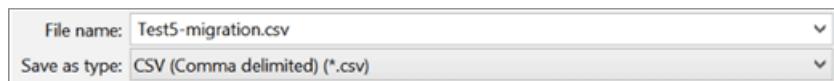
- Spalte C** enthält das Kennwort für das Postfach des Benutzers.

	A	B	C	
1	EmailAddress	UserName	Password	
2	<a href="mailto:alberta@contoso.com">alberta@contoso.com</a>	alberta	password1	
3	<a href="mailto:mathew@contoso.com">mathew@contoso.com</a>	mathew	password2	
4	<a href="mailto:bot@contoso.com">bot</a>	Enter one mailbox per row with the email address, user name, and password for each mailbox you want to migrate.		
5	<a href="mailto:kat@contoso.com">kat</a>			
6	<a href="mailto:irw@contoso.com">irw</a>			

Wenn Sie die Kennwörter der Benutzer nicht wissen, müssen Sie diese Kennwörter auf Ihnen bekannte Kennwörter zurücksetzen und dann diese Kennwörter in die Migrationsdatei eingeben. Dies ist für Benutzer unbequem, aber es führt kein Weg daran vorbei, es sei denn, Ihr Quell-E-Mail-System unterstützt Superuser-Anmeldeinformationen.

Wenn Benutzer Zugriff auf das Quell-E-Mail-System haben sollen, können Sie nach Abschluss der Migration neue Kennwörter an das Quell-E-Mail-System verteilen. In der vorliegenden Vorgehensweise werden die neuen Kennwörter verteilt, nachdem die Migration abgeschlossen ist.

7. Setzen Sie die Kennwörter zurück, und notieren Sie sich die neuen Kennwörter in der Migrationsdatei. Die genauen Schritte hängen von Ihrem Quell-E-Mail-System ab. Die Option zum Zurücksetzen eines Kennworts können Sie vermutlich finden, wenn Sie das E-Mail-Konto des Benutzers anzeigen.
8. Speichern Sie die Datei als CSV-Datei, und schließen Sie Excel.



#### **Erstellen einer Liste von Benutzerpostfächern mithilfe von Administratoranmeldeberechtigungen für den Zugriff**

Für diese Aufgabe erstellen Sie eine Migrationsdatei, die eine Liste der Postfächer enthält, die nach Office 365 migriert werden sollen. Am einfachsten lässt sich die Migrationsdatei mit Excel erstellen, weshalb Excel in diesen Anleitungen verwendet wird. Sie können Excel 2013, Excel 2010 oder Excel 2007 verwenden.

Wenn Sie eine Migrationsdatei für diese Aufgabe erstellen, geben Sie Ihr Postfach Administratoranmeldeinformationen und Benutzernamen, die Verwendung eines speziellen Formats ein. Dadurch können Sie den Zugriff auf Benutzerpostfächer ohne wissen oder die Benutzerkennwörter zurücksetzen. Wir stellen das Format von Exchange, Dovecot und Mirapoint IMAP-Servern verwendet. Wenn es sich bei Ihrem e-Mail-System nicht hier aufgeführt, und Sie nicht das richtige Format kennen, müssen Sie dennoch die Möglichkeit, Zurücksetzen von Benutzerkennwörtern. Überspringen Sie diesen Schritt, und wechseln Sie zum [Erstellen der Liste der Benutzerpostfächer, wenn Sie wissen, dass die Benutzerkennwörter oder benötigen Sie die Kennwörter zurücksetzen](#).

Sie müssen nicht alle Postfächer gleichzeitig migrieren. Sie können sie nach Zweckmäßigkeit in Batches migrieren. Sie können bis zu 50.000 Postfächer (eine Zeile für jeden Benutzer) in die Migrationsdatei einfügen, deren maximale Größe 10 MB beträgt.

1. Wechseln Sie zu Ihrem E-Mail-System (dasjenige, aus dem Sie migrieren), und navigieren Sie zu der Liste der Postfächer, die Sie migrieren möchten. Wir würden Ihnen die genauen Schritte mitteilen, wenn wir könnten, aber es gibt so viele verschiedene E-Mail-Systeme, dass Sie diese Schritte selbst in Erfahrung bringen müssen. Wenn Sie die Liste der Postfächer gefunden haben, belassen Sie dieses Fenster geöffnet, damit Sie sich auf die Postfächer beziehen können.
2. Navigieren Sie zum Office 365 Admin Center.
3. Navigieren Sie zu **Benutzern > aktive Benutzer**. Achten Sie auf der Spalte **Benutzername**. Verwenden Sie diese Informationen in einer Minute. Beibehalten der Office 365 Admin Center-Seite zu öffnen.

Select a view:		
	DISPLAY NAME	USER NAME
	STATUS	
<input type="checkbox"/>	Albert	Navigate to <b>Users &gt; Active users</b> to keep track of the USER NAME column.
<input type="checkbox"/>	Bobby	In cloud
<input type="checkbox"/>	Irwin Hume	irwin@Contoso.com
<input type="checkbox"/>	Katrina Hernandez	katrina@Contoso.com
<input type="checkbox"/>	Mathew Slattery	mathew@Contoso.com
		In cloud
		In cloud
		In cloud

4. Starten Sie Excel.
5. Verwenden Sie das folgende Bildschirmfoto als Vorlage zum Erstellen der Migrationsdatei in Excel.  
Beginnen Sie mit den Überschriften in Zeile 1. Achten Sie darauf, dass die Überschriften genau mit denen auf dem Bildschirmfoto übereinstimmen und keine Leerzeichen enthalten. Die genauen Überschriften lauten:

- **EmailAddress** in Zelle A1
- **UserName** in Zelle B1
- **Password** in Zelle C1

	A	B	C
1	EmailAddress	UserName	Password
2			
3			
4		Make sure your spreadsheet matches this picture exactly and doesn't contain spaces.	
5			
6			

6. Geben Sie im nächsten Schritt die e-Mail-Adresse, Benutzername und Kennwort für jedes Postfach, das Sie migrieren möchten. Geben Sie ein Postfach pro Zeile ein.
- **Spalte A** ist der e-Mail-Adresse des Office 365-Postfach des Benutzers. Dies ist was angezeigt wird, in der Spalte **Benutzername** unter **Benutzer > aktive Benutzer** in Office 365 Administrationscenter.
- **Spalte B** ist die Kombination der Name des Postfachs Admin und Username, die speziell für das Quellsystem e-Mail ist. Finden Sie unter [Format Admin Postfachanmeldeinformationen für verschiedene IMAP-Server](#) zum Formatieren von Anweisungen.
- **Spalte C** ist das Kennwort für das Postfach-Administratorkonto.

7. Speichern Sie die Datei als CSV-Datei, und schließen Sie Excel dann.

	A	B	C
1	EmailAddress	UserName	Password
2	<a href="mailto:alberta@contoso.com">alberta@contoso.com</a>	alberta	password1
3	<a href="mailto:mathew@contoso.com">mathew@contoso.com</a>	mathew	password2
4	<a href="mailto:bob">bob</a>	Enter one mailbox per row with the email address, user name, and password for each mailbox you want to migrate.	
5	<a href="mailto:kat">kat</a>		
6	<a href="mailto:irw">irw</a>		

## Formatieren von Postfach-Administratoranmeldeinformationen für verschiedene IMAP-Server

In der Migrationsdatei jede Zelle in der Spalte **Benutzername** besteht aus zwei kombinierten Namen: der Benutzername der Person, deren e-Mail wird migriert, und den Benutzernamen des Kontos ein Postfach Admin. Das unterstützte Format für Admin Postfachanmeldeinformationen unterscheidet sich je nach Ihrem e-Mail-System. Hier sind die Formate für verschiedene Arten von e-Mail-Quellsystemen.

### Microsoft Exchange

Wenn beim Migrieren von e-Mail von IMAP-Implementierung für Exchange verwenden Sie das Format

**Domäne/Admin\_UserName/User\_UserName** für das Attribut **UserName** in der Migrationsdatei.

Angenommen, Sie e-Mails von Exchange für Interessen Greene, Bobby Overby, Irwin Hume, Katrina Hernandez und Matthew Slattery migrieren. Sie müssen ein Postfach Administratorkonto, in dem der Benutzername ist **Mailadmin** und das Kennwort lautet **\*\*P@ssw0rd\*\***. Nachfolgend finden Sie Ihre Migrationsdatei würde folgendermaßen aussehen:

	A	B	C
1	EmailAddress	UserName	Password
2	alberta@contoso.com	contoso/mailadmin/alberta	P@ssw0rd
3	mathew@contoso.com	contoso/mailadmin/mathew	P@ssw0rd
4	bobby@contoso.com	contoso/mailadmin/bobby	P@ssw0rd
5	katrina@contoso.com	contoso/mailadmin/katrina	P@ssw0rd
6	irwin@contoso.com	contoso/mailadmin/irwin	P@ssw0rd

### Dovecot

Für ein Quell-E-Mail-System, z. B. ein Dovecot-IMAP-Server, das SASL (Simple Authentication and Security Layer) unterstützt, wird das Format **Benutzer\_UserName\*Admin\_UserName** verwendet. Nehmen Sie an, Sie migrieren E-Mails von einem Dovecot-IMAP-Server mit den Postfach-Administratoranmeldeinformationen **mailadmin** und **\*\*P@ssw0rd\*\***. Ihre Migrationsdatei würde wie folgt aussehen:

	A	B	C
1	EmailAddress	UserName	Password
2	alberta@contoso.com	alberta*mailadmin	P@ssw0rd
3	mathew@contoso.com	mathew*mailadmin	P@ssw0rd
4	bobby@contoso.com	bobby*mailadmin	P@ssw0rd
5	katrina@contoso.com	katrina*mailadmin	P@ssw0rd
6	irwin@contoso.com	irwin*mailadmin	P@ssw0rd

### Mirapoint

Wenn Sie E-Mails aus Mirapoint Message Server migrieren, verwenden Sie das Format

**\*\*#Benutzer@Domäne#Admin\_UserName#\*\***. Nehmen Sie an, Sie migrieren E-Mails mit den Postfach-Administratoranmeldeinformationen **mailadmin** und **\*\*P@ssw0rd\*\***. Ihre Migrationsdatei würde wie folgt aussehen:

	A	B	C
1	EmailAddress	UserName	Password
2	alberta@contoso.com	#alberta@contoso.com#mailadmin#	P@ssw0rd
3	mathew@contoso.com	#mathew@contoso.com#mailadmin#	P@ssw0rd
4	bobby@contoso.com	#bobby@contoso.com#mailadmin#	P@ssw0rd
5	katrina@contoso.com	#katrina@contoso.com#mailadmin#	P@ssw0rd
6	irwin@contoso.com	#irwin@contoso.com#mailadmin#	P@ssw0rd

### Courier IMAP und Oracle IMAP

Einige Quelle e-Mail-Systemen wie Courier IMAP und Oracle IMAP unterstützen nicht mit Postfach-Administratoranmeldeinformationen zum Migrieren von Postfächern zu Office 365. Stattdessen können Sie Ihrem e-Mail-System einrichten, virtuelle freigegebenen Ordner verwenden. Virtuelle freigegebenen Ordner können Sie die Postfach-Admin-Anmeldeinformationen verwenden, um auf Benutzerpostfächer im Quellsystem-e-Mail zuzugreifen. Weitere Informationen zum Konfigurieren von virtuellen freigegebene Ordner für Courier IMAP, finden Sie unter [Freigegebene Ordner](#).

Um Postfächer zu migrieren, nachdem Sie virtuelle freigegebene Ordner in Ihrem Quell-E-Mail-System

eingerichtet haben, müssen Sie das optionale Attribut **UserRoot** in die Migrationsdatei einfügen. Dieses Attribut gibt für das Postfach jedes Benutzers den Speicherort an, den es im Quell-E-Mail-System in der Struktur der virtuellen freigegebenen Ordner hat. Das Postfach von Alberta hat beispielsweise den Pfad **/users/alberta**.

Dies ist ein Beispiel für eine Migrationsdatei, die das Attribut **UserRoot** enthält:

	A	B	C	D
1	EmailAddress	UserName	Password	UserRoot
2	alberta@contoso.com	mailadmin	P@ssw0rd	/users/alberta
3	mathew@contoso.com	mailadmin	P@ssw0rd	/users/mathew
4	bobby@contoso.com	mailadmin	P@ssw0rd	/users/bobby
5	katrina@contoso.com	mailadmin	P@ssw0rd	/users/katrina
6	irwin@contoso.com	mailadmin	P@ssw0rd	/users/irwin

### Schritt 3: Herstellen einer Verbindung zwischen Office 365 und Ihrem E-Mail-System

Damit E-Mails erfolgreich migriert werden können, muss Office 365 mit dem Quell-E-Mail-System verbunden werden und mit diesem System kommunizieren können. Dazu verwendet Office 365 einen Migrationsendpunkt. Dies ist ein technischer Begriff, der die Einstellungen beschreibt, mit denen die Verbindung hergestellt wird. Sie erstellen den Migrationsendpunkt in dieser Aufgabe.

1. Wechseln Sie zum Exchange Admin Center.
2. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Migration > Weitere ... > migrationsendpunkte**.



3. Klicken Sie auf **neu +** um einen neuen migrationsendpunkt zu erstellen.
4. Wählen Sie auf der Seite **Typ des Migrationsendpunkts auswählen** die Option **IMAP** aus.
5. Geben Sie auf der Seite **IMAP-Migrationskonfiguration** die folgende Informationen ein:
  - \*\* \* IMAP-Server\*\*: Geben Sie den *Servernamen messaging* (beispielsweise "IMAP.contoso.com") des Quellservers e-Mail.
  - Übernehmen Sie für die weiteren Informationen die Standardeinstellungen. Diese funktionieren in den meisten Fällen.
6. Klicken Sie auf **Weiter**. Der Migrationsdienst verwendet die Einstellungen, um die Verbindung mit Ihrem E-Mail-Server zu testen. Wenn die Verbindung funktioniert, wird die Seite **Allgemeine Informationen eingeben** angezeigt.
7. Geben Sie auf der Seite **Allgemeine Informationen eingeben** einen *migrationsendpunktnamen* ein, beispielsweise Test5-Endpunkt. Lassen Sie die beiden anderen Felder leer, verwenden Sie die Standardwerte.

Help

**new migration endpoint**

Enter general information

Enter the value for the general information for the migration endpoint that'll be applied to the associated migrations. [Learn more](#)

\*Migration endpoint name:  
 Type a Migration endpoint name, for example, Test5-endpoint. Leave the other two boxes blank to use the default values.

Maximum concurrent migrations:  
 Maximum concurrent in

Maximum concurrent in:

[back](#) [new](#) [cancel](#)

8. Klicken Sie auf **Neu**, um den Migrationsendpunkt zu erstellen.

#### Schritt 4: Erstellen eines Migrationsbatches und Migrieren der Postfächer

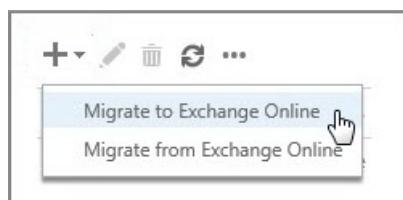
Sie verwenden einen Migrationsbatch, um Gruppen von E-Mail-Postfächern gleichzeitig nach Office 365 zu migrieren. Der Batch besteht aus den Postfächern, die Sie in der Migrationsdatei in der vorherigen Aufgabe aufgelistet haben.

##### TIP

Es empfiehlt sich, einen Testmigrationsbatch mit einer kleinen Anzahl von Postfächern zu erstellen, um den Prozess zunächst zu testen. > Verwenden Sie die Migrationsdateien mit identischer Anzahl von Zeilen, und führen Sie die Batches zu ähnlichen Zeiten während des Tages aus. Vergleichen Sie dann die Gesamtausführungszeiten aller Testbatches. Dieser Vergleich erleichtert Ihnen die Abschätzung, wie lange ein Migrieren aller Postfächer dauern könnte, wie umfangreich jeder Migrationsbatch sein sollte und wie viele gleichzeitige Verbindungen mit dem Quell-E-Mail-System verwendet werden sollten, um einen sinnvollen Kompromiss zwischen Migrationsgeschwindigkeit und Internetbandbreite zu erzielen.

1. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.

2. Klicken Sie auf **neu + > zu Exchange Online migrieren**.



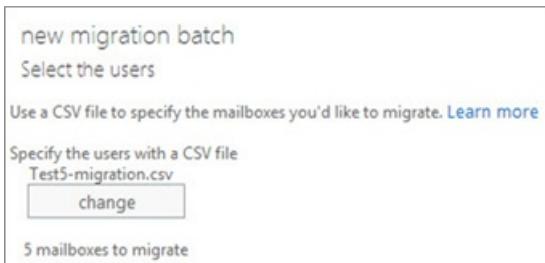
3. Wählen Sie **IMAP-Migration > Weiter** aus.

4. Klicken Sie auf der Seite **Benutzer auswählen** auf die Schaltfläche **Durchsuchen**, um die Migrationsdatei anzugeben, die Sie erstellt haben. Nachdem Sie Ihre Migrationsdatei ausgewählt haben, wird diese von Office 365 geprüft, um Folgendes sicherzustellen:

- Die Datei ist nicht leer.
- Sie ist mit Kommas als Trennzeichen formatiert.
- Sie enthält nicht mehr als 50.000 Zeilen.
- Sie enthält die erforderlichen Attribute in der Überschriftenzeile.
- Sie enthält Zeilen mit derselben Anzahl von Spalten wie die Überschriftenzeile.

Tritt bei einer dieser Prüfungen ein Fehler auf, wird eine Fehlermeldung angezeigt, in der der Grund für den Fehler beschrieben ist. Wird eine Fehlermeldung angezeigt, müssen Sie die Migrationsdatei korrigieren und erneut senden, damit ein Migrationsbatch erstellt wird.

5. Nachdem Office 365 die Migrationsdatei geprüft hat, wird die Anzahl von Benutzern, die in der Datei aufgeführt sind, als Anzahl der zu migrierenden Postfächer angezeigt.



6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf der Seite **IMAP-Migrationskonfiguration** auf die Schaltfläche **Weiter**.
8. Wählen Sie auf dieser Seite den Migrationsendpunkt aus, den Sie in [Schritt 3: Herstellen einer Verbindung zwischen Office 365 und Ihrem E-Mail-System](#) erstellt haben.
9. Klicken Sie auf der Seite **Konfiguration verschieben** Geben Sie den *Namen* (ohne Leerzeichen oder Sonderzeichen) des migrationsbatches, beispielsweise Test5-Migration, und klicken Sie dann auf **Weiter**.

Der standardmäßige Migrationsbatchname, der angezeigt wird, ist der Name der Migrationsdatei, die Sie angegeben haben. Die Migrationsbatchname wird in der Liste auf dem Migrationsdashboard angezeigt, nachdem Sie den Migrationsbatch erstellt haben.

Sie können die Namen der Ordner, den, die Sie migrieren, beispielsweise Shared, Junk-e-Mail und gelöschte verhindern möchten, optional auch eingeben. Klicken Sie auf **neu +** So fügen sie der Liste der ausgeschlossenen hinzu. Sie können auch auf **Bearbeiten** klicken + so ändern Sie einen Ordnernamen und **Löschen** – Name für einen Ordner löschen.

#### IMPORTANT

Wenn Sie E-Mails aus Microsoft Exchange Server migrieren, empfiehlt es sich, dass Sie öffentliche Ordner aus der Migration ausschließen. Tun Sie dies nicht, werden die Inhalte der öffentlichen Ordner in das Office 365-Postfach jedes Benutzers kopiert, der in der Migrationsdatei aufgeführt ist.

new migration batch

Move configuration

These configuration settings will be applied to the new batch. Learn more

\*New migration batch name:

Test5-migration

The migration batch name is the name of the migration file that you specified and you can optionally exclude folders.

Exclude folders:

Deleted

Junk Email

10. Klicken Sie auf **Weiter**.

11. Führen Sie auf der Seite **Batch starten** die folgenden Aktionen aus:

- Klicken Sie auf **Durchsuchen**, um eine Kopie der Migrationsberichte an andere Benutzer zu senden. Standardmäßig werden Migrationsberichte per E-Mail an Sie gesendet. Sie können auch über die Eigenschaftenseite des Migrationsbatches auf die Migrationsberichte zugreifen.
- Wählen Sie **Batch automatisch starten** aus. Die Migration wird gestartet, sobald Sie den neuen Migrationsbatch gespeichert haben. Der Batchstatus ist zunächst gleich **Erstellt** und ändert sich in **Synchronisierung**, nachdem die Migration begonnen wurde.

NAME	STATUS	TOTAL	SYNCED	FINALIZED	FAILED
Test5-migration	Syncing	5	0	0	0

### Überprüfen, ob diese Aufgabe erfolgreich ausgeführt wurde

- Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**. Vergewissern Sie sich, dass der Batch auf dem Migrationsdashboard angezeigt wird. Wenn die Migration erfolgreich abgeschlossen wurde, ist der **Status** gleich **Synchronisiert**.

Wenn diese Aufgabe fehlschlägt, überprüfen Sie den zugeordneten Postfachstatusbericht auf bestimmte Fehler, und vergewissern Sie sich, dass Ihre Migrationsdatei die richtige Office 365-E-Mail-Adresse in der Spalte **EmailAddress** enthält.

### Überprüfen einer erfolgreichen Migration von Postfächern zu Office 365

- Bitten Sie die Benutzer mit migrierten Postfächern, die folgenden Aufgaben auszuführen:
  - Melden Sie sich bei Office 365 mit Ihrer Arbeit oder Schule Konto. Verwenden Sie Ihr temporäre Kennwort ein.
  - Aktualisieren Sie Ihr Kennwort, und legen Sie die Zeitzone fest. Es ist wichtig, dass Sie die richtige Zeitzone auswählen, um sicherzustellen, dass Ihre Kalender- und E-Mail-Einstellungen korrekt sind.
  - Sobald Outlook Web App geöffnet ist, senden Sie eine E-Mail-Nachricht an einen anderen Office 365-Benutzer, um zu überprüfen, ob Sie E-Mails senden können.
  - Wählen Sie **Outlook** aus, und vergewissern Sie sich, dass Ihre E-Mail-Nachrichten und Ordner vollständig vorhanden sind.

### Optional: Verringern von E-Mail-Verzögerungen

**Diese Aufgabe ist optional.** Es ist nicht erforderlich, dass Sie diese Aufgabe ausführen, aber wenn Sie sie überspringen, kann es etwas länger, bis E-Mails erstmalig in den neuen Office 365-Postfächern angezeigt werden.

Wenn Personen, die nicht zu Ihrer Organisation gehören, E-Mails an Sie senden, wird von den E-Mail-Systemen dieser Personen nicht jedes Mal geprüft, wohin die E-Mails gesendet werden sollen. Stattdessen speichern diese Systeme den Speicherort Ihres E-Mail-Systems anhand einer Einstellung in Ihrem DNS-Server, die als Gültigkeitsdauer (Time-to-live, TTL) bezeichnet wird. Wenn Sie den Speicherort Ihres E-Mail-Systems ändern, bevor die TTL abgelaufen ist, versuchen die E-Mail-Systeme der Absender, E-Mails an den alten Speicherort zu senden, bevor sie feststellen, dass sich der Speicherort geändert hat. Dies kann zu einer Verzögerung in der E-Mail-Zustellung führen. Eine Möglichkeit, dies zu vermeiden, besteht darin, den TTL-Wert zu verringern, den Ihr

DNS-Server Servern bereitstellt, die nicht zu Ihrer Organisation gehören. Dadurch werden die anderen Organisationen veranlasst, den Speicherort Ihres E-Mail-Systems häufiger zu aktualisieren.

Die Verwendung eines kurzen Intervalls, z. B. 3.600 Sekunden (eine Stunde) oder weniger, bedeutet, dass die meisten E-Mail-Systeme jede Stunde einen aktualisierten Speicherort anfordern. Es wird empfohlen, dass Sie das Intervall mindestens auf diesen niedrigen Wert festlegen, bevor Sie die E-Mail-Migration starten. Dies bietet allen Systemen, die E-Mails an Sie senden, genügend Zeit, die Änderung zu verarbeiten. Wenn Sie dann den endgültigen Umstieg auf Office 365 vorgenommen haben, können Sie den TTL-Wert wieder in ein längeres Intervall ändern.

Die TTL-Einstellung ändern Sie im Mail-Exchanger-Eintrag Ihres E-Mail-Systems, der auch als MX-Eintrag bezeichnet wird. Der MX-Eintrag befindet sich auf Ihrem öffentlichen DNS-System. Wenn Sie mehrere MX-Einträge haben, müssen Sie den Wert für jeden Eintrag in 3.600 oder weniger ändern.

Machen Sie sich keine Gedanken Sie, wenn Sie diese Aufgabe überspringen. Möglicherweise dauert es etwas länger, bis Sie E-Mails in Ihren neuen Office 365-Postfächern sehen, aber die E-Mails gelangen dorthin.

Wenn Sie Unterstützung für das Konfigurieren Ihrer DNS-Einstellungen benötigen, sollten Sie [Erstellen von DNS-Einträgen für Office 365, wenn Sie Ihre DNS-Einträge verwalten](#) lesen. Bei Verwendung von Office 365, betrieben von 21Vianet in China lesen Sie stattdessen die folgende Version des Artikels: [Create DNS records for Office 365 when you manage your DNS records](#).

#### Schritt 5: Direktes Weiterleiten von E-Mails an Office 365

E-Mail-Systeme verwenden einen als MX-Eintrag bezeichneten DNS-Eintrag, um zu ermitteln, wohin E-Mails gesendet werden sollen. Während der E-Mail-Migration war Ihr MX-Eintrag so festgelegt, dass er auf Ihr Quell-E-Mail-System verwiesen hat. Nachdem die E-Mail-Migration zu Office 365 nun abgeschlossen ist, sollte Ihr MX-Eintrag auf Office 365 verweisen. Dadurch ist sichergestellt, dass E-Mails an Ihre Office 365-Postfächer gesendet werden. Das Verschieben des MX-Eintrags ermöglicht es Ihnen außerdem, das alte E-Mail-System zu deaktivieren, wenn Sie fertig sind.

Für viele DNS-Anbieter gibt es spezielle Anweisungen zum Ändern der MX-Einträge. Sie finden diese Anweisungen unter [Erstellen von DNS-Einträgen für Office 365, wenn Sie Ihre DNS-Einträge verwalten](#). Bei Verwendung von Office 365, betrieben von 21Vianet in China lesen Sie stattdessen die folgende Version des Artikels: [Create DNS records for Office 365 when you manage your DNS records](#). Für den Fall, dass Ihr DNS-Anbieter nicht aufgeführt ist oder Sie eine Vorstellung von den allgemeinen Anweisungen erhalten möchten, stehen auch allgemeine Anweisungen für MX-Einträge bereit. Sie finden diese Anweisungen unter [Erstellen von DNS-Einträgen bei einem beliebigen DNS-Hostinganbieter für Office 365](#). Bei Verwendung von Office 365 in China lesen Sie die folgende Version des Artikels: [Create DNS records at any DNS hosting provider for Office 365](#).

Es kann bis zu 72 Stunden dauern, bis die E-Mail-Systeme Ihrer Kunden und Partner den geänderten MX-Eintrag erkannt haben. Warten Sie mindestens 72 Stunden, bevor Sie die nächste Aufgabe ausführen, um die E-Mail-Synchronisierung zu beenden.

#### Schritt 6: Beenden der E-Mail-Synchronisierung

In der letzten Aufgabe haben Sie den MX-Eintrag geändert. Nun müssen Sie sich vergewissern, dass alle für Sie vorgesehenen E-Mails an Office 365 weitergeleitet werden. Danach können Sie den Migrationsbatch löschen. Dieses Löschen bewirkt, dass die Synchronisierung zwischen Ihrem Quell-E-Mail-System und Office 365 beendet wird. Vor dem Löschen sollten Sie sicherstellen, dass Folgendes zutrifft:

- Die Benutzer verwenden für ihre E-Mails ausschließlich Office 365. Nachdem Sie den Migrationsbatch gelöscht haben, werden E-Mails, die an Postfächer in Ihrem Quell-E-Mail-System gesendet wurden, nicht nach Office 365 kopiert. Dies bedeutet, dass Ihre Benutzer diese E-Mails nicht empfangen können. Daher sollten Sie sicherstellen, dass sich alle Benutzer im neuen System befinden.
- Löschen Sie den Migrationsbatch erst, nachdem er mindestens 72 Stunden ausgeführt wurde. Dadurch

werden die beiden folgenden Punkte viel wahrscheinlicher:

- Ihr Quell-E-Mail-System- und Office 365-Postfächer wurden mindestens einmal synchronisiert (sie werden einmal pro Tag synchronisiert).
- Die E-Mail-Systeme Ihrer Kunden und Partner haben die Änderungen an den MX-Einträgen erkannt und senden jetzt ordnungsgemäß E-Mails an Ihre Office 365-Postfächer.

Wenn Sie den Migrationsbatch löschen, bereinigt der Migrationsdienst alle Einträge, die mit dem Migrationsbatch zu tun haben, und entfernt den Batch dann aus dem Migrationsdashboard.

### Löschen eines Migrationsbatches

1. Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**.
2. Wählen Sie auf dem Migrationsdashboard den Batch aus, und klicken Sie dann auf **Löschen**.

Click to view the status for all current migration batches. <a href="#">Status for all batches</a>				
NAME	STATUS	TOTAL	SYNCED	
Test5-migration	Synced	5	5	

### Bestätigen, dass der Löschvorgang erfolgreich war

- Navigieren Sie im Exchange Admin Center zu **Empfänger > Migration**. Vergewissern Sie sich, dass der Migrationsbatch nicht mehr auf dem Migrationsdashboard aufgeführt wird.

### Siehe auch

[Migrieren von IMAP-Postfächern zu Office 365](#)

[Möglichkeiten zum Migrieren von E-Mail zu Office 365](#)

[Tipps für die Optimierung von IMAP-Migrationen](#)

# IMAP-Migration in Office 365 Administrationscenter

18.12.2018 • 6 minutes to read

Nachdem Sie Ihre Benutzer zu Office 365 hinzugefügt haben, können Sie Internet Message Access Protocol (IMAP) zum Migrieren von e-Mail für diese Benutzer von ihren IMAP-aktiviertes e-Mail-Server verwenden.

Wechseln Sie in das Office 365 Administrationscenter zu **Setup > Datenmigration** zu migrieren, IMAP-e-Mails aktiviert. Die e-Mail-Migrationen Seite ist für Migrationen von Google Mail, Outlook, Hotmail und Yahoo vorkonfiguriert. Sie können auch eingeben eigener IMAP-Server und die Verbindungszeichenfolge Parameter, um von einem e-Mail-Dienst zu migrieren, die nicht aufgeführt ist.

## IMPORTANT

Bevor Sie eine IMAP-Migration für Ihre Benutzer verwenden können, müssen haben sie zuerst Ihrem Office 365-Mandanten hinzugefügt. Anweisungen finden Sie unter [Hinzufügen von Benutzern zu Office 365 für Unternehmen](#).

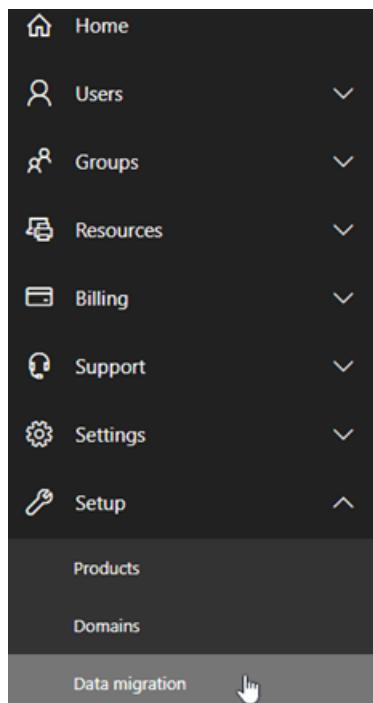
Lesen Sie vor der Migration, [Was Sie benötigen zum Migrieren Ihrer IMAP-Postfächern zu Office 365 kennen](#).

Zum Ausführen einer IMAP-Migrations mithilfe der Exchange-Verwaltungskonsole (EAC) finden Sie unter [Migrieren von anderen Arten von IMAP-Postfächern zu Office 365](#).

Zum Migrieren von Exchange-Mail zu Office 365 finden Sie unter [Verwendung express Migration zu Exchange-Postfächern zu Office 365 migrieren](#)

## Migrieren von IMAP-Postfächern zu Office 365

1. Melden Sie sich die [Informationen zu Office 365 Administrationscenter](#).
2. Navigieren Sie zu **Setup > Datenmigration**.



**Wählen Sie den Datendienst** Dashboard wird geöffnet.

## Select your data service.

You can migrate your users' data after connecting to your email service, or upload files directly.



Important: Before you migrate data, you need to complete a few steps to prepare.



Important: Before you migrate data, you need to complete a few steps to prepare.



Important: Before you migrate data, you need to complete a few steps to prepare.



Other email sources...

### 3. Vom Dienstanbieter wird aufgeführt:

- Wählen Sie den e-Mail-Anbieter, von dem Sie migrieren.

#### IMPORTANT

Wenn Sie e-Mails von Google Mail migrieren, müssen Sie die Benutzer zum Erstellen eines app-Kennwort zu erhalten, Sie anstelle von ihr Kontokennwort verwenden müssen. Wenn Sie e-Mails von Outlook.com oder Hotmail.com migrieren, müssen Sie bitten Sie die Benutzer in zwei Schritten Überprüfung einrichten und ein Kennwort für die app zu erhalten. Wenn Sie eine Verbindung zwischen Outlook.com oder Hotmail.com und Office 365 herstellen, verwenden Sie eine ihrer app Kennwort anstelle von ihr Kontokennwort.

- Nachdem Sie einen Anbieter auswählen, werden alle Benutzer die Seite Wählen Sie Benutzer zu migrieren, e-Mail-Nachrichten mit der e-Mail-Quelle vorab ausgefüllt aufgelistet.

The screenshot shows a user interface for selecting users for migration. At the top, there are buttons for 'Start migration', 'Stop migration', 'Close connection', and 'Settings'. Below these are fields for 'Display name' (with a dropdown arrow), 'Source email', 'Password', and 'Status'. A table lists two users: Alberta Greene (@outlook.com) and Alex Darrow (@outlook.com). Both users have checkboxes next to their names, and the checkboxes for both are checked.

Display name	Source email	Password	Status
Alberta Greene	@outlook.com		
Alex Darrow	@outlook.com		

#### Ihr Provider ist nicht aufgeführt:

- Wählen Sie aus anderen Quellen e-Mail:
- Füllen Sie auf der Seite Wählen Sie den Datendienst in die entsprechenden IMAP-Verbindungsdaten zum Testen der Verbindung. Sie können jedes Konto für diese verwenden.

Das folgende Beispiel für eine Google apps-Domäne "contoso.com" ist, und den Namen des IMAP-Servers ist daher imap.gmail.com.

Da das Beispiel für Google apps ist, beachten Sie, dass das Kennwort das Kennwort 16-stellige app für die e-Mail-Konto, der eingegeben wird ist, um zu überprüfen, die Verbindung mit dem Server.

#### IMPORTANT

Wenn Sie e-Mails von Google Apps migrieren, in dem Sie die Domäne besitzen, müssen Sie die Benutzer zum Erstellen eines app-Kennwort zu erhalten, Sie anstelle von ihr Kontokennwort verwenden müssen.

Select your data service.

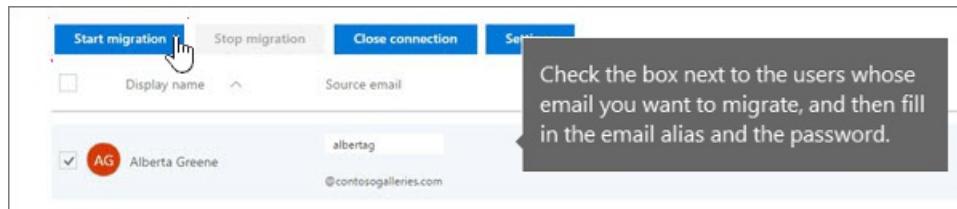
Please let us know how to connect with your email service.

IMAP server name *	Port *	Security *
imap.gmail.com	: 993	<input checked="" type="radio"/> SSL <input type="radio"/> TLS
Email address *	<input type="text" value="albertag@contoso.com"/>	
Password *	<input type="password" value="*****"/> 	
<p>Note that the password is the 16-digit Google app password for the email account to verify the server connection.</p>		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

3. Klicken Sie auf **Speichern**, um die Verbindung zu testen. Nachdem die Verbindung überprüft worden ist, werden die **e-Mail-Migration** Statusseite alle hinzugefügten Benutzer mit der e-Mail-Adresse aufgelistet, die Sie bereitgestellt.
4. **Dies und die folgenden Schritte gelten für sowohl einen aufgeführten e-Mail-Anbieter oder "Andere":**

Aktivieren Sie das Kontrollkästchen neben den Benutzern, deren e-Mail zu migrieren, und geben Sie dann den e-Mail-Alias und das Kennwort (app Wenn Sie migrieren von e-Mails von Google Mail oder Google apps sind).

5. Wählen Sie die **Migration starten**, nachdem Sie die erforderliche Informationen eingegeben haben.



6. Der Status der Migration werden:

- **Starten**
- **In der Warteschlange**
- **Synchronisierung**
- **Synchronisiert**

Wenn der Status **synchronisiert** ist weiterhin die IMAP-Migration synchronisieren mit der e-Mail-Quelle in regelmäßigen Abständen, bis Sie auswählen, dass die **Migration zu beenden**.

Wenn Sie fertig sind, wählen Sie **Verbindung schließen**. Dadurch können Sie eine neue Migration starten, wenn Sie e-Mails von anderen Anbietern als auch migrieren möchten.

7. Wenn Sie von Google apps migrieren, in dem Sie die Domäne besitzen, müssen Sie zum [Erstellen von DNS-Einträge bei Google Domänen für Office 365](#) wechseln, wenn Sie e-Mail-Migration abgeschlossen haben, damit die e-Mail-Nachricht an Office 365-Postfächer anstelle von Google apps gesendet wird.

Wenn Sie von einer anderen IMAP-Anbieter migrieren, in dem Sie die Domäne, und [Überprüfen Sie diese Anweisungen](#), um Ihre Domäne-Anbieter finden besitzen.

Wenn Sie als Teil der Setup-Erfahrung migriert haben, können Sie auf das Setup zurückkehren. Die Installationsschritte führt Sie durch die DNS-Datensätze zu aktualisieren.

## Verwandte Themen

[Vorbereiten Sie Ihrer Google Mail oder Google Apps-Konto für die Verbindung mit Outlook und Office 365](#)

[Vorbereiten Sie Ihrer Outlook.com oder Hotmail-Konto für IMAP-migration](#)

# Verwenden des Office 365-Setup-Assistenten zum Durchführen einer IMAP-Migration

18.12.2018 • 11 minutes to read

Der Assistent für das erweiterte Setup kann automatisierte Prüfungen ausführen, um zu ermitteln, wie Ihre aktuelle Umgebung eingerichtet ist, und dann basierend auf den Ergebnissen einen Weg zu Office 365 empfehlen. Wenn Sie dem Office 365-Setup-Assistenten mitteilen, dass Ihr Quell-E-Mail-System IMAP verwendet und Sie über weniger als 151 Postfächer verfügen, empfiehlt er Ihnen, dass Sie den Office 365-Setup-Assistenten verwenden, um die E-Mails Ihrer Benutzer mithilfe der IMAP-Migration zu Office 365 zu kopieren.

Sie können eine IMAP-Migration auch über das Exchange Admin Center (EAC) durchführen. Für die EAC-Schritte lesen Sie [Migrieren von Google Apps-Postfächern zu Office 365](#) oder [Migrieren anderer Typen von IMAP-Postfächern zu Office 365](#).

## Voraussetzungen

Zum Vorbereiten der IMAP-Migration stellen Sie sicher, dass bestimmte Voraussetzungen erfüllt sind:

- Ihr Quell-E-Mail-System muss IMAP-aktiviert sein. Entsprechende Anweisungen finden Sie unter [Aktivieren des POP- oder IMAP-Zugriffs für das Herstellen einer Verbindung mit einem anderen Konto](#).
- Wenn Sie von Gmail oder Google-Apps migrieren, müssen Sie für Ihr Office 365-Konto ein App-Kennwort erstellen, um den Zugriff des Kontos zu gewährleisten. Anleitungen hierzu finden Sie unter [Vorbereiten Ihres Gmail-Kontos für die Verbindung zu Outlook und Office 365](#).
- Wenn Sie von "Outlook.com" oder "Hotmail.com" migrieren, müssen Sie ein App-Kennwort erstellen, um den Zugriff des Office 365-Kontos zu gewährleisten. Anweisungen finden Sie unter [Vorbereiten Ihres Outlook.com- oder Hotmail.com-Kontos für die IMAP-Migration](#).

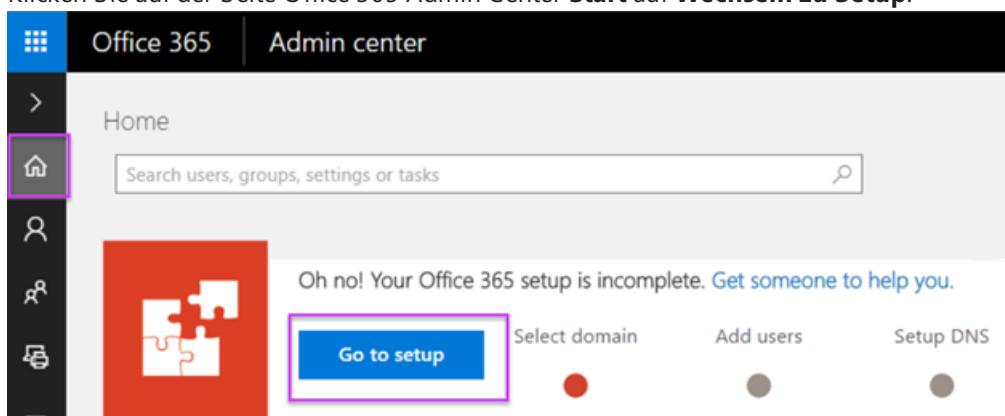
## IMAP-Migrationsaufgaben

In [Migrieren Ihrer IMAP-Postfächer zu Office 365](#) erhalten Sie einen Überblick über den IMAP-Migrationsprozess. Lesen Sie zuerst dieses Thema, wenn Sie vor dem Start des Vorgangs weitere Informationen benötigen.

Wenn Sie bereit für die ersten Schritte sind, führen Sie die folgenden Aufgaben aus:

## Schritt 1: Starten des Setup-Assistenten

Klicken Sie auf der Seite Office 365 Admin Center **Start** auf **Wechseln zu Setup**.



## Schritt 2: Verwenden des Setup-Assistenten, um zu überprüfen, ob Sie der Besitzer Ihrer Domäne sind

Im ersten Schritt wird Office 365 mitgeteilt, dass Sie der Besitzer der Domäne(n) sind, die Sie zu Office 365 migrieren.

### NOTE

Sie müssen diese Schritte für jede Domäne wiederholen, deren Besitzer Sie sind und die Sie in Office 365 verwenden möchten.

1. Wählen Sie auf der Seite **Lassen Sie uns das Setup anpassen** die Option **Ja, ich muss Daten für meine Benutzer kopieren** aus. Verfahren Sie anschließend wie folgt:

- In der **Was Ihrer aktuellen e-Mail-System ist? IMAP (outlook.com, Hotmail, Google Mail)** wählen Sie im Feld.
- Geben Sie im Feld **Wie viele Benutzer sind vorhanden?** die Anzahl der Benutzer an (weniger als 151).

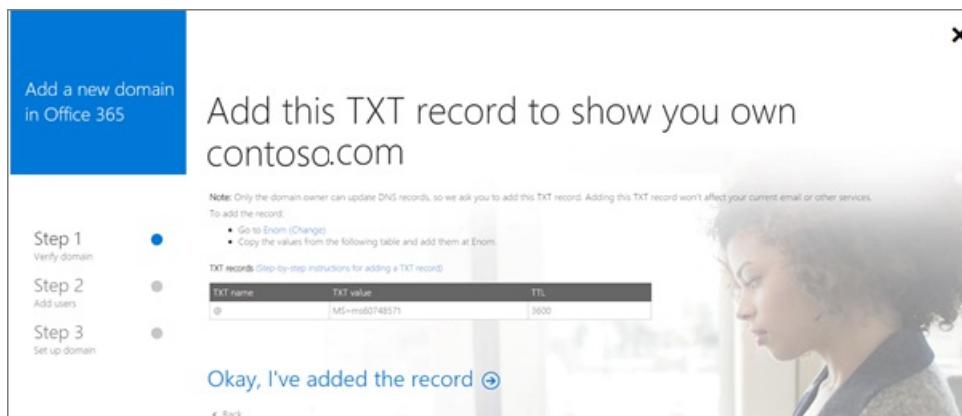
```
> [!NOTE]
> <span data-ttu-id="b9bd6-p108">Wenn Sie E-Mails mithilfe des Office 365-Setup-Assistenten zu Office 365 migrieren möchten, muss die Anzahl der Benutzer weniger als 151 betragen. Sie können den Office 365-Setup-Assistenten jedoch mehrmals ausführen, wenn Sie mehr als 150 IMAP-Kontos migrieren möchten.</span><span class="sxs-lookup"><span data-stu-id="b9bd6-p108">In order to use the Office 365 Setup wizard to migrate emails to Office 365, the number of users has to be less than 151. You can, however, run the Office 365 Setup wizard multiple times if you want to migrate more than 150 IMAP accounts.</span></span>
```

2. Wählen Sie auf der Seite **Was Sie über Domänen und DNS wissen müssen** die Option **Fangen wir an!** aus.

Wenn Sie mehr zu Domänen erfahren möchten, schauen Sie sich das Video auf der Seite an.

3. Geben Sie auf der Seite **Welche Domäne möchten Sie verwenden?** Ihre Domäne ein, beispielsweise "contoso.com".
4. Auf der Seite **Fügen Sie diesen TXT-Eintrag hinzu, um anzugeben, dass Sie " <Name Ihrer Domäne> " besitzen** wird ein für Sie spezifischer TXT-Eintrag im Format "MS=ms######" aufgelistet. Fügen Sie diesen Eintrag Ihrem DNS-Host zu. Entsprechende Anweisungen finden Sie unter [Erstellen von DNS-Einträgen für Office 365, wenn Sie Ihre DNS-Einträge verwalten](#).

Nachdem Sie den TXT-Eintrag bei Ihrem DNS-Host hinzugefügt haben, warten Sie ein paar Minuten, und wählen Sie dann **OK, ich habe den Eintrag hinzugefügt**, aus, um mit dem nächsten Schritt fortzufahren.



#### NOTE

Der TXT-Eintrag wird normalerweise schnell überprüft. Wenn aber eine Fehlermeldung angezeigt wird, warten Sie einen Moment, und klicken Sie erneut auf **OK, ich habe den Eintrag hinzugefügt**.

5. Wählen Sie auf der Seite **Wir haben geprüft, dass Ihnen die Domäne "<Name Ihrer Domäne>" gehört** die Option **Weiter** aus.

## Schritt 3: Hinzufügen von Benutzern und Kopieren von Daten

In diesem Schritt wird das Administratorkonto auf die hinzugefügte Domäne aktualisiert. Anschließend fügen Sie Benutzer mithilfe des Office 365-Setup-Assistenten hinzu.

1. Klicken Sie auf die \*\*wir Aktualisieren Ihrer aktuellen Office 365 <Ihren Domänennamen> \*\* Seite, beachten Sie das neue Administratorkonto Username, wählen Sie sie aus und klicken Sie dann so aktualisieren Sie das Administratorkonto ein, um die neue Domäne verwenden die Option **ausgewählte Benutzer aktualisieren**.

Wählen Sie im Dialogfeld **zum Abschließen der Änderung Abmelden Abmelden**, um den Vorgang fortzusetzen. Sie müssen sich mit Ihren neuen Benutzernamen anmelden. Office 365 Setup-Assistant wieder mit dem Setup Schritt gelangen Sie hatte, nachdem Sie sich anmelden.

#### NOTE

Wenn Sie den Office 365-Setup-Assistenten mehrmals ausführen, müssen Sie das Administratorkonto nur bei der ersten Ausführung hinzufügen.

### Sign out to complete the change

Sign out, and then sign in using admin@b2013.cpubtest.com. Don't worry, we'll bring you back here to continue setting up.

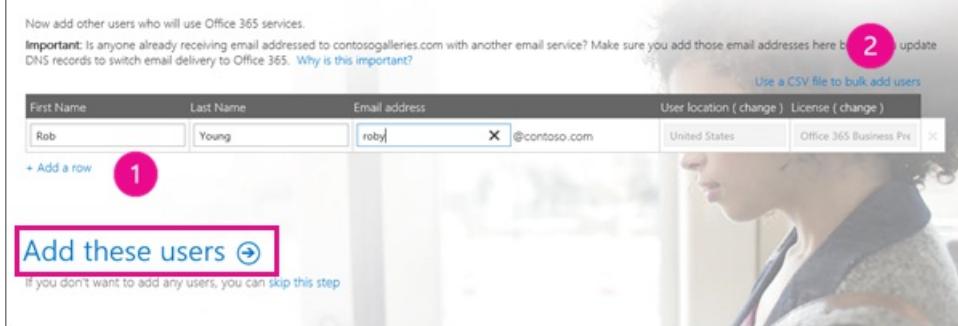
[Sign out](#)

1. Nach der Anmeldung wird die Seite **Hinzufügen von Benutzern wird übersprungen** angezeigt. Wählen Sie **Weiter** aus.
2. Lesen Sie die Informationen auf der Seite **Bereiten Sie sich auf das Kopieren der Daten nach Office 365 vor**, und klicken Sie auf **Weiter**.
3. Geben Sie auf der Seite **Neue Benutzer hinzufügen** einen Vornamen, einen Nachnamen und einen E-Mail-Alias in der Tabelle ein. Wählen Sie dann **+ Zeile hinzufügen (1)** aus, um weitere Benutzer einzugeben.

Sie können auch **CSV-Datei für massenweises Hinzufügen von Benutzern verwenden** (2) auswählen, um viele Benutzer auf einmal hinzuzufügen.

Wenn Sie damit fertig sind, klicken Sie auf **Diese Benutzer hinzufügen**.

## Add new users



4. Klicken Sie auf der Seite **<Anzahl Benutzer> wurde erfolgreich hinzugefügt** auf die Option **Weiter**, und folgen Sie den Anweisungen zum Installieren der Microsoft Office-Apps. Wenn Ihr Abonnement die Desktop-Apps nicht enthält, wird diese Seite möglicherweise nicht angezeigt.  
Sie können die Seite auch überspringen und die Apps zu einem späteren Zeitpunkt installieren.
5. Klicken Sie auf der Seite **Kopieren von Daten** wählen Sie jeden Benutzer, den Sie der e-Mail migrieren möchten, und geben Sie im Feld **Quell-e-Mail-Adresse** das Konto mit IMAP aktiviert, dem die e-Mails von dem Sie kopieren. Dies kann der Office 365-Adresse identisch sein, wenn der Benutzername und Domäne identisch sind, aber es auch, eine Google Mail-Adresse, outlook.com Adresse usw. sein kann.
6. Geben Sie für jeden Benutzer das **Kennwort** für die Quell-E-Mail ein. Klicken Sie dann auf **Weiter**, um mit dem Kopieren von E-Mails zu beginnen.
7. Geben Sie auf der Seite **Serververbindung hinzufügen** den IMAP-Servernamen, die Nummer des **Ports** und den **Sicherheitstyp** ein. Wählen Sie dann **Daten kopieren** aus.

Bei Gmail lauten die Werte:

- **IMAP-Server:** imap.gmail.com
- **Port:** 993
- **Sicherheit:** SSL

Anweisungen, wie Sie Ihren IMAP-Servernamen ermitteln können, finden Sie unter [Weitere Informationen zum Einrichten Ihrer IMAP-Serververbindung](#).

8. Klicken Sie auf der Seite **Kopieren von Daten während der Verarbeitung** können Sie den Status der Migration überwachen. Nach Abschluss die Migration, klicken Sie auf **Weiter** um die Domäne eingerichtet fortzusetzen wie unter [Hinzufügen einer Domäne zu Office 365](#)beschrieben.

### NOTE

Wenn Sie den Office 365-Setup-Assistenten mehrmals ausführen möchten, klicken Sie auf das X in der oberen rechten Ecke, um den Assistenten zu beenden. Wählen Sie bei der entsprechenden Aufforderung **Nein, ich möchte von vorn beginnen** aus. Auf diese Weise können Sie den Assistenten erneut ausführen, wenn Sie E-Mails in kleineren Batches kopieren möchten. Nachdem der letzte Batch verarbeitet wurde, können Sie das Einrichten Ihrer Domäne abschließen.

## Siehe auch

[Migrieren von IMAP-Postfächern zu Office 365](#)

[Möglichkeiten zum Migrieren von E-Mail zu Office 365](#)

## Tipps für die Optimierung von IMAP-Migrationen

# Weitere Informationen zum Einrichten Ihrer IMAP-Serververbindung

18.12.2018 • 2 minutes to read

☐ Zum Migrieren Ihrer E-Mail mithilfe der IMAP (Internet Message Access Protocol)-Migration muss Office 365 den Namen und die Verbindungseinstellungen Ihres IMAP-Servers kennen.

## Ermitteln des IMAP-Servernamens

Office 365 benötigt den Namen des Quell-E-Mail-Servers, aus dem Sie Postfächer migrieren möchten. In dieser Aufgabe wird erläutert, wie Sie den Namen des Systems mit Outlook Web App ermitteln. Wenn Sie keinen Zugriff auf Outlook Web App haben oder Ihr IMAP-Servername dort nicht aufgelistet ist, wenden Sie sich entweder an den Support, oder konsultieren Sie die Hilfedokumentation Ihres Quell-E-Mail-Systems.

### So ermitteln Sie den Namen Ihres Quell-E-Mail-Quellsystems mithilfe von TE102821288

- Wählen Sie in Outlook Web App, klicken Sie auf der Symbolleiste auf die Registerkarte **Einstellungen**  > **Optionen** > **Mail** > **Konten** > **POP und IMAP**. Klicken Sie unten Ihre Kontoinformationen sehen Sie einen Link zu **Einstellungen für POP- und IMAP-Zugriff**. IMAP-Servername ist aktiviert, unter IMAP-Einstellung aufgeführt.

POP and IMAP settings

Use the information on this page if you need to use POP or IMAP to connect your mailbox.

**POP setting**

Server name: outlook.office365.com  
Port: 995  
Encryption method: SSL

⋮

**IMAP setting**

Server name: outlook.office365.com  
Port: 993  
Encryption method: SSL

Your IMAP server name, if enabled,  
is listed under IMAP setting.

**SMTP setting**

Server name: smtp.office365.com  
Port: 587  
Encryption method: TLS

Der IMAP-Server für Gmail ist: **imap.gmail.com**.

Weitere Informationen zu IMAP-Verbindungen in Office 365 finden Sie unter [POP- und IMAP-E-Mail-Einstellungen für Outlook](#).

## Werte für Sicherheit und Port

Office 365 benötigt außerdem die Werte für die Verschlüsselungsmethode und TCP-Portnummer, die vom IMAP-Quell-E-Mail-Server verwendet werden.

- **Sicherheit:** Dies ist die Verschlüsselungsmethode vom IMAP-Server verwendet werden. Der Standardwert für secure Sockets Layer (SSL) eignet sich für die meisten IMAP-Server.
- **Port:** Dies ist die TCP-Portnummer an, die zum Verbinden mit dem IMAP-Server. Verwenden Sie Port 143 für unverschlüsselte Verbindungen, Port 143 für Transport Layer Security (TLS) Verbindungen oder Port

993 (Standard), für die SSL-Verbindungen. Port 993 eignet sich für die meisten IMAP-Server.

# Tipps zum Optimieren von IMAP-Migrationen

18.12.2018 • 8 minutes to read

Wenn Sie eine IMAP (Internet Message Access Protocol)-Migration von einem lokalen Exchange Server zu Office 365 durchführen, stehen Ihnen einige Möglichkeiten zur Optimierung der Migrationsleistung zur Verfügung.

## Optimieren von IMAP-Migrationen

Es folgen einige Tipps zum Optimieren einer IMAP-Migration:

- **Erhöhen Sie die Grenzwerte für die Verbindung mit Ihrem IMAP-Server:** viele e-Mail-Servern und Firewalls für pro Benutzer, pro IP-Adresse Grenzwerte und allgemeine Verbindungslimits haben. Bevor Sie Postfächer migrieren, stellen Sie sicher, dass Ihre Firewall und IMAP-Server für eine große oder maximum, Anzahl der Verbindungen für die folgenden Einstellungen konfiguriert werden:
  - Die Gesamtzahl der Verbindungen mit dem IMAP-Server.
  - Die Anzahl der Verbindungen eines bestimmten Benutzers. Dies ist wichtig, wenn Sie ein Administratorkonto in der CSV-Migrationsdatei (Datei mit durch Kommas getrennten Werten) verwenden, da alle Verbindungen mit dem IMAP-Server über dieses Benutzerkonto erfolgen.
  - Die Anzahl der Verbindungen von einer einzelnen IP-Adresse. Dieses Limit wird in der Regel durch die Firewall oder den E-Mail-Server erzwungen.

Wenn auf Ihrem IMAP-Server Microsoft Exchange Server 2010 oder Exchange 2007 ausgeführt wird, sind die Standardeinstellungen für Verbindungslimits niedrig. Achten Sie darauf, diese Limits zu erhöhen, bevor Sie E-Mails migrieren. In Exchange 2003 ist die Anzahl der Verbindungen standardmäßig nicht eingeschränkt.

Weitere Informationen finden Sie unter:

- Exchange 2013: [Festlegen von Verbindungseinschränkungen für IMAP4](#)
  - Exchange Server 2010: [Anzeigen oder Konfigurieren der IMAP4-Eigenschaften](#)
  - Exchange 2007: [So legen Sie Verbindungseinschränkungen für IMAP4 fest](#)
  - Exchange 2003: [Festlegen von Verbindungsbeschränkungen](#)
- **Ändern Sie die Einstellung DNS - TTL (TTL) auf Ihren MX-Eintrag:** vor der Migration von Postfächern, die Einstellung TTL Domain Name System (DNS) auf Ihren aktuellen MX-Eintrag auf einen kürzeren Intervall, z. B. 3.600 Sekunden (eine Stunde). Beim Ändern des MX-Eintrags, um auf Office 365-e-Mail-Organisation zu verweisen, nachdem alle Postfächer migriert werden, sollten Sie dann der aktualisierte MX-Eintrag schneller aufgrund der verkürzte TTL-Intervall weitergeben.
  - **Führen Sie mindestens einen Test migrationsbatches:** Führen Sie ein paar kleine IMAP-migrationsbatches vor der Migration größere Anzahl von Benutzern. Bei der Testmigration können Sie Folgendes ein:
    - Überprüfen des Formats der CSV-Datei.
    - Testen des Migrationsendpunkts, der zum Herstellen einer Verbindung mit dem IMAP-Server verwendet wird.

- Überprüfen, ob E-Mails unter Verwendung von Administratoranmeldeinformationen erfolgreich migriert werden können (falls zutreffend).
- Ermitteln der optimalen Anzahl gleichzeitiger Verbindungen mit dem IMAP-Server, durch die Auswirkungen auf die Internetbandbreite auf ein Minimum reduziert werden.
- Sicherstellen, dass von Ihnen ausgeschlossene Ordner nicht zu Office 365-Postfächern migriert werden.
- Ermitteln der Zeitdauer für die Migration einer Gruppe von Benutzern.
- Verwenden Sie die CSV-Dateien mit identischer Anzahl von Zeilen, und führen Sie die Batches zu ähnlichen Zeiten während des Tages aus. Vergleichen Sie dann die Gesamtausführungszeiten aller Testbatches. Dieser Vergleich erleichtert Ihnen die Abschätzung, wie lange das Migrieren aller Postfächer dauern wird, wie umfangreich jeder Migrationsbatch sein sollte und wie viele gleichzeitige Verbindungen mit dem IMAP-Server verwendet werden sollten, um einen sinnvollen Kompromiss zwischen Migrationsgeschwindigkeit und Internetbandbreite zu erzielen.

- **Verwendung von Administratoranmeldeinformationen in der CSV-Datei zum Migrieren von e-Mail:**

Diese Methode ist die am wenigsten störende und für Benutzer unangenehme und hilft minimieren Synchronisierungsfehler verursacht, wenn der Benutzer das Kennwort für ihre lokale Konto ändern. Es erspart auch Sie abzurufen oder Ändern von Benutzerkennwörtern. Wenn Sie diese Methode verwenden, müssen Sie sicherstellen, dass das Administratorkonto ein, den, das Sie verwenden, verfügt über die erforderlichen Berechtigungen auf die Postfächer zugreifen, die Sie migrieren.

**NOTE**

Wenn Sie sich für die Verwendung von Benutzeranmeldeinformationen in der CSV-Datei entscheiden, überlegen Sie, ob Sie Benutzerkennwörter global ändern und dann verhindern, dass Benutzer ihre Kennwörter auf dem lokalen Konto ändern, bevor Sie deren Postfächer migrieren. Wenn Benutzer ihr Kennwort ändert, bevor ihr Postfach zum cloudbasierten Postfach migriert wurde, schlägt die Migration fehl. Wenn Benutzer ihr Kennwort ändert, nachdem das Postfach migriert wurde, werden neue E-Mails, die an das Postfach auf dem IMAP-Server gesendet werden, nicht zu ihrem Office 365-Postfach migriert.

- **Löschen von Postfächern oder Ändern ihrer SMTP-Adressen während der Migration nicht:** das migrationssystem meldet einen Fehler, wenn ein Postfach nicht gefunden werden kann, die migriert wurde. Achten Sie darauf, dass die Migration abschließen und Löschen des migrationsbatches, vor dem Löschen oder ändern Sie die SMTP-Adresse eines Office 365 oder lokalen Postfach, das migriert wurde.

- **Kommunikation mit den Benutzern:** Benutzer im Voraus wissen, dass Sie den Inhalt von ihren lokalen Postfächern zu Office 365-Organisation migrieren werden können. Beachten Sie Folgendes:

- Informieren Sie die Benutzer, dass E-Mail-Nachrichten mit einer Größe von mehr als 35 MB nicht migriert werden. Bitten Sie die Benutzer, sehr umfangreiche Nachrichten und Anlagen auf ihrem lokalen Computer oder einem USB-Wechseldatenträger zu speichern.
- Fordern Sie die Benutzer auf, vor der Migration alte oder nicht erforderliche E-Mails in ihren lokalen Postfächern zu löschen. Auf diese Weise kann die zu migrierende Datenmenge verringert und die Gesamtzeit reduziert werden. Alternativ können Sie selbst die Postfächer der Benutzer bereinigen.
- Schlagen Sie vor, dass Benutzer ihre Posteingänge sichern.
- Informieren Sie die Benutzer, welche Ordner nicht migriert werden (falls zutreffend).
- Ordner mit einem Schrägstrich (/) im Ordnernamen werden nicht migriert. Wenn die Benutzer Ordner migrieren möchten, die Schrägstriche im Namen enthalten, müssen sie die Ordner

umbenennen oder die Schrägstriche durch ein anderes Zeichen ersetzen, z. B. einen Unterstrich (\_) oder einen Bindestrich (-).

# CSV-Dateien für IMAP-Migrationsbatches

18.12.2018 • 11 minutes to read

Die CSV-Datei (Comma-Separated Values, durch Trennzeichen getrennte Werte), die Sie zum Migrieren der Inhalte von Benutzerpostfächern in einer IMAP-Migration verwenden, enthält eine Zeile für jeden Benutzer. Jede Zeile enthält Informationen zum Office 365-Postfach des jeweiligen Benutzers, und Office 365 verwendet diese Informationen zum Verarbeiten der Migration.

## Erforderliche Attribute

Dies sind die erforderlichen Attribute für jeden Benutzer:

- " **EmailAddress** " gibt die Benutzer-ID für das Office 365-Postfach des Benutzers an.
- **Benutzername** gibt den Benutzeranmeldenamen für das Postfach des Benutzers auf dem IMAP-Server. Sie können der Benutzername oder Domäne\Benutzername Format verwenden. Beispielsweise `hollyh` oder `contoso\hollyh`.
- " **Password** " ist das Kennwort für das Benutzerkonto im IMAP-Messaging-System.

Die Migration schlägt fehl, wenn eines dieser Attribute nicht in die Überschriftenzeile der CSV-Datei einbezogen wird. Achten Sie auch darauf, die Attribute genauso einzugeben, wie sie angezeigt werden. Attribute dürfen keine Leerzeichen enthalten. Sie müssen ein einziges Wort sein. So ist beispielsweise " **Email Address** " ungültig. Sie müssen " **EmailAddress** " verwenden.

## CSV-Dateiformat

Hier ist ein Beispiel für das Format der CSV-Datei. In diesem Beispiel werden die Benutzeranmeldeinformationen zum Migrieren von drei Postfächern verwendet.

```
EmailAddress,UserName,Password
terrya@contoso.edu,contoso\terry.adams,1091990
annb@contoso.edu,contoso\ann.beebe,2111991
paulc@contoso.edu,contoso\paul.cannon,3281986
```

In der ersten Zeile (oder Überschriftenzeile) der CSV-Datei sind die Namen der Attribute (oder Felder) aufgelistet, die in den folgenden Zeilen angegeben sind. Die einzelnen Attributnamen sind durch ein Komma getrennt.

Jede Zeile unterhalb der Überschriftenzeile steht für einen Benutzer und stellt die Informationen bereit, die zum Migrieren von dessen Postfach verwendet werden. Die Attributwerte in den einzelnen Zeilen müssen dieselbe Reihenfolge wie die Attributnamen in der Überschriftenzeile aufweisen. Die einzelnen Attributwerte sind durch ein Komma getrennt.

Sie können die CSV-Datei mit einem beliebigen Texteditor oder einer Anwendung wie Microsoft Excel erstellen. Speichern Sie die Datei als CSV- oder TXT-Datei.

**TIP**

Wenn die CSV-Datei ASCII-fremde Zeichen oder Sonderzeichen enthält, speichern Sie sie mit UTF-8 oder einer anderen Unicode-Codierung. Je nach Anwendung kann es möglicherweise einfacher sein, die CSV-Datei mit UTF-8 oder einer anderen Unicode-Codierung zu speichern, wenn das Systemgebietschema des Computers mit der in der CSV-Datei verwendeten Sprache übereinstimmt.

## Aufteilen einer großen Migration in mehrere Batches

Die CSV-Datei kann bis zu 50.000 Zeilen - eine Zeile für jeden Benutzer - enthalten und maximal 10 MB groß sein. Es empfiehlt sich jedoch, Benutzer in mehreren kleineren Batches zu migrieren.

Wenn Sie eine Migration von vielen Benutzern planen, entscheiden Sie, welche Benutzer in die einzelnen Batches einbezogen werden sollen. Wenn Sie beispielsweise 10.000 Konten migrieren müssen, könnten Sie vier Batches mit jeweils 2.500 Benutzern zusammenstellen. Sie könnten die Batches auch alphabetisch aufteilen: nach Benutzertyp, z. B. Lehrkräfte, Studenten und ehemaligen Absolventen; nach Jahrgangsstufen in der Schule, z. B. Unterstufe, Mittelstufe, Oberstufe; oder auf andere Arten, die den Anforderungen Ihrer Organisation entsprechen.

**TIP**

Eine Strategie besteht darin, Office 365-Postfächer erstellen und Migrieren der e-Mails für eine Gruppe von Benutzern. Beispielsweise wenn 100 neue Benutzer in Office 365-Organisation importiert werden, erstellen Sie einen migrationsbatch für die gleichen 100 Benutzer. Dies ist eine effektive Möglichkeit zum Organisieren und Verwalten der Migrations von einem lokalen Messagingsystem zu Office 365.

## Bereitstellen von Anmeldeinformationen für Benutzer oder Administratoren

In der CSV-Datei Sie müssen angeben den Benutzernamen und das Kennwort für des Benutzers lokale Konto. Dadurch wird den Migrationsprozess Zugriff auf das Konto. Es gibt zwei Methoden, um diese Schritte durchzuführen:

- **Verwendung von Benutzeranmeldeinformationen:** Dies erfordert, dass die Kennwörter von Benutzern zu erhalten oder ihre Kennwörter auf einen anderen Wert ändern, die Sie kennen, sodass Sie ihn in der CSV-Datei einfügen können.

**TIP**

Wenn Sie diese Option verwenden, müssen Sie verhindern, dass die Benutzer die Kennwörter ihrer lokalen Konten ändern. Sollten die Benutzer nämlich ihre Kennwörter nach der Erstmigration ändern, schlagen nachfolgende Synchronisierungen zwischen den Postfächern auf dem IMAP-Server und den Office 365-Postfächern fehl.

- **Super Benutzer oder Administrator-Anmeldeinformationen verwenden:** Dies erfordert, dass Sie ein Konto in Ihrem IMAP-Messagingsystem an, die über die entsprechenden Rechte zum Zugriff auf alle Benutzerpostfächer verwenden. In der CSV-Datei verwenden Sie die Anmeldeinformationen für dieses Konto für jede Zeile. Informationen dazu, ob der IMAP-Server diesem Ansatz und zum Aktivieren unterstützt, finden Sie unter der Dokumentation zu Ihrem IMAP-Server.

#### NOTE

Es empfiehlt sich, Administratoranmeldeinformationen zu verwenden, weil sie sich nicht auf die Benutzer auswirken oder ihnen Unannehmlichkeiten bereiten. So ist es beispielsweise unerheblich, ob Benutzer ihre Kennwörter nach der Erstmigration ändern.

## Formatieren für die Administratoranmeldeinformationen bei unterschiedlichen IMAP-Servern

Sie können den Benutzernamen und das Kennwort eines Administratorkontos in den Feldern **Benutzername** und **Kennwort** für jede Zeile der CSV-Datei verwenden. Der Benutzername für die Anmeldeinformationen eines Farmadministrators ist eine Kombination aus der Benutzername der Person, deren e-Mail migriert wird, und den Benutzernamen für ein Administratorkonto die Berechtigung zum Zugriff auf alle Benutzerpostfächer hat. Administratoranmeldeinformationen für das unterstützte Format unterscheidet sich je nach dem IMAP-Server, den, dem Sie e-Mails von migrieren. Weitere Informationen zur Verwendung von Administratoranmeldeinformationen, finden Sie in der Dokumentation zu Ihrem IMAP-Server.

#### NOTE

Wenn Sie eine neue Migrationsanforderung übermitteln, wird die CSV-Datei über eine SSL-Verbindung (Secure Sockets Layer) in das Microsoft-Datencenter hochgeladen. Die Informationen in der CSV-Datei werden verschlüsselt und auf den Microsoft Exchange-Servern im Microsoft-Datencenter gespeichert.

In den nachstehenden Abschnitten wird erläutert, wie die Administratoranmeldeinformationen in der CSV-Datei formatiert werden, die Sie zum Migrieren von E-Mails von unterschiedlichen Typen von IMAP-Servern verwenden.

### Microsoft Exchange Server

Wenn beim Migrieren von e-Mail von der IMAP-Implementierung für Microsoft Exchange verwenden Sie das Format **Domäne/Admin\_UserName/User\_UserName** für das Attribut **UserName** in der CSV-Datei. Angenommen, Sie e-Mails von Exchange für Terry Adams, Ann Beebe und Paul Cannon migrieren. Sie haben eine Mail-Administratorkonto, in dem der Benutzername ist Mailadmin und das Kennwort lautet P@ssw0rd. Nachfolgend finden Sie die CSV-Datei würde folgendermaßen aussehen:

```
EmailAddress,UserName,Password  
terrya@contoso.edu,contoso-students/mailadmin/terry.adams,P@ssw0rd  
annb@contoso.edu,contoso-students/mailadmin/ann.beebe,P@ssw0rd  
paulc@contoso.edu,contoso-students/mailadmin/paul.cannon,P@ssw0rd
```

### Dovecot

Verwenden Sie bei IMAP-Servern, die Simple Authentication and Security Layer (SASL) unterstützen, z. B. einem Dovecot-IMAP-Server, das Format "**User\_UserName\*Admin\_UserName**". Dabei ist das Sternchen (\*) ein konfigurierbares Trennzeichen. Angenommen, Sie migrieren E-Mails derselben Benutzer von einem Dovecot-IMAP-Server mit den Administratoranmeldeinformationen mailadmin und dem Kennwort P@ssw0rd. Dann würde Ihre CSV-Datei so aussehen:

```
EmailAddress,UserName,Password  
terrya@contoso.edu,terry.adams*mailadmin,P@ssw0rd  
annb@contoso.edu,ann.beebe*mailadmin,P@ssw0rd  
paulc@contoso.edu,paul.cannon*mailadmin,P@ssw0rd
```

## Mirapoint

Wenn Sie E-Mails aus Mirapoint Message Server migrieren, verwenden Sie für die Administratoranmeldeinformationen das Format " \*\*#user@domain#Admin\_UserName## ". Zum Migrieren von E-Mails aus Mirapoint unter Angabe der Administratoranmeldeinformationen mailadmin und des Kennworts P@ssw0rd würde Ihre CSV-Datei so aussehen:

```
EmailAddress,UserName,Password  
terrya@contoso.edu,#terry.adams@contoso-students.edu#mailadmin#,P@ssw0rd  
annb@contoso.edu,#ann.beebe@contoso-students.edu#mailadmin#,P@ssw0rd  
paulc@contoso.edu,#paul.cannon@contoso-students.edu#mailadmin#,P@ssw0rd
```

## Verwenden des optionalen Attributs "UserRoot"

Einige IMAP-Server, z. B. Courier IMAP, unterstützen keine Administratoranmeldeinformationen für ein Migrieren von Postfächern zu Office 365. Wenn Sie Administratoranmeldeinformationen zum Migrieren von Postfächern verwenden möchten, können Sie Ihren IMAP-Server so konfigurieren, dass er virtuelle freigegebene Ordner verwendet. Virtuelle freigegebene Ordner ermöglichen es Administratoren, unter Angabe der Administratoranmeldeinformationen auf Benutzerpostfächer auf dem IMAP-Server zuzugreifen. Weitere Informationen zum Konfigurieren von virtuellen freigegebenen Ordnern für Courier IMAP finden Sie unter [Freigegebene Ordner](#).

Um Postfächer zu migrieren, nachdem Sie virtuelle freigegebene Ordner auf Ihrem IMAP-Server eingerichtet haben, müssen Sie das optionale Attribut " **UserRoot** " in die CSV-Datei einfügen. Dieses Attribut gibt für das Postfach jedes Benutzers den Speicherort an, den es in der Struktur der virtuellen freigegebenen Ordner auf dem IMAP-Server hat.

Hier ist ein Beispiel für eine CSV-Datei, die das Attribut " **UserRoot** " enthält:

```
EmailAddress,UserName,Password,UserRoot  
terrya@contoso.edu,mailadmin,P@ssw0rd,/users/terry.adams  
annb@contoso.edu,mailadmin,P@ssw0rd,/users/ann.beebe  
paulc@contoso.edu,mailadmin,P@ssw0rd,/users/paul.cannon
```

# Vorbereiten Ihres Gmail- oder G Suite-Kontos für die Verbindung mit Outlook und Office 365

18.12.2018 • 6 minutes to read

Vor dem [Herstellen einer Verbindung mit Ihrem Gmail-Konto](#) von Outlook im Web aus oder dem [Hinzufügen eines Gmail-Kontos](#) zu Outlook müssen Sie Ihr Gmail-Konto vorbereiten. Sie müssen die Bestätigung in zwei Schritten für Gmail aktivieren und dann ein App-Kennwort erstellen, das von Office 365 zusammen mit Ihrer Gmail-Adresse zum Herstellen einer Verbindung verwendet wird.

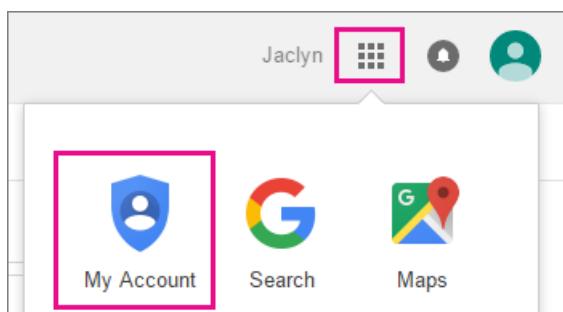
Dies ist auch dann erforderlich, wenn Ihr Administrator eine Migration von [Gmail](#) oder [G Suite Gmail](#) zu Office 365 plant.

## Aktivieren von Gmail für eine Verbindung von Office 365 aus

Wenn Sie ein App-Kennwort für Gmail verwenden möchten, müssen Sie zunächst die Bestätigung in zwei Schritten aktivieren und dann das App-Kennwort abrufen. Sobald Sie über ein App-Kennwort verfügen, können Sie dieses in Kombination mit Ihrem Benutzernamen zum Herstellen einer Verbindung mit Gmail verwenden.

### So aktivieren Sie die Bestätigung in zwei Schritten

1. Melden Sie sich bei Ihrem Gmail-Konto an.
2. Wählen Sie **Google-Apps > Mein Konto** aus.



3. Wählen Sie auf der Seite **Mein Konto -Anmeldung & Security**.
4. Klicken Sie unter der **Kennwort & -in-Methode**, wählen Sie den Pfeil neben der **Überprüfung für-Schritt 2**, und geben Sie Ihr Kennwort ein, wenn Sie aufgefordert werden.

The screenshot shows the 'Mein Konto -Anmeldung & Security' page. At the top, it says 'Password & sign-in method'. Below that, a paragraph explains that your password protects your account and that adding 2-Step Verification provides an extra layer of security by sending a one-time code to your phone. A note below states that changing these settings requires confirming your password. Two sections are shown: 'Password' (last changed: November 18, 11:59 AM) and '2-Step Verification' (set to 'Off'). The '2-Step Verification' section has a pink rectangular box around the 'Off' status and the adjacent arrow button.

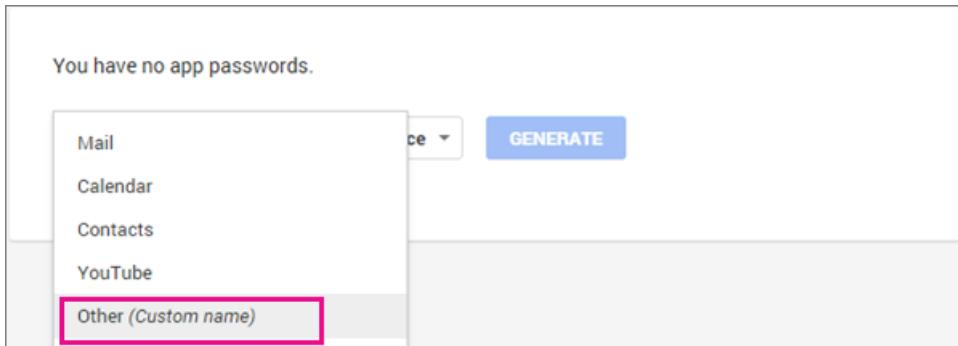
#### NOTE

Wenn Sie über ein Google Apps-Konto verfügen und diese Einstellung nicht angezeigt wird, muss sie zuerst vom Administrator aktiviert werden. Anweisungen dazu (für den Administrator) finden Sie unter [Aktivieren der Bestätigung in zwei Schritten für Ihre G Suite-Benutzer](#).

5. Wählen Sie auf der Seite **Mit der Bestätigung in zwei Schritten anmelden** die Option **Einrichtung starten** aus.
6. Geben Sie bei Aufforderung Ihr Kennwort erneut ein, und geben Sie dann im Schritt **Telefon einrichten** Ihre Mobiltelefonnummer ein, oder prüfen Sie die angegebene Nummer. Geben Sie im nächsten Schritt den Bestätigungscode ein, der an Ihr Mobiltelefon gesendet wurde, und wählen Sie **Bestätigen** aus.
7. Wählen Sie im Schritt **Diesen Computer als vertrauenswürdig einstufen?** die Option **Weiter** aus, und wählen Sie im Schritt **Bestätigung in zwei Schritten aktivieren** die Option **Bestätigen** aus.

#### So erstellen Sie ein App-Kennwort

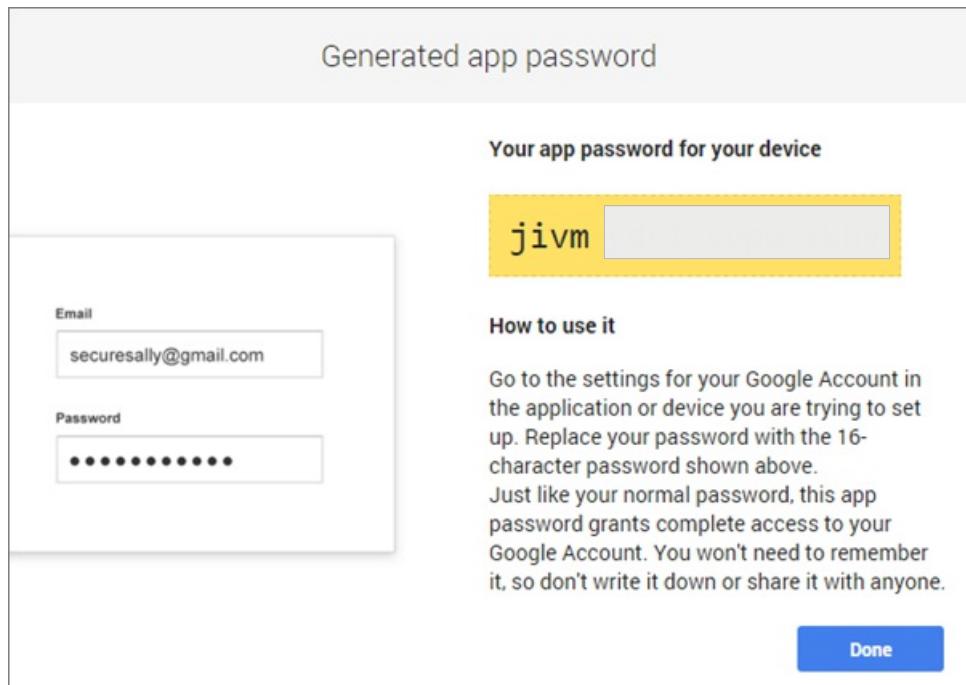
1. Melden Sie sich bei Ihrem Gmail-Konto an.
2. Wählen Sie **Google-Apps > Mein Konto** aus.
3. Wählen Sie auf der Seite **Mein Konto -Anmeldung & Security**.
4. Klicken Sie unter der **Kennwort & -in-Methode**, wählen Sie den Pfeil neben der **App-Kennwörtern**, und geben Sie Ihr Kennwort ein, wenn Sie aufgefordert werden.
5. Wählen Sie auf der Seite **App-Passwörter** in der Dropdownliste **App auswählen** den Eintrag **Andere (benutzerdefinierter Name)** aus.



6. Geben Sie einen Namen, beispielsweise Myconnection > **generieren**.

Beachten Sie das app-Kennwort unter **Ihrer app-Kennwort für Ihr Gerät**. Dies können mit Ihrer Google Mail-Adresse in der app, die Sie eine Verbindung mit Ihrer Google Mail-Konto (oder Sie Google Mail-Konto zu hinzufügen). Diese Kombination gewährt uneingeschränkten Zugriff auf Ihre Google Mail-Konto von der app, die verwendet wird.

Nachdem Sie das App-Kennwort eingegeben haben, müssen Sie es sich nicht merken.



#### IMPORTANT

Das aus 16 Zeichen bestehende App-Kennwort wird mit Leerzeichen angezeigt, sodass es leichter zu lesen ist. Wenn Sie es in der App eingeben, mit der Sie eine Verbindung herstellen möchten, ignorieren Sie die Leerzeichen, und geben Sie die 16 Zeichen als ununterbrochene Zeichenfolge ein.

7. Sie können nun Ihre Google Mail-Konto zu Outlook hinzufügen. Wenn Sie ein Kennwort, *Geben Sie diese app-Kennwort für Ihr Konto Gmail* aufgefordert werden. Geben Sie Ihr Kennwort Google Mail. Anleitung zum Hinzufügen von Google Mail-Konto zu Outlook finden Sie in diesen Artikeln:

- [Hinzufügen eines E-Mail-Kontos zu Outlook](#)
- [Verbinden von E-Mail-Konten in Outlook im Web \(Office 365\)](#)

#### Optionales Widerrufen des App-Kennworts

Wenn Sie die Gmail-Verbindung nur für kurze Zeit benötigen, z. B. für eine IMAP-Postfachmigration, die vom Administrator ausgeführt wird, können Sie das App-Kennwort später widerrufen.

#### So widerrufen Sie das App-Kennwort

1. Melden Sie sich bei Ihrem Gmail-Konto an.
2. Wählen Sie **Google-Apps > Mein Konto** aus.
3. Wählen Sie auf der Seite **Mein Konto -Anmeldung & Security**.
4. Klicken Sie unter der **Kennwort & -in-Methode**, wählen Sie den Pfeil neben der **App-Kennwörtern**, und geben Sie Ihr Kennwort ein, wenn Sie aufgefordert werden.
5. Wählen Sie auf der Seite **App-Passwörter** neben dem App-Kennwort, das Sie widerrufen möchten, die Option **WIDERRUFEN** aus.

Your app passwords

Name	Created	Last used
migrate	Jan 6, 2016	Jan 6, 2016

Select the app and device you want to generate the app password for.

Select app ▾ Select device ▾

**GENERATE**

## Verwandte Themen

[Migrieren von E-Mails und Kontakten zu Office 365](#)

[Methoden zum Migrieren mehrerer E-Mail-Konten zu Office 365](#)

# Migrieren Ihres Outlook.com-Kontos zu Office 365

18.12.2018 • 6 minutes to read

Wenn Sie Ihr Outlook.com- oder Hotmail.com-Konto zu Office 365 migrieren, müssen Sie die Überprüfung in zwei Schritten (auch bekannt als zweistufige Authentifizierung) aktivieren.

Die Überprüfung in zwei Schritten dient zu Ihrem Schutz, indem sie es für andere schwieriger macht, sich bei Ihrem E-Mail-Konto anzumelden. Sie verwendet zwei verschiedene Formen von Identität: Ihr Kennwort und eine Kontaktmethode. Selbst wenn eine fremde Person Ihr Kennwort erfährt, kommt sie damit nicht weit, wenn Sie keinen Zugriff auf Ihre anderen Geräte oder Konten hat.

Die Überprüfung in zwei Schritten kann mit einer E-Mail-Adresse, einer Telefonnummer oder einer Authentifizierungs-App eingerichtet werden. Wenn Sie sich bei einem neuen Gerät oder von einem neuen Ort aus anmelden, senden wir Ihnen einen Sicherheitscode, den Sie auf der Anmeldeseite als zweite Authentifizierung über das Kennwort hinaus eingeben.

Nachdem Sie die Überprüfung in zwei Schritten eingerichtet haben, können Sie auch ein App-Kennwort anfordern, das von Ihnen verwendet werden muss, um die IMAP-Migration (Internet Message Access Protocol) zum Kopieren von E-Mail-Nachrichten aus Ihrem Outlook.com- oder Hotmail.com-Konto in Ihr Office 365 Business-Konto zu verwenden. Wenn Ihr Office 365-Administrator E-Mail-Nachrichten von Ihrem Outlook.com- oder Hotmail.com-Konto in Ihrem Auftrag nach Office 365 verschiebt, müssen Sie ihm Ihr App-Kennwort geben.

## Aktivieren der Überprüfung in zwei Schritten und Erstellen eines App-Kennworts in Outlook.com oder Hotmail.com

1. Melden Sie sich bei [Outlook.com](#) oder [Hotmail.com](#) an.
2. Wechseln Sie zur Seite [Sicherheitseinstellungen](#). Geben Sie, falls Sie dazu aufgefordert werden, Ihr Kennwort ein.

Wenn Sie auf der Seite Sicherheitseinstellungen navigieren möchten, Outlook.com klicken oder tippen Sie auf Ihr Profilbild auf der oberen rechten Ecke > **Konto anzeigen**, und wählen Sie auf der Seite Konto auf der Seite **Konto Sicherheit** auf die blaue Leiste und dann, \*\* Weitere Sicherheitsoptionen\*\*.

3. Scrollen Sie auf der Seite nach unten, und wählen Sie **Prüfung in zwei Schritten einrichten** unter **Überprüfung in zwei Schritten** aus.

The screenshot shows the Microsoft Account security settings page. At the top, there's a navigation bar with links for Microsoft Store, Products, Support, Account, Your info, Privacy, Security (which is highlighted in blue), Rewards, and Payment & billing. Below the navigation bar, the title "Security settings" is displayed. The main content area is divided into several sections:

- Password**: A message states "Your password was changed on 5/4/2016." with a link to "Change your password".
- Security info helps keep your account secure**: A message says "When you need to prove you're you or a change is made to your account, we'll use your security info to cor". Below this are two sections:
  - "Will receive alerts": A placeholder box with a "Remove" button.
  - "Won't receive alerts": A placeholder box with a "Remove" button.
- Add security info** and **Change alert options** buttons are located here.
- Sign-in preferences**: A message says "To make it harder for someone to break in to your account, turn off sign-in preferences for any email addre". Below this is a "Change sign-in preferences" link.
- Two-step verification**: A message says "Two-step verification is an advanced security feature that makes it harder for someone to break in to your account". Below this are two buttons:
  - "Set up two-step verification"
  - A blue button with white text: "Choose Set up two-step verification."

4. Wählen Sie **Weiter** aus, um den Setup-Assistenten zu starten.
5. Achten Sie auf der Seite **Einrichten des Smartphones mit einem App-Kennwort** unter der Liste **Aktualisieren von Windows Phone 8 (oder früher) mit einem App-Kennwort** auf das 16-stellige App-Kennwort in der Liste:



Wenn Sie ein Windows Phone 8 (oder früher) verwenden, müssen Sie das Kennwort, das Sie für die Anmeldung bei der E-Mail verwenden, durch das App-Kennwort ersetzen.

#### **IMPORTANT**

Obwohl auf der Seite angegeben ist, dass dies für Windows Phone 8 (oder eine frühere Version) gilt, **enthält diese Liste das App-Kennwort, das Ihr Administrator benötigt**, um Ihre Hotmail.com- oder Outlook.com-E-Mail zu Office 365 Business zu migrieren. Sie benötigen dieses App-Kennwort auch dann, wenn Sie die Überprüfung in zwei Schritten mithilfe eines Android-Geräts oder einem iPhone einrichten.

Dies ist auch das App-Kennwort, das von Ihnen oder Ihrem Administrator für die [Migration Ihrer hotmail.com- oder outlook.com-E-Mail](#) zu Office 365 Business verwendet wird.

6. Laden Sie auf Ihrem mobilen Gerät Microsoft Authenticator aus dem App Store herunter.

Wählen Sie einen der Links aus, mit denen Sie zu Microsoft Authenticator für [Windows Phone](#), [Android](#) oder [iOS](#) gelangen.

7. Öffnen Sie auf Ihrem mobilen Gerät die Microsoft Authenticator-App, und wählen Sie + aus. Scannen Sie den Code auf der Seite **Einrichten einer Authentifikator-App**.
8. Geben Sie in Schritt 4 auf der Seite **Einrichten einer Authentifikator-App** den sechsstelligen Code ein, der auf Ihrem mobilen Gerät angezeigt wird (Beispiel: 555111; Leerzeichen müssen nicht eingegeben werden).

Sie brauchen sich dieses Kennwort nicht zu merken. Es ändert sich ständig, und neue Kennwörter werden Ihnen über die Microsoft Authenticator-App zugesendet. Daher kommt die hohe Sicherheit. Immer, wenn Sie sich von einem neuen Gerät oder Ort aus bei Ihrem E-Mail-Konto anmelden, werfen Sie einen Blick auf Ihre Microsoft Authenticator-App, und melden Sie sich mithilfe des neuesten App-Kennworts an, das an Sie gesendet wurde, statt Ihr altes statisches Kennwort zu verwenden.

9. Sie erhalten die Meldung, die in zwei Schritten Überprüfung aktiviert ist. Drucken Sie neuen *Wiederherstellungscode* (Dies ist das app-Kennwort nicht). Wenn Sie Zugriff auf dieses Konto wiederherstellen müssen, helfen diesen Wiederherstellungscode. Es ist ratsam, unerheblich an einem sicheren Ort zu behalten.
10. Wählen Sie **Weiter** aus.

# Aktivieren Sie Schritt 2-Überprüfung für Ihre Google apps Benutzer

18.12.2018 • 2 minutes to read

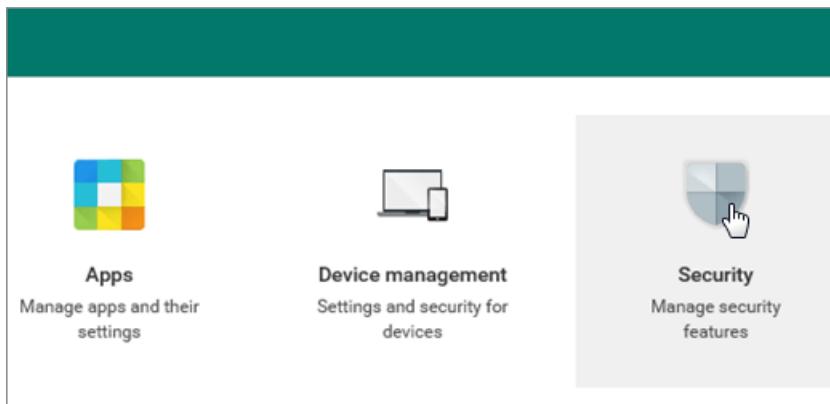
Wenn Sie Ihre Google app-Benutzer-e-Mail zu Office 365 migrieren möchten, müssen die Benutzer ein Kennwort app erstellen, die Sie zusammen mit ihren Google apps Kennwort zum Herstellen einer Verbindung ihrer Google Mail verwenden. Bevor sie ein Kennwort für die app erstellen können, müssen Sie so aktivieren Sie Schritt 2 Überprüfung in der Google Admin-Konsole zu können.

## Schritt 2-Verifizierung aktivieren

In der Reihenfolge für die Benutzer, eine app-Kennwort zu erstellen haben sie sich auf die erste Enable-Schritt 2 Prüfung.

### Zum Aktivieren der Überprüfung für Ihre Google apps Domäne-Schritt 2

1. Melden Sie sich die Google-Admin-Konsole.
2. Wählen Sie in der Konsole **Sicherheitsaus**.



3. Wählen Sie auf der Seite **Sicherheit grundlegender Einstellungenaus**.



## Security

contosogalleries.com

### Basic settings

Set password strength policies, enforce 2-step verification.

### Password monitoring

Monitor the password strength by user.

### API reference

Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

### Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

Show more

Und überprüfen Sie dann das Kontrollkästchen neben **Benutzern erlauben, 2-Schritt-Überprüfung zu aktivieren.**

<b>Two-step verification</b>	2-Step Verification adds an extra layer of security to your Google Apps accounts. Users are required to enter a verification code sent by Google (in addition to their username and password) when they sign in. ⓘ
<input checked="" type="checkbox"/> Allow users to turn on 2-step verification	
<a href="#">Go to advanced settings to enforce 2-step verification »</a>	

Check box to allow users to turn on 2-step verification.

4. Ihre Benutzer können jetzt 2 Schritt Überprüfung aktivieren und ein Kennwort für die app erstellen, wie hier beschrieben: [Vorbereiten Ihrer Google Mail-Konto für die Verbindung mit Outlook und Office 365](#).

# Migrieren von Postfächern von einem Office 365-Mandanten zu einem anderen

18.12.2018 • 22 minutes to read

[] In diesem Artikel wird mithilfe des Szenarios einer Firmenfusion erläutert, wie Sie Postfächer und Dienstinstellungen von einem Mandanten (Office 365) zu einem anderen Mandanten (Office 365) migrieren. Wenn mehr als 500 Benutzer oder eine große Menge SharePoint-Daten migriert werden müssen, empfiehlt es sich, mit einem [Office 365-Partner](#) zusammenzuarbeiten.

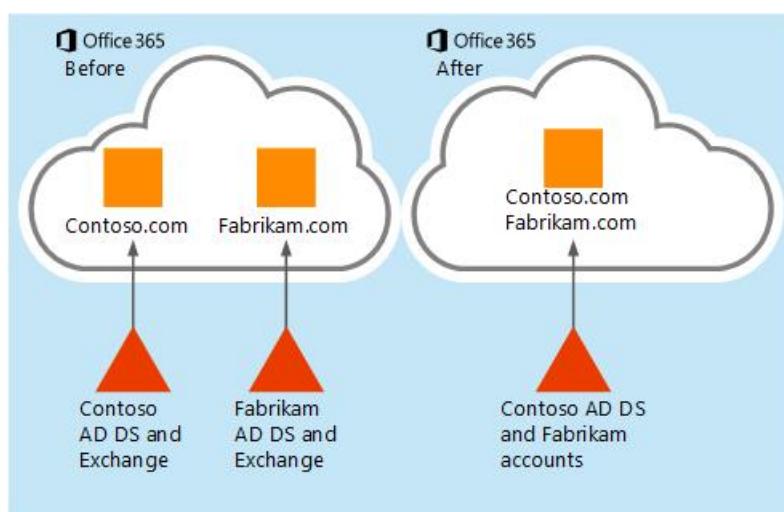
Das Szenario in diesem Artikel basiert auf zwei fiktiven Firmen, Contoso.com und Fabricam.com, die derzeit mit zwei verschiedenen Office 365-Mandanten arbeiten. Contoso hat Fabricam übernommen und möchte die Fabricam-Benutzer und -Daten in den Office 365-Mandanten von contoso.com verschieben.

	<b>MANDANT 1 (ZIEL)</b>	<b>MANDANT 2 (QUELLE)</b>
<b>Benutzerdefinierte E-Mail-Domäne:</b>	contoso.com	Fabricam.com
<b>Erste Office 365-Domäne:</b>	Contoso.onmicrosoft.com	Fabricam.onmicrosoft.com

## Szenario: Migration mit dem Migrationstool eines Drittanbieters

In diesem Szenario wird davon ausgegangen, dass Benutzer, Gruppen und andere Objekte der Firma Fabricam in Office 365 manuell erstellt werden, dann über ein Skript in das Portal importiert oder über AD DS-Konsolidierung (Active Directory Domain Services) mit dem Active Directory von Contoso zusammengeführt werden.

Nach Abschluss des Vorgangs sind alle Fabricam-Konten im Office 365-Mandanten von Contoso.com vorhanden und verwenden jeweils @fabrikam.com als UPN (Benutzerprinzipalname). Das endgültige Adressierungsschema wurde der Einfachheit und der Kürze halber ausgewählt, kann aber natürlich Ihren Anforderungen entsprechend angepasst werden.



### Planung: Zwei Wochen vor der Migration

Wenn Sie für die Migration Ihrer Benutzer das Migrationstool eines Drittanbieters verwenden, erwerben Sie die für Ihre Migration erforderlichen Lizenzen.

### Clientbezogene Überlegungen

Bei Outlook 2010 und Outlook 2013 müssen Sie lediglich das Outlook-Benutzerprofil löschen.

Bei Outlook 2007 und Outlook 2010 werden bei einem Neustart der Client per automatischer Erkennung konfiguriert und die OST-Datei wiederhergestellt.

Im Lync-Client müssen Sie nach Abschluss der Migration Kontakte hinzufügen.

## **Vorbereitung und Lizenzierung des Mandanten**

Der Quellmandant ist der Office 365-Mandant von Fabrikam, von dem aus Sie Benutzer und Daten migrieren. Der Zielmandant ist der Office 365-Mandant von Contoso, in den die Migration erfolgt.

1. Erhöhen Sie die Anzahl der Lizenzen im Office 365-Zielmandanten, um alle Postfächer abzudecken, die vom Quellmandanten migriert werden sollen.
2. Erstellen Sie Administratorkonten in den Quell- und Zielmandanten für die Migration von einem Office 365-System zu einem anderen Office 365-System. Einige Migrationstools setzen möglicherweise mehr als ein Administratorkonto im Quellmandanten voraus, um den Datendurchsatz zu optimieren.

## **Erstellen der Objekte "Raum", "Ressource", "Verteilergruppe" und "Benutzer" im Zielmandanten**

So erstellen Sie die Ressourcen im Zielmandanten (Contoso)

1. Wenn das Tool [Azure AD Connect](#) für die Synchronisierung aller Objekte in den Active Directory Domain Services (AD DS) von Contoso verwendet wird, müssen die Objekte aus den AD DS des Quellmandanten (Fabrikam) per Konsolidierung in den AD DS des Zielmandanten (Contoso) erstellt werden.
2. Die AD DS-Konsolidierung kann mithilfe einer Reihe von AD DS-Tools erfolgen. Je nach Menge der zu verschiebenden Objekte kann für die Konsolidierung zusätzliche Zeit und Planungsaufwand anfallen, daher sollte sie ggf. vor der eigentlichen Migration erfolgen.
3. Vergewissern Sie sich, dass alle neuen Benutzer und Gruppen über die Verzeichnissynchronisierung mit dem Zielmandanten Contoso.com synchronisiert werden. Die Objekte sollten als benutzer@contoso.onmicrosoft.com im neuen Mandanten angezeigt werden, da die Fabrikam-Domäne zu diesem Zeitpunkt noch nicht übernommen wurde. Die primäre E-Mail-Adresse der Benutzer und Gruppen kann auf @fabricam.com aktualisiert werden, nachdem die Domäne verschoben wurde.
4. Wenn die Verzeichnissynchronisierung nicht verwendet werden soll oder wenn irgendwelche Räume, Ressourcen, Gruppen oder Benutzer im Office 365 Admin Center des Quellmandanten verwaltet werden, müssen diese Objekte im Zielmandanten erstellt werden. Objekte können im Office 365 Admin Center manuell erstellt oder, bei einer größeren Anzahl, mithilfe einer CSV-Datei und der Funktion "Massenhinzufügung" im Office 365 Admin Center oder mit Windows PowerShell importiert werden.

## **Kommunikation mit den Endbenutzern**

So informieren Sie die Endbenutzer in der Organisation über die Migration

1. Erstellen Sie einen Migrationsplan, und beginnen Sie, die Benutzer zu der anstehenden Migration und den Änderungen im Dienst zu informieren.
2. Nach der Migration muss der Outlook-Cache für Spitznamen auf allen Outlook-Clients gelöscht werden. Lesen Sie [Gewusst wie: Zurücksetzen des Caches für Spitznamen und des Caches für automatische Vervollständigung in Outlook](#). Hier finden Sie ein automatisiertes Fix it-Tool, das von den Endbenutzern ausgeführt werden kann.
3. Informieren Sie die Benutzer, wie sie mit ihren neuen Anmeldeinformationen die Verbindung zu Outlook Web App herstellen können, falls nach der Migration ein Problem auftritt.

## **Vorbereitung und notwendige Schritte vor der Migration: Drei Tage vor der Migration**

## Domänenvorbereitung

Führen Sie die folgenden Schritte aus, um die Domäne für die Migration vorzubereiten.

1. Starten Sie auf dem Zielmandanten (Contoso) das Überprüfungsverfahren für die E-Mail-Domäne Fabrikam.com.
2. Fügen Sie im Office 365 Admin Center von contoso.com die Domäne fabrikam.com hinzu, und erstellen Sie TXT-Einträge im DNS (Domain Name System) zur Überprüfung.

### NOTE

Die Überprüfung schlägt fehl, da die Domäne noch von einem anderen Mandanten verwendet wird.

Wenn Sie diesen Schritt jetzt durchführen, geben Sie dem DNS-Eintrag Zeit für die Verbreitung, da diese bis zu 72 Stunden in Anspruch nehmen kann. Die abschließende Überprüfung erfolgt dann später.

## Migrationsplanung

Planen der Migration:

1. Erstellen Sie eine Masterliste mit Benutzerpostfächern, die migriert werden sollen.
2. Postfach-Zuordnung zu erstellen. CSV-Datei für das Migrationstool von Drittanbietern, die, das Sie verwenden. Diese Datei zur Zuordnung wird vom Migrationstool, der das Quellpostfach mit der Zielpostfach Mandanten entspricht, tritt Migration verwendet werden. *Es wird empfohlen, für die Verwendung der \*. "anfänglichen" Domäne "onmicrosoft.com" für die Quellkonten zuordnen, da die benutzerdefinierte e-Mail-Domäne ständig.*

A	B
1 <b>Source Email</b>	<b>Destination Email</b>
2 asmith@fabrikam.onmicrosoft.com	asmith@contoso.com
3 tandersen@fabrikam.onmicrosoft.com	tandersen@contoso.com
4 abaker@fabrikam.onmicrosoft.com	abaker@contoso.com
5 ablack@fabrikam.onmicrosoft.com	ablack@contoso.com
6	

## TTL-Test (Time to Live, Gültigkeitsdauer) des MX-Eintrags (Mail Exchanger)

Im nächsten Schritt planen Sie den TTL-Test.

1. Ändern Sie im DNS den TTL-Wert des MX-Eintrags der primäre E-Mail-Domäne, die Sie übertragen möchten, auf eine kleine Zahl (z. B. 5 Minuten). Wenn der TTL-Wert nicht auf 5 Minuten herabgesetzt werden kann, notieren Sie den niedrigsten Wert. Beispiel: Wenn der niedrigste Wert 4 Stunden beträgt, muss der MX-Eintrag 4 Stunden vor Beginn der Migration geändert werden.
2. [Die MX-Suche](#) kann verwendet werden, um MX- und DNS-Änderungen zu überprüfen.

## Deaktivieren der Verzeichnissynchronisierung im Quellmandanten

Deaktivieren Sie im Office 365 Admin Center des Quellmandanten die Verzeichnissynchronisierung. Dieser Vorgang kann 24 Stunden oder mehr in Anspruch nehmen, daher muss er vor der Migration durchgeführt werden. Nach der Deaktivierung im Portal werden Änderungen am AD DS des Quellmandanten nicht mehr mit dem Office 365-Mandanten synchronisiert. Passen Sie den vorhandenen Bereitstellungsprozess für Benutzer und Gruppen entsprechend an.

## Migration: Der Tag der Migration

Hier die Schritte, die Sie am Tag der Migration ausführen müssen.

## Ändern des MX-Eintrags - Stoppen des eingehenden E-Mail-Flusses

Ändern Sie den primären MX-Eintrag von Office 365 auf eine Domäne, die nicht erreichbar ist, wie "unerreichbar.beispiel.com". Internet-E-Mail-Server, die versuchen, neue E-Mails zu übermitteln, setzen diese E-Mails in die Warteschlange und versuchen 24 Stunden lang, sie erneut zuzustellen. Bei dieser Methode wird je nach Server, der versucht, die E-Mails zuzustellen, für einige E-Mails möglicherweise ein Unzustellbarkeitsbericht (NDR) zurückgegeben. Wenn dies ein Problem darstellt, verwenden Sie einen Datensicherungsdienst für den MX-Eintrag. Es gibt zahlreiche Drittanbieter-Dienste, die Ihre E-Mails tage- oder wochenlang für Sie in einer Warteschlange speichern. Nach Abschluss der Migration übermitteln diese Dienste die E-Mails aus der Warteschlange an den neuen Office 365-Mandanten.

### TIP

Wenn Ihr TTL-Wert nur kurz ist, beispielsweise 5 Minuten, kann dieser Schritt am Ende des Arbeitstags durchgeführt werden, um weniger Unterbrechungen zu verursachen. Bei einem größeren TTL-Wert müssen Sie den MX-Eintrag früh genug ändern, damit die Gültigkeitsdauer ablaufen kann. Beispiel: Ein TTL von 4 Stunden muss vor 14:00 Uhr geändert werden, wenn die Migration um 18:00 Uhr beginnen soll.

Überprüfen Sie bei Bedarf Ihre MX- und DNS-Änderungen. Zum Überprüfen von MX- und DNS-Änderungen kann Nslookup oder ein Dienst wie [MxToolbox](#) verwendet werden.

## Vorbereitung des Quellmandanten

Die primäre E-Mail-Domäne, fabrikam.com, muss von allen Objekten im Quellmandanten entfernt werden, bevor die Domäne in den Zielmandanten verschoben werden kann.

1. Wenn die Domäne zudem über eine öffentliche SharePoint Online-Website verfügt, müssen Sie die URL der Website erst auf die ursprüngliche Domäne zurücksetzen, bevor Sie die Domäne entfernen können.
2. Entfernen Sie im Lync-Administratorportal alle Lync-Lizenzen von den Benutzern im Quellmandanten. Damit wird die Lync-Sip-Adresse entfernt, die mit Fabrikam.com verbunden ist.
3. Setzen Sie die Standard-E-Mail-Adressen für die Office 365-Quellpostfächer auf die ursprüngliche Domäne (fabrikam.onmicrosoft.com) zurück.
4. Setzen Sie die Standard-E-Mail-Adressen im Quellmandanten für alle Verteilerlisten, Räume und Ressourcen auf die ursprüngliche Domäne (fabrikam.onmicrosoft.com) zurück.
5. Entfernen Sie alle sekundären (Proxy-) E-Mail-Adressen von Benutzerobjekten, die immer noch @fabrikam.com verwenden.
6. Legen Sie die Standarddomäne im Quellmandanten auf die Routingdomäne fabrikam.onmicrosoft.com fest (klicken Sie im Administratorportal in der oberen rechten Ecke auf Ihren Firmennamen).
7. Verwenden Sie den Windows PowerShell-Befehl Get-MsolUser -DomainName Fabrikam.com, um eine Liste aller Objekte abzurufen, die die Domäne weiterhin verwenden und die Entfernung blockieren.
8. Informationen zu häufig auftretenden Problemen beim Entfernen von Domänen finden Sie unter [Sie erhalten eine Fehlermeldung bei dem Versuch, eine Domäne aus Office 365 zu entfernen](#).

## Vorbereitung des Zielmandanten

Schließen Sie die Überprüfung der Domäne Fabrikam.com im Mandanten Contoso.com ab. Nach dem Entfernen der Domäne im alten Mandanten müssen Sie nun ggf. eine Stunde warten.

1. Konfigurieren Sie optional die automatische CNAME-Erkennung (intern/extern).
2. Wenn Sie AD FS verwenden, konfigurieren Sie die neue Domäne im Zielmandanten für AD FS.

3. Postfach-Aktivierung in den Mandanten "contoso.com" beginnen > aller der neuen Benutzerkonten Lizenzen zuweisen.
4. Legen Sie die E-Mail-Domäne fabrikam.com als primäre Adresse für die neuen Benutzer fest. Hierfür markieren/bearbeiten Sie mehrere nicht lizenzierte Benutzer im Portal oder verwenden Windows PowerShell.
5. Wenn Sie nicht die Funktion "Kennwort Hash Sync", Pass-Through-Authentifizierung oder AD FS verwenden, legen Sie das Kennwort für alle Postfächer im Mandanten Ziel (Contoso). Wenn Sie ein gemeinsames Kennwort nicht verwenden, benachrichtigen Sie Benutzer, der das neue Kennwort ein.
6. Nachdem die Postfächer mit Lizenzen versehen wurden und aktiv sind, beginnen Sie mit dem E-Mail-Routing. Sorgen Sie dafür, dass der Fabrikam-MX-Eintrag auf den Office 365-Zielmandanten (Contoso) verweist. Wenn der MX TTL abgelaufen ist, werden E-Mails an die neuen leeren Postfächer übermittelt. Wenn Sie einen MX-Datensicherungsdienst verwenden, können Sie veranlassen, dass E-Mails an die neuen Postfächer übertragen werden.
7. Überprüfen Sie den E-Mail-Fluss an die neuen Postfächern bzw. aus den neuen Postfächern im Zielmandanten.
8. Wenn Sie Exchange Online Protection (EOP) verwenden: Erstellen Sie im Zielmandanten die Transportregeln, Connectors, weißen und schwarzen Listen usw. des Quellmandanten erneut.

### **Starten der Migration**

Ermitteln Sie die beste Methode für die Migration, um Ausfallzeiten und Unannehmlichkeiten für die Benutzer möglichst gering zu halten.

- Migration von 500 oder weniger Benutzern: Migrieren Sie E-Mails, Kalender und Kontaktdaten in die Postfächer des Zielmandanten. Begrenzen Sie die E-Mail-Migration möglichst nach Datum. Migrieren Sie beispielsweise nur die Daten der letzten sechs Monate.
- Migration von mehr als 500 Benutzern: Arbeiten Sie mit mehreren Durchgängen, indem Sie zunächst die Kontakte, Kalender und nur die E-Mails der letzten Woche für alle Benutzer migrieren. Anschließend können Sie in den folgenden Tagen oder Wochen die Postfächer nach und nach mit älteren E-Mail-Daten füllen.

Beginnen Sie die E-Mail-Migration mit dem Migrationstool eines Drittanbieters.

1. Überwachen Sie den Migrationsfortschritt mithilfe der Tools des Anbieters. Geben Sie während der Migrations regelmäßig Fortschrittsberichte an das Verwaltungs- und Migrationsteam aus.
2. Nehmen Sie optional mehrstufige Migrationen vor, wenn alle Migrationen abgeschlossen sind.

Am Ende der Migration synchronisieren Outlook 2007 und 2010 das gesamte Postfach für jeden Benutzer, was je nach Menge der für jedes Postfach migrierten Daten eine erhebliche Bandbreite erfordert. In Outlook 2013 werden standardmäßig nur die Daten der letzten 12 Monate zwischengespeichert. Diese Einstellung kann für mehr oder weniger Daten konfiguriert werden. So können Sie beispielsweise nur die Daten der letzten drei Monate einbeziehen, was die Bandbreitenbelastung verringern kann.

### **Nach der Migration: Bereinigung**

Die Benutzer erhalten ggf. NDRs, wenn sie auf migrierte E-Mail-Nachrichten antworten. Der Outlook-Cache für Spitznamen muss gelöscht werden. Lesen Sie hierzu [Gewusst wie: Zurücksetzen des Caches für Spitznamen und des Caches für automatische Vervollständigung in Outlook](#). Alternativ können Sie für alle Benutzer den alten Legacy-DN als x.500-Proxyadresse hinzufügen.

## **Beispiele für Windows PowerShell-Skripts**

Verwenden Sie die folgenden Beispiele für Windows PowerShell-Skripts als Ausgangspunkt für die Erstellung eigener Skripts.

### **Massenzurücksetzung von Office 365-Kennwörter**

1. Erstellen Sie eine CSV-Datei mit dem Namen "password.csv".
2. Fügen Sie in dieser Datei die Spalten "upn" und "newpassword" ein (Beispiel:  
johanns@contoso.com,Kennwort1)
3. Verwenden Sie den Windows PowerShell-Befehl:

```
Import-Csv password.csv |%{Set-MsolUserPassword -userPrincipalName $_.upn -NewPassword $_.newpassword -ForceChangePassword $false}
```

### **Kopieren aller Office 365-Konten mit einer bestimmten Proxyadresse in eine CSV-Datei**

```
#####
# Script: showproxies.ps1
# Copies all accounts in Office 365 that contain/don't contain a specific
# proxyaddress to a .CSV file (addresses.csv)
#
# Change the following variable to the proxy address string you want to find:
# $proxyaddr = "onmicrosoft.com"
#####
$proxyaddr = "onmicrosoft.com"
# Create an object to hold the results
$addresses = @()
# Get every mailbox in the Exchange Organisation
$Mailboxes = Get-Mailbox -ResultSize Unlimited
# Loop through the mailboxes
ForEach ($mbx in $Mailboxes) {
    # Loop through every address assigned to the mailbox
    Foreach ($address in $mbx.EmailAddresses) {
        # If it contains XXX, Record it
        if ($address.ToString().ToLower().contains($proxyaddr)) {
            # This is an email address. Add it to the list
            $obj = "" | Select-Object Alias,EmailAddress
            $obj.Alias = $mbx.Alias
            $obj.EmailAddress = $address.ToString() #.Substring(10)
            $addresses += $obj
        }
    }
}
# Export the final object to a csv in the working directory

$addresses | Export-Csv addresses.csv -NoTypeInformation
# Open the csv with the default handler
Invoke-Item addresses.csv

##### END OF SHOWPROXIES.PS1
```

### **Massen erstellen es in Office 365**

```

#####
# Script: create-rooms.ps1
# Description:*** RUN THIS SCRIPT FROM A WINDOWS POWERSHELL SESSION ***
#This script creates rooms in Office 365.
# Syntax:Create-Rooms.ps1 -inputfile "file name.csv"
#
# Dependencies: Input file should contain 3 columns: RoomName, RoomSMTPAddress, RoomCapacity
#
#####
param( $inputFile )
Function Usage
{
$strScriptFileName = ($MyInvocation.ScriptName).substring(($MyInvocation.ScriptName).lastindexofany("\") +
1).ToString()
@"
NAME:
$strScriptFileName
EXAMPLE:
C:\PS> .\$strScriptFileName -inputfile `"file name.csv`"
@"
}
If (-not $inputFile) {Usage;Exit}
#Get MSO creds and initialize session
If ($cred -eq $NULL) {$Global:cred = Get-Credential}
#
If ($ExchRemoteCmdlets.AccessMode -ne "ReadWrite")
{
Write-Host
Write-Host Connecting to Office 365...
Write-Host
$NewSession = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://ps.outlook.com/powershell -Credential $cred -Authentication Basic -AllowRedirection
$Global:ExchRemoteCmdlets = Import-PSSession $NewSession
}
#Import the CSV file
$csv = Import-CSV $inputfile
#Create Rooms contained in the CSV file
$csv | foreach-object{
New-mailbox -Name $_.RoomName -room -primarysmtpaddress $_.RoomSMTPAddress -resourcecapacity $_.RoomCapacity
}
##### END OF CREATE-ROOMS.PS1

```

## **Massenentfernung von sekundären E-Mail-Adressen aus Postfächern**

```

#####
# Script: remove-proxy.ps1
#Description:*** RUN THIS SCRIPT FROM A WINDOWS POWERSHELL SESSION ***
#This script will remove a secondary email address from many users
#
# Syntax:remove-proxy.ps1 -inputfile "filename.csv"
#
# Dependencies:Input file should contain 2 columns: Username, Emailsuffix
# Example: Username=tim, Emailsuffix=fabrikam.com
#Script will remove the address tim@fabrikam.com from the mailbox for Tim.
#NOTE: Address must be secondary; it will not remove primary email address.
#
#####
param( $inputFile )
Function Usage
{
$strScriptFileName = ($MyInvocation.ScriptName).substring(($MyInvocation.ScriptName).lastIndexOfany("\" ) + 1).ToString()
@"
NAME:
$strScriptFileName
EXAMPLE:
C:\PS> .\$strScriptFileName -inputfile `"file name.csv`"
@"
}
If (-not $inputFile) {Usage;Exit}
#Get MSO creds and initialize session
If ($cred -eq $NULL) {$Global:cred = Get-Credential}
#
If ($ExchRemoteCmdlets.AccessMode -ne "ReadWrite")
{
Write-Host
Write-Host Connecting to Office 365...
Write-Host
$NewSession = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://ps.outlook.com/powershell -Credential $cred -Authentication Basic -AllowRedirection
$Global:ExchRemoteCmdlets = Import-PSSession $NewSession
}
#Import the CSV file and change primary smtp address
$csv = Import-CSV $inputfile
$csv | foreach-object{
# Set variable for email address to remove
$removeaddr = $_.username + "@" + $_.emailsuffix
Write-Host ("Processing User: " + $_.UserName +" - Removing " + $removeaddr)
Set-Mailbox $_.Username -EmailAddresses @{Remove=$removeaddr}
}
##### END OF REMOVE-PROXY.PS1

```

# Migrieren von Lotus Notes zu Office 365

18.12.2018 • 2 minutes to read

Beim Planen der Migration von e-Mail von IBM Lotus Notes zu Office 365, verwenden Sie die Anwendung Microsoft Online Notes Inspector (MONTI) für ausgewertet werden soll, wie viele Daten von Lotus Notes-Umgebung eines Kunden zu Office 365 migriert werden müssen.

Hier wird die Funktionsweise von MONTI:

- Er verarbeitet Mail-Dateien, um die Gesamtgröße der Datenbanken, Dokument Count (Kalender, Kontakte, Gruppen, e-Mail-Nachrichten und Aufgaben) und Größe von Tagen zu bestimmen.
- Mail-Datenbanken zum Bestimmen der Gesamtdatenbankgröße und Größe von Tagen verarbeitet.
- Es zurücksendet Ergebnisse unter Ansichten Personen, Mail-Datenbanken und Protokolle. Sie können diese Berichte manuell oder nach einem Zeitplan erstellen.

Laden Sie die [MONTI-Anwendung und die zugehörige Dokumentation](#) aus dem Microsoft Download Center herunter.

Die Dokumentation wird beschrieben, wie bereitstellen, konfigurieren und die MONTI-Anwendung in einem Kunden Domino-Umgebung ausführen.

# Hinzufügen eines SSL-Zertifikats zu Exchange 2013

18.12.2018 • 6 minutes to read

[] Einige Dienste, wie z. B. Outlook Anywhere, Übernahmemigration zu Office 365 und Exchange ActiveSync, erfordern das Konfigurieren von Zertifikaten auf Ihrem Exchange 2013-Server. In diesem Artikel wird gezeigt, wie Sie ein SSL-Zertifikat von einer Drittanbieter-Zertifizierungsstelle konfigurieren.

## Welche Berechtigungen sind erforderlich?

Zum Hinzufügen von Zertifikaten muss Ihnen die Rollengruppe [Organisationsverwaltung](#) auf dem Exchange Server 2013 zugewiesen sein.

## Schritte zum Hinzufügen eines SSL-Zertifikats

Hinzufügen ein SSL-Zertifikat auf Exchange Server 2013 ist ein Threestep-Vorgang.

1. Erstellen einer Zertifikatanforderung
2. Senden der Anforderung an die Zertifizierungsstelle
3. Importieren des Zertifikats

## Erstellen einer Zertifikatanforderung

### So erstellen Sie eine Zertifikatanforderung

1. Öffnen Sie das Exchange Admin Center (EAC), indem Sie zur URL Ihres Clientzugriffsservers wechseln, z. B. "<https://Ex2013CAS/ECP>".
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort mithilfe von im Format Domäne\Benutzername für Benutzername und auf **Anmelden**.
3. Wechseln Sie zu **Server > Zertifikate**. Stellen Sie auf der Seite **Zertifikate** sicher, dass im Feld **Server auswählen** der Clientzugriffsserver ausgewählt ist, und wählen Sie dann **neu +**.
4. Im **neuen Exchange-Zertifikat**-Assistenten wählen Sie **eine Anforderung für ein Zertifikat von einer Zertifizierungsstelle erstellen** aus, und wählen Sie dann auf **Weiter**.
5. Geben Sie einen Namen für dieses Zertifikat an, und wählen Sie dann **Weiter** aus.
6. Wenn Sie ein Platzhalterzertifikat anfordern möchten, wählen Sie **Platzhalterzertifikat anfordern** aus, und geben Sie dann die Stammdomäne alle Unterdomänen im Feld **Stammdomäne** an. Wenn Sie kein Platzhalterzertifikat anfordern möchten, sondern stattdessen jede Domäne, die zum Zertifikat hinzugefügt werden soll, angeben möchten, lassen Sie diese Seite leer. Wählen Sie **Weiter** aus.
7. Wählen Sie **Durchsuchen** aus, und geben Sie einen Exchange-Server an, auf dem das Zertifikat gespeichert werden soll. Bei dem ausgewählten Server sollte es sich um den Clientzugriffsserver mit Internetverbindung handeln. Wählen Sie **Weiter** aus.
8. Stellen Sie für jeden in der Liste angezeigten Dienst sicher, dass die externen oder internen Servernamen richtig sind, mit denen die Benutzer eine Verbindung mit dem Exchange-Server herstellen. Beispiel:
  - Wenn Sie die internen und externen URLs so konfiguriert haben, dass sie identisch sind, sollte für Outlook Web App (bei Zugriff über das Internet) und Outlook Web App (bei Zugriff über das Intranet)

"owa.contoso.com" angezeigt werden. Für das Offlineadressbuch (OAB) (bei Zugriff über das Internet) und OAB (bei Zugriff über das Intranet) sollte "mail.contoso.com" angezeigt werden.

- Wenn Sie die internen URLs so konfiguriert haben, dass sie "internal.contoso.com" lauten, sollte für Outlook Web App (bei Zugriff über das Internet) "owa.contoso.com" und für Outlook Web App (bei Zugriff über das Intranet) "internal.contoso.com" angezeigt werden.

Diese Domänen werden zum Erstellen der SSL-Zertifikatanforderung verwendet. Wählen Sie **Weiter** aus.

9. Fügen Sie alle zusätzlichen Domänen hinzu, die in das SSL-Zertifikat aufgenommen werden sollen.
10. Wählen Sie die Domäne, die den allgemeinen Namen für das Zertifikat enthalten sein sollen > **als allgemeiner Name festgelegt**. Beispielsweise "contoso.com". Wählen Sie auf **Weiter**.
11. Geben Sie Informationen zu Ihrer Organisation an. Diese Informationen werden in das SSL-Zertifikat aufgenommen. Wählen Sie **Weiter** aus.
12. Geben Sie den Netzwerkspeicherort an, an dem diese Zertifikatanforderung gespeichert werden soll. Wählen Sie **Fertig stellen** aus.

## Senden der Anforderung an die Zertifizierungsstelle

Nachdem Sie die Zertifikatanforderung gespeichert haben, senden Sie die Anforderung an Ihre Zertifizierungsstelle. Je nach Organisation kann es sich dabei um eine interne Zertifizierungsstelle oder eine Drittanbieter-Zertifizierungsstelle handeln. Clients, die eine Verbindung mit dem Clientzugriffsserver herstellen, müssen der verwendeten Zertifizierungsstelle vertrauen. Sie können auf der Website der Zertifizierungsstelle nach den jeweiligen Schritten zum Senden Ihrer Anforderung suchen.

## Importieren des Zertifikats

Nachdem Sie das Zertifikat von der Zertifizierungsstelle erhalten haben, führen Sie die folgenden Schritte aus.

### So importieren Sie das Zertifikat

1. Wählen Sie im EAC auf der Seite **Server > Zertifikate** die von Ihnen in den vorherigen Schritten erstellte Zertifikatanforderung aus.
2. Wählen Sie im Detailbereich der Zertifikatanforderung unter **Status** die Option **Abschließen** aus.
3. Geben Sie auf der Seite anstehende Anforderungen abschließen, den Pfad zum SSL-Zertifikat an > **OK**.
4. Wählen Sie das neue Zertifikat, das Sie gerade hinzugefügt, und wählen Sie dann auf **Bearbeiten** .
5. Wählen Sie auf der Zertifikatseite die Option **Dienste** aus.
6. Wählen Sie die Dienste aus, die Sie diesem Zertifikat zuweisen möchten. Sie sollten mindesten SMTP und IIS auswählen. Wählen Sie **Speichern** aus.
7. Wenn die Warnung **Soll das vorhandene SMTP-Standardzertifikat überschrieben werden?** angezeigt wird, wählen Sie **Ja** aus.

# Fügen Sie ein SSL-Zertifikat auf Exchange 2010

18.12.2018 • 6 minutes to read

Einige Dienste, wie Outlook Anywhere übernahmemigration in Office 365 und Exchange ActiveSync, müssen Zertifikate auf Ihrem Exchange 2010-Server konfiguriert werden. In diesem Artikel zeigt, wie ein SSL-Zertifikat von einer Drittanbieter-Zertifizierungsstelle (CA) zu konfigurieren.

## Welche Berechtigungen benötigen Sie?

Um Zertifikate hinzufügen möchten, müssen Sie die Rollengruppe "[Organisationsverwaltung](#)" auf dem Exchange 2010 zugewiesen werden.

## Schritte zum Hinzufügen eines SSL-Zertifikats

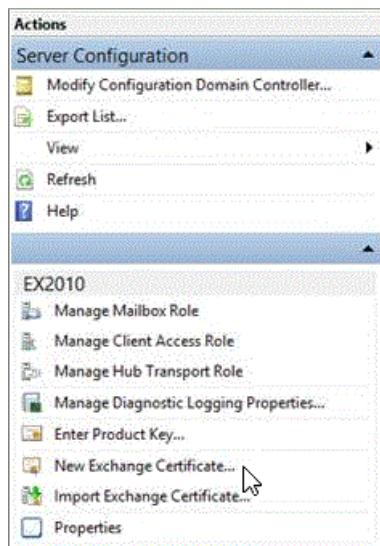
Hinzufügen ein SSL-Zertifikat auf Exchange 2010 ist drei Schritten.

1. Erstellen Sie eine zertifikatanforderung
2. Die Anforderung an die Zertifizierungsstelle übermitteln
3. Importieren des Zertifikats

## Erstellen Sie eine zertifikatanforderung

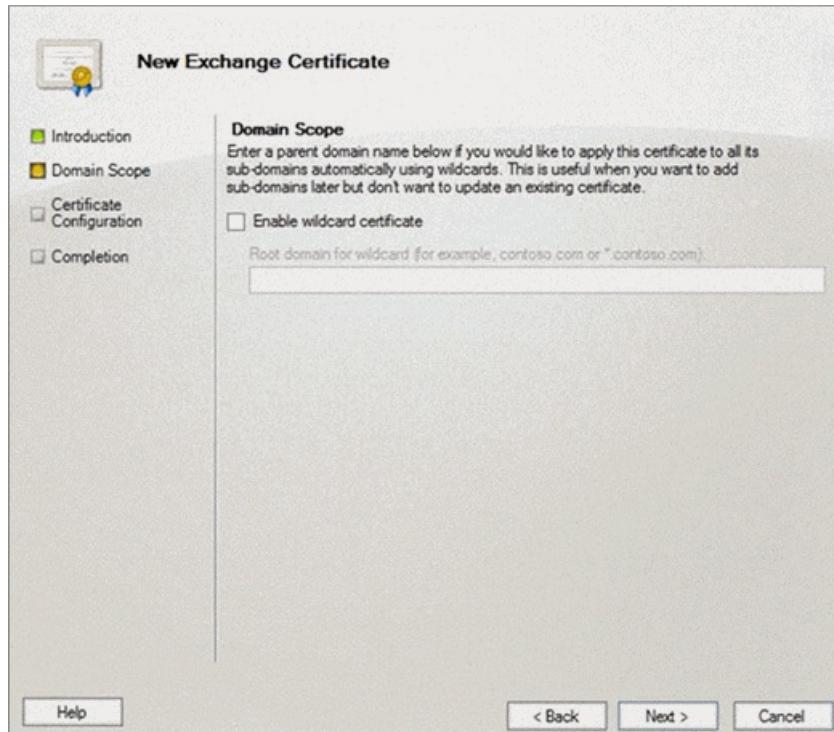
### So erstellen Sie eine zertifikatanforderung

1. Öffnen Sie die Exchange-Verwaltungskonsole (EMC).
2. Wählen Sie das Zertifikat hinzufügen möchten.
3. Wählen Sie im **Aktionsbereich Neue Exchange-Zertifikataus.**



4. Die **neue Exchange-Zertifikat**-Assistenten geben Sie einen Namen für dieses Zertifikat, und wählen Sie dann auf **Weiter**.
5. Geben Sie auf der Seite Domänenbereich der Stammdomäne für alle Unterdomänen in der **Stammdomäne** dar. Wenn Sie einen Platzhalter anfordern möchten, wählen Sie **Platzhalterzertifikat aktivieren**. Wenn Sie ein Platzhalterzertifikat anfordern möchten, müssen Sie jede Domäne angeben, den

Sie das Zertifikat auf der nächsten Seite hinzufügen möchten. Wählen Sie auf **Weiter**.



6. Stellen Sie sicher, dass die externe oder interne Servernamen, die Benutzer verwenden für den Exchange-Server die Verbindung richtig sind, auf der Seite **Exchange-Konfiguration** für jeden Dienst in der Liste angezeigt. Zum Beispiel:
  - Wenn Sie Ihren internen und externen URLs liegend konfiguriert sollte owa.contoso.com identisch, Outlook Web App (wenn über das Internet zugegriffen wird) und Outlook Web App (bei aus dem Intranet zugegriffen) angezeigt werden. Mail.contoso.com sollte Offline Address Book (OAB) (wenn über das Internet zugegriffen wird) und OAB (wenn aus dem Intranet zugegriffen) angezeigt werden.
  - Wenn Sie die internen URLs liegend internal.contoso.com konfiguriert haben, Outlook Web App (wenn über das Internet zugegriffen) owa.contoso.com sollte angezeigt werden, und Outlook Web App (bei aus dem Intranet zugegriffen) internal.contoso.com anzeigen.
7. Diese Domänen werden zum Erstellen der SSL-Zertifikat-Anforderung verwendet werden. Wählen Sie auf **Weiter**.
8. Fügen Sie auf der Seite **Zertifikat Domänen** beliebige zusätzlichen Domänen gewünschten auf das SSL-Zertifikat enthalten.

Wählen Sie die Domäne, die den allgemeinen Namen für das Zertifikat enthalten sein sollen > **als allgemeiner Name festgelegt**. Beispielsweise "contoso.com". Wählen Sie auf **Weiter**.
9. Geben Sie auf der Seite **Organisation und Ort** Informationen über Ihre Organisation. Diese Informationen werden mit dem SSL-Zertifikat eingeschlossen.

Geben Sie den Speicherort im Netzwerk dieses zertifikatanforderung gespeichert werden soll. Wählen Sie auf **Weiter**.
10. Überprüfen Sie auf der Seite **Zertifikatkonfiguration** zusammenfassende Informationen zu, wählen Sie **neu** aus, um das Zertifikat zu erstellen, und wählen Sie dann auf der **abschließenden Seite Fertig stellen**.

## Die Anforderung an die Zertifizierungsstelle übermitteln

Nachdem Sie die zertifikatanforderung gespeichert haben, senden Sie die Anforderung an die Zertifizierungsstelle (CA). Dies kann einer internen Zertifizierungsstelle oder einer Drittanbieter-Zertifizierungsstelle, abhängig von

Ihrer Organisation sein. Clients, auf denen die Clientzugriffs-Server hergestellt werden soll, müssen der Zertifizierungsstelle vertrauen, die Sie verwenden. Sie können die Website der Zertifizierungsstelle für die einzelnen Schritte für die Übermittlung Ihrer Anforderung suchen.

## Importieren des Zertifikats

Nachdem Sie das Zertifikat von der Zertifizierungsstelle erhalten haben, führen Sie die folgenden Schritte aus.

### So importieren Sie die zertifikatanforderung

1. Öffnen Sie die Exchange-Verwaltungskonsole.
2. Wählen Sie den Server, den Sie das Zertifikat importieren möchten.
3. Klicken Sie im **Exchange-Zertifikate** wählen Sie die Anforderung, die Sie zuvor erstellt haben, und wählen Sie im Bereich **Aktionen Anstehende Anforderung abschließen**.



4. Geben Sie auf der Seite **Abgeschlossen ausstehende Anforderung** den Pfad zum SSL-Zertifikat an, von der Zertifizierungsstelle erhalten > **abgeschlossen**.
5. Wählen Sie auf der Seite **Fertigstellung Fertig stellen**.
6. Wählen Sie den Exchange-Server, und wählen Sie auf der Registerkarte **Exchange-Zertifikate** das Zertifikat aus, Dienste, um auf die Exchange-Verwaltungskonsole, dieses Zertifikat zuzuweisen.  
Wählen Sie im Bereich **Aktionen Dem Zertifikat Dienste zuordnen**.
7. Wählen Sie den Namen des Servers, dem Sie das Zertifikat hinzufügen möchten, auf der Seite **Server auswählen** des Assistenten zum **Zuordnen von Diensten zum Zertifikat** > **Weiter**.
8. Wählen Sie die Dienste, den, die Sie diesem Zertifikat zuweisen möchten, klicken Sie auf der Seite **Dienste auswählen**. Sie sollten mindestens SMTP und IIS auswählen. Wählen Sie auf **Weiter**.
9. Wählen Sie auf der Seite **Dienste zuweisen zuweisen**.

Wenn Sie die Warnung **das vorhandene SMTP-Standardzertifikat überschrieben?**, wählen Sie **Ja** > **Fertig stellen**.

# Hinzufügen eines SSL-Zertifikats zu Exchange 2007

18.12.2018 • 5 minutes to read

[] Einige Dienste, wie z. B. Outlook Anywhere, Übernahmemigration zu Office 365 und Exchange ActiveSync, erfordern das Konfigurieren von Zertifikaten auf Ihrem Server mit Microsoft Exchange Server 2007. In diesem Artikel wird gezeigt, wie Sie ein SSL-Zertifikat von einer Drittanbieter-Zertifizierungsstelle konfigurieren.

## Schritte zum Hinzufügen eines SSL-Zertifikats

Das Hinzufügen eines SSL-Zertifikats zu Microsoft Exchange Server 2007 erfolgt in drei Schritten.

1. Erstellen einer Zertifikatanforderung
2. Senden der Anforderung an die Zertifizierungsstelle
3. Importieren des Zertifikats

## Erstellen einer Zertifikatanforderung

Zum Erstellen einer Zertifikatanforderung in Microsoft Exchange Server 2007 verwenden Sie den Befehl [New-ExchangeCertificate](#). Um den Befehl **New-ExchangeCertificate** auszuführen, muss das verwendete Konto der Exchange-Serveradministrator-Rolle und der Gruppe der lokalen Administratoren für den Zielserver angehören.

### So erstellen Sie eine Zertifikatanforderung

1. Öffnen Sie die Exchange-Verwaltungsshell auf dem lokalen Server.
2. Geben Sie in der Befehlszeile Folgendes ein:

```
New-ExchangeCertificate -DomainName  
"owa.servername.contoso.com","mail.servername.contoso.com","autodiscover.servername.contoso.com","sts.se  
rvername,contoso.com","oos.servername.contoso.com","mail12.servername.contoso.com","edge.servername.cont  
oso.com" -FriendlyName "Exchange 2007 Certificate" -GenerateRequest:$true -KeySize 2048 -Path  
"C:\certlocation" -PrivateKeyExportable $true -SubjectName "c=us, o=ContosoCorporation,  
cn=servername,contoso.com"
```

Im obigen Befehlsbeispiel ist *Servername* der Name Ihres Servers, "contoso.com" ist ein Beispiel für einen Domänennamen und *Certlocation* einen Pfad zu dem Speicherort, der die Anforderung gespeichert werden soll, sobald diese generiert wird, werden sollen. Ersetzen Sie alle diese Platzhalter durch die Informationen, die für die Exchange Server 2007 YourMicrosoft geeignet.

Fügen Sie den Domänennamen für die Zertifikatanforderung im Parameter *DomainName* hinzu. Wenn Sie Ihren internen und externen URLs dieselben konfiguriert haben, sollte beispielsweise der Domänennamen für Outlook Web App (wenn über das Internet zugegriffen wird) und Outlook Web App (bei aus dem Intranet zugegriffen) wie Owa aussehen. *Servername*. contoso.com.

Verwenden Sie den Parameter *SubjectName*, um den Antragstellernamen auf das sich ergebende Zertifikat anzugeben. Dieses Feld wird von den Diensten für DNS-fähigen verwendet und bindet ein Zertifikat an einen bestimmten Domänennamen ein.

Geben Sie den Parameter *GenerateRequest* als `$true`. Andernfalls, erstellen Sie ein selbstsigniertes Zertifikat.

3. Nach der Ausführung des obigen Befehls wird eine Zertifikatanforderung Speicherort der Datei gespeichert,

die Sie mithilfe des Parameters *Pfad* angegeben.

Der Befehl **New-ExchangeCertificate** erstellt auch einen *Fingerabdruck*-Output-Parameter, die Sie verwenden, wenn Sie die Anforderung an eine Drittanbieter-Zertifizierungsstelle im nächsten Schritt übermitteln.

## Senden der Anforderung an die Zertifizierungsstelle

Nachdem Sie die Zertifikatanforderung gespeichert haben, senden Sie die Anforderung an Ihre Zertifizierungsstelle. Je nach Organisation kann es sich dabei um eine interne Zertifizierungsstelle oder eine Drittanbieter-Zertifizierungsstelle handeln. Clients, die eine Verbindung mit dem Clientzugriffsserver herstellen, müssen der verwendeten Zertifizierungsstelle vertrauen. Sie können auf der Website der Zertifizierungsstelle nach den jeweiligen Schritten zum Senden Ihrer Anforderung suchen.

## Importieren des Zertifikats

Nachdem Sie das Zertifikat von der Zertifizierungsstelle erhalten haben, verwenden Sie den Befehl **Import-ExchangeCertificate** zum Importieren des Zertifikats.

### So importieren Sie das Zertifikat

1. Öffnen Sie die Exchange-Verwaltungsshell auf dem lokalen Server.
2. Geben Sie in der Befehlszeile Folgendes ein:

```
Import-ExchangeCertificate C:\filepath
```

Parameters *Filepath* gibt den Speicherort der Zertifikatsdatei an, die von der Zertifizierungsstelle, die von Drittanbietern bereitgestellt wurde.

Wenn Sie diesen Befehl ausführen, erstellt es einen *Fingerabdruck*-Output-Parameter, die Sie verwenden, um das Zertifikat im nächsten Schritt zu ermöglichen.

### So aktivieren Sie das Zertifikat

1. Zum Aktivieren des Zertifikats verwenden Sie den Befehl **Enable-ExchangeCertificate**. Geben Sie in der Befehlszeile Folgendes ein:

```
Enable-ExchangeCertificate -Thumbprint 5113ae0233a72fccb75b1d0198628675333d010e -Services  
iis,smtp,pop,imap
```

Der Parameter *Thumbprint* gibt der Datenbankserver empfangene als Ausgabe an, wenn Sie den Befehl **Import-ExchangeCertificate** ausgeführt haben.

Geben Sie im Parameter *Dienste* die Dienste, den, die Sie diesem Zertifikat zuweisen möchten. Sie sollten mindestens SMTP und IIS angeben.

2. Wenn Sie die Warnung **das vorhandene SMTP-Standardzertifikat überschrieben?**, geben Sie im  (Ja für alle).

## Siehe auch

[Blogartikel zum Hinzufügen von SSL zu Exchange Server 2007](#)

# Aktivieren Sie Ihre Google Mail-Konto für IMAP

18.12.2018 • 2 minutes to read

Internet Message Access Protocol (IMAP) ist ein Protokoll, das Herunterladen von Nachrichten von Servern einen e-Mail-Anbieter, wie für Gmail, auf dem Computer, damit Sie Microsoft Outlook verwenden können, anzeigen und bearbeiten Ihre e-Mail-Adresse, wann sogar ermöglicht, werden nicht verbunden mit dem Internet.

## Aktivieren Sie auf IMAP für Ihre Google Mail-Konto

Um Ihre Google Mail-Nachrichten von Microsoft Outlook zugreifen zu können, müssen Sie ihn für IMAP aktivieren.

1. Melden Sie sich mit Ihrem Google Mail-Konto mithilfe eines Browsers, das unterstützten (Google Chrome, Firefox, Internet Explorer oder Safari) ist.
2. Wählen Sie aus, oder klicken Sie auf das Symbol (Zahnrad)  auf der rechten oberen Ecke.
3. **Auswählen von > Weiterleitung und POP/IMAP.**
4. Wählen Sie **IMAP aktivieren** aus, und wählen Sie dann auf **Speichern**.

# Office 365-Migrationsleistung und bewährte Methoden

18.12.2018 • 55 minutes to read

Es gibt viele Möglichkeiten zum Migrieren von Daten aus einer lokalen E-Mail-Organisation zu Microsoft Office 365. Bei der Planung der Migration zu Office 365 stellt sich häufig die Frage, wie die Leistung bei der Datenmigration verbessert und die Geschwindigkeit bei der Migration erhöht werden können.

## NOTE

Die in diesem Artikel aufgeführten Leistungsangaben gelten nicht für den Office 365-Dienst für dedizierte Abonnementpläne. Weitere Informationen zu dedizierten Plänen finden Sie unter [Dedizierte Office 365-Pläne - Dienstbeschreibungen](#).

## Übersicht über das Migrieren von E-Mails zu Office 365

Office 365 unterstützt mehrere Methoden zum Migrieren von E-Mail-, Kalender- und Kontaktdaten aus Ihrer vorhandenen Messaging-Umgebung zu Office 365, wie unter [Methoden zum Migrieren von mehreren E-Mail-Konten zu Office 365](#) beschrieben.

Weitere Informationen zu Netzwerkfunktionen und zur Leistung von Office 365 finden Sie unter [Netzwerkplanung und Leistungsoptimierung für Office 365](#).

## Häufig verwendete Migrationsmethoden

MIGRATIONSMETHODE	BESCHREIBUNG	RESSOURCEN
IMAP (Internet Message Access Protocol)-Migration	Sie können die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell zum Migrieren des Inhalts von Benutzerpostfächern aus einem IMAP-Messagingsystem in Ihre Office 365-Postfächer verwenden. Dazu gehört das Migrieren von Postfächern von anderen gehosteten e-Mail-Diensten wie Gmail oder Yahoo Mail.	<a href="#">Migrieren von IMAP-Postfächern zu Office 365</a>

MIGRATIONSMETHODEN	BESCHREIBUNG	RESSOURCEN
Übernahmemigration	<p>Mit einer einstufigen Migration, migrieren Sie alle lokalen Postfächern zu Office 365 in einigen Tagen. Verwenden Sie übernahmemigration, wenn Sie planen, Ihre gesamte e-Mail-Organisation zu Office 365 zu verschieben und verwaltet Benutzerkonten in Office 365. Sie können maximal 2.000 Postfächer aus Ihrer lokalen Exchange-Organisation zu Office 365 mit einer einstufigen Migration migrieren. Die empfohlene Anzahl von Postfächern, ist jedoch <b>150</b>. Mit Zahlen höher ist als die Leistungsfähigkeit wird. Die e-Mail-Kontakte und Verteilergruppen in Ihrer lokalen Exchange-Organisation werden ebenfalls migriert.</p>	<a href="#">Übernahmemigration zu Office 365</a>
Mehrstufige Migration	<p>Wenn Sie schließlich planen, sämtliche Postfächer in Ihrer Organisation zu Office 365 zu migrieren, verwenden Sie die mehrstufige Migration. Bei der mehrstufigen Migration migrieren Sie Gruppen von lokalen Postfächern innerhalb weniger Wochen oder Monate zu Office 365.</p>	<a href="#">Wichtige Informationen zur mehrstufigen E-Mail-Migration nach Office 365</a>
Hybridbereitstellung	<p>Eine hybridbereitstellung Organisationen bietet die Möglichkeit, die funktionsreiche bereichert und Verwaltungsfunktionen, die sie mit ihren vorhandenen lokalen Exchange-Organisation in der Cloud. Eine hybridbereitstellung bietet das nahtlose Aussehen und Verhalten einer einzelnen Exchange-Organisation zwischen einer lokalen Exchange-Organisation und Exchange Online in Microsoft Office 365. Darüber hinaus kann eine hybridbereitstellung als intermediate Schritt für die Migration vollständig zu einer Office 365-Organisation unterstützen.</p>	<a href="#">Hybridbereitstellungen in Exchange Server 2013</a>

MIGRATIONSMETHODEN	BESCHREIBUNG	RESSOURCEN
Drittanbietermigration	<p>Es stehen viele Tools von Drittanbietern zur Verfügung. Sie verwenden unverkennbare Protokolle und Ansätze, um E-Mail-Migrationen von E-Mail-Plattformen wie IBM Lotus Notes und Novell GroupWise durchzuführen.</p>	<p>Unten sind einige Migrationstools von Drittanbietern und Partnerunternehmen aufgeführt, die Sie bei Exchange-Migrationen von Drittanbieter-Plattformen unterstützen können:</p> <p><b>Binary Tree:</b> Anbieter von plattformübergreifende Migration und Koexistenz Messagingsoftware, mit Produkten, die für die Analyse der und der Koexistenz und Migration zwischen lokalen und online Enterprise messaging und Zusammenarbeit bereitstellen Umgebungen, die basierend auf IBM Lotus Notes und Domino und Exchange und SharePoint.</p> <p><b>BitTitan:</b> Anbieter von Lösungen für die Migration zu Office 365.</p> <p><b>Metalogix:</b> Anbieter von Lösungen für die Migration zu Office 365 und SharePoint Online.</p> <p><b>Quadrotech:</b> Anbieter von Lösungen für die Migration zu Office 365.</p> <p><b>SkyKick:</b> Anbieter von Lösungen für die automatische Migration zum Verschieben der lokale Exchange, Google Mail, POP3, IMAP, Lotus Notes zu Office 365. Die End-to-End-Migrationstools Hilfe-Partner mit dem Umsatz, Planung, Migration, Verwaltung und vor-Ort-Phasen des Migrationsprojekts.</p> <p><b>TransVault:</b> Anbieter von Lösungen für die Migration zu Office 365.</p>

## Leistung für Migrationsmethoden

In den folgenden Abschnitten werden Mailbox Migration Arbeitslasten und die beobachteten Leistungsergebnisse für die verschiedenen Migrationsmethoden zum Migrieren von Postfächern und Postfachdaten in Office 365 verglichen. Diese Ergebnisse basieren auf internen Tests und tatsächlichen Kunden Migrationen zu Office 365.

### IMPORTANT

Aufgrund der Unterschiede bei wie Migrationen durchgeführt werden und wann sie ausgeführt werden kann die tatsächliche Migration Bremsen kann variieren.

### Kunden Migration Arbeitslasten

Die folgende Tabelle beschreibt die verschiedenen Arbeitslasten eine Migration, und die Optionen für die einzelnen und Herausforderungen beteiligt.

ARBEITSLAST	HINWEISE
Onboarding (Migrieren zu Office 365)	Microsoft bietet Daten Migrationsfunktion und Tools für Kunden zu verwenden, um ihre Daten zu Exchange Online (M365) aus der lokalen Exchange-Server zu migrieren. Es gibt eine Reihe von Methoden zum Migrieren von Postfächern und Postfachdaten, beginnend mit Einstufige Migrationen und mehrstufige Migrationen, die basieren auf Zusammenführen und Synchronisieren von Verschiebungen und weiter oben in diesem Artikel beschrieben werden. Die wichtigsten Migrationsmethode umfasst Hybrid wechselt, das ist zurzeit die am häufigsten verwendeten-Methode. Sie können entscheiden Sie genau beim Migrieren zu Microsoft 365, basierend auf Ihrer geschäftlichen Anforderungen.
Multi-Geo	Multinationale Unternehmen mit Büros auf der ganzen Welt benötigen häufig ihre Mitarbeiter Daten am-Rest in bestimmten Regionen zu speichern, um ihre Daten vor-Ort-Anforderungen zu erfüllen. Multi-Geo ermöglicht einen einzelnen Office 365-Mandanten umfassen über mehrere Regionen für Office 365-Datacenter (Geos), die Sie zum Speichern von Exchange-Daten ermöglicht, am-Rest, auf eine einzelne Benutzer in der ausgewählten Geos. Weitere Informationen finden Sie unter <a href="#">Unternehmensklasse globalen Speicherort Datensteuerelemente mit Multi-Geo erhalten möchten</a> .
Verschlüsselung	O365-Dienst-Verschlüsselung mit Kundenschlüssel ist ein Feature, mit dem Kunden für die Bereitstellung und Verwaltung der Stammschlüssel, die zum Verschlüsseln von Daten unter-Rest auf Anwendungsebene in Office 365 verwendet werden kann. Für ein Postfach zum ersten Mal verschlüsselt werden ist eine postfachverschiebung erforderlich. Weitere Informationen finden Sie unter <a href="#">Service-Verschlüsselung mit Kundenschlüssel für Office 365 – häufig gestellte Fragen</a> .
GoLocal	Microsoft weiterhin neue Rechenzentren für Office 365 in neue Regionen oder Geos zu öffnen. Bestehende Kunden können beim berechtigt, ihre Office 365 Kundendaten aus ihrer ursprünglichen Datacenter in eine neue Geo verschoben haben anfordern. Die Zeitspanne, in dem Sie diese Anforderung machen, ist in der Regel ein oder zwei Jahre, je nach die allgemeine Anforderungen an den Dienst. Notiz, die diese Zeitspanne, in dem Sie Ihre Kunden haben anfordern können, Daten verschoben wird kürzer, sobald ein Datacenter (DC) für die neue Geo (an diesem Punkt, mit denen Sie ungefähr drei bis sechs Monate Zeit startet, um eine Verschiebung anfordern). Details sind in <a href="#">Wechsel zu neuen Office 365 Datacenter Geos Core-Datenverfügbar</a> .

Beim Migrieren von Postfächern in Rechenzentren Microsoft 365 erfordert jeder Verschieben eines Postfachs oder Massen-postfachverschiebung Zeit für den Vorgang abgeschlossen ist. Es gibt eine Reihe von Faktoren, wie beispielsweise Microsoft 365 Serviceaktivität, die genau wie viel Zeit auswirken können. Der Dienst ist darauf ausgelegt, gedrosselt discretionary Arbeitslasten wie Verschieben von Postfächern um sicherzustellen, dass der Dienst optimal für alle Benutzer ausgeführt wird. Sie können weiterhin erwarten, dass das Verschieben von Postfächern, allerdings je nach den Dienst nach Ermessen ressourcenverfügbarkeit verarbeitet werden. Weitere Informationen zu ressourcensteuerung finden Sie in [diesem Blogbeitrag](#).

###Geschätzte Zeit für die migration

Als Hilfe bei der Planung der Migration präsentieren in den folgenden Tabellen Richtlinien zur Postfachmigration Massen oder einzelne Migrationen für die Durchführung auf Sie zukommt. Schätzung der Kosten basieren auf einer Analyse der vorherigen Kunden Migrationen. Da jede Umgebung eindeutig ist, kann die genaue migrationsgeschwindigkeit variieren.

#### **Dauer der Postfach-Migration basierend auf Postfach Größe Profile:**

##### 1. Onboarding / PSTImport

POSTFACHGRÖSSE (GB)	50. QUANTIL DAUER (IN TAGEN)	90 QUANTIL DAUER (IN TAGEN)
<1	1	7
1 - 10	1	7
10 - 50	3	14
50 - 100	3	30
100 – 200	8	45
>200	Nicht unterstützt	Nicht unterstützt

##### 2. Multi-Geo / GoLocal / Verschlüsselung

POSTFACHGRÖSSE (GB)	50. QUANTIL DAUER (IN TAGEN)	90 QUANTIL DAUER (IN TAGEN)
<1	1	7
1 - 10	1	10
10 - 50	3	30
50 - 100	15	45
100 – 200	30	60
>200	Nicht unterstützt	Nicht unterstützt

#### **Migration einer Dauer von 90 % des Postfachs abgeschlossen wird basierend auf Mandanten Größe Profile verschoben:**

MANDANTEN GRÖSSE (ANZAHL DER POSTFÄCHER)	DAUER (IN TAGEN)	KANN SO VIELE TAGE DAUERN, BIS
<1.000	5	14
1.000 - 5.000	10	30
5.000 - 10.000	20	45
10.000 - 50.000	30	60
50.000 – 100.000	45	90

MANDANTEN GRÖSSE (ANZAHL DER POSTFÄCHER)	DAUER (IN TAGEN)	KANN SO VIELE TAGE DAUERN, BIS
>1000,000	60	180

Beachten Sie, dass einige Postfächer Ausreißer länger dauert würde basierend auf das Postfach Profil. Auch, wenn ein Mandant durchschnittlich größer Postfächer verfügt, kann dies auch auf die erweiterten Dauer der Migration beitragen.

## Migrationsleistungsfaktoren

Bei der E-Mail-Migration sind einige allgemeine Faktoren gegeben, die sich auf die Migrationsleistung auswirken können.

### Allgemeine Faktoren für die Migrationsleistung

In der folgenden Tabelle ist eine Liste der allgemeinen Faktoren aufgeführt, die sich auf die Migrationsleistung auswirken können. Weitere Details werden in den Abschnitten behandelt, in denen die einzelnen Migrationsmethoden beschrieben sind.

FAKTOR	BESCHREIBUNG	BEISPIEL
Datenquelle	Das Gerät oder der Dienst, das bzw. der die zu migrierenden Daten hostet. Für die Datenquelle gelten möglicherweise viele Einschränkungen aufgrund von Hardwarespezifikationen, Endbenutzerarbeitsauslastung und Back-End-Wartungsaufgaben.	Gmail beschränkt die Menge der Daten, die während eines bestimmten Zeitraums extrahiert werden können.
Datentyp und -dichte	Aufgrund der eindeutigen Eigenschaft des Unternehmens eines Kunden können Typ und Kombination von E-Mail-Elementen innerhalb der Postfächer stark variieren.	Ein Postfach von 4 GB mit 400 Elementen, von denen jedes 10 MB an Anlagen umfasst, kann schneller migriert werden als ein Postfach von 4 GB mit 100.000 kleineren Elementen.
Migrationsserver	Viele Migrationslösungen verwenden einen Migrationsserver vom Typ "Jump-Box" oder "Arbeitsstation", um die Migration durchzuführen.	Kunden verwenden häufig einen virtuellen Computer mit geringer Leistung als Host für den MRSProxy-Dienst für Hybridbereitstellungen oder für nicht hybride Migrationen von Clientcomputern.
Migrationsmodul	Das Daten Migrationsmodul verantwortlich für das Abrufen von Daten vom Quellsystem konvertiert Daten, falls erforderlich. Das Modul klicken Sie dann die Daten über das Netzwerk übermittelt und fügt die Daten in der Office 365-Postfach. Postfach.	Der MRSProxy-Dienst weist eigene Stärken und Schwächen auf.
Lokale Network Appliances	Die End-to-End-Netzwerkleistung - von der Datenquelle zu den Exchange Online-Clientzugriffsserven - wirkt sich auf die Migrationsleistung aus.	Firewallkonfiguration und -spezifikationen in der lokalen Organisation.

FAKTOR	BESCHREIBUNG	BEISPIEL
Office 365-Dienst	Office 365 verfügt über die integrierte Unterstützung der Verwaltung der bei der Migration auftretenden Arbeitsauslastung sowie über die erforderlichen Features.	Die Benutzereinschränkungsrichtlinie weist Standardeinstellungen auf und beschränkt die maximale Gesamtübertragungsrate.

### Faktoren für die Netzwerkleistung

In diesem Abschnitt werden die bewährten Methoden zum Optimieren der Netzwerkleistung während der Migration beschrieben. Die Diskussion ist allgemein ausgerichtet, da die Hardware von Drittanbietern und Internetdienstanbieter (ISPs) während der Migration die größte Auswirkung auf die Leistung des Netzwerks haben.

Verwenden Sie den Exchange Analyzer, um die Netzwerkverbindungen mit Office 365 besser zu verstehen. Zum Ausführen der Exchange Analyzer-Tests im [Support- und Wiederherstellungs-Assistenten](#) wechseln Sie zu "Erweiterte Diagnosen" > "Exchange Online" > "Exchange Online-Netzwerkkonnektivität überprüfen" > "Ja". Weitere Informationen zum Support- und Wiederherstellungs-Assistenten finden Sie unter [Beheben von Outlook- und Office 365-Problemen mit dem Support- und Wiederherstellungs-Assistenten für Office 365](#).

FAKTOR	BESCHREIBUNG	BEWÄHRTE METHODEN
Netzwerkkapazität	Die zum Migrieren von Postfächern zu Office 365 erforderliche Zeitspanne wird durch die verfügbare und maximale Kapazität des Netzwerks bestimmt.	Identifizieren Sie die verfügbare Kapazität Ihres Netzwerk, und bestimmen Sie die maximale Kapazität für das Hochladen. Wenden Sie sich an Ihren Internetdienstanbieter, um Ihre zugewiesene Bandbreite zu bestätigen sowie Details zu Einschränkungen zu erhalten, z. B. zur Gesamtmenge der Daten, die in einem bestimmten Zeitraum übertragen werden kann. Verwenden Sie entsprechende Tools, um die tatsächliche Netzwerkkapazität auszuwerten. Stellen Sie sicher, dass Sie den End-to-End-Datenfluss von der lokalen Datenquelle zu den Microsoft Datacenter-Gatewayservern testen. Identifizieren Sie andere Auslastungen in Ihrem Netzwerk (z. B. Sicherungsdienstprogramme und geplante Wartungen), die sich auf die Netzwerkkapazität auswirken können.
Netzwerkstabilität	Schnelle Netzwerke führen nicht immer zu schnellen Migrationen. Wenn das Netzwerk nicht stabil ist, kann die Datenübertragung aufgrund der möglichen Fehlerkorrektur länger dauern. Je nach Migrationstyp kann die Fehlerkorrektur die Migrationsleistung erheblich beeinträchtigen.	Netzwerkhardware- und Treiberprobleme können häufig die Stabilität des Netzwerks beeinträchtigen. Arbeiten Sie mit den Hardwareanbietern zusammen, um Ihre Netzwerkgeräte zu verstehen, und wenden Sie die neuesten empfohlenen Treiber des Herstellers sowie entsprechende Softwareupdates an.

FAKTOR	BESCHREIBUNG	BEWÄHRTE METHODEN
Netzwerkverzögerungen	Für eine Netzwerkfirewall konfigurierte Funktionen zur Angriffserkennung verursachen häufig erhebliche Netzwerkverzögerungen und beeinträchtigen die Migrationsleistung. Das Migrieren von Daten zu Office 365-Postfächern hängt von Ihrer Internetverbindung ab. Verzögerungen im Internet beeinträchtigen die allgemeine Migrationsleistung. Darüber hinaus verfügen Benutzer in derselben Firma möglicherweise über Cloudpostfächer, die sich in Datencentern an unterschiedlichen geografischen Standorten befinden. Je nach Internetdienstanbieter des Kunden kann die Migrationsleistung variieren.	Werten Sie Netzwerkverzögerungen für alle potenziellen Microsoft-Datencenter aus, um sicherzustellen, dass das Ergebnis konsistent ist. (Dies hinterlässt für Endbenutzer zudem einen konsistenten Eindruck.) Arbeiten Sie mit Ihrem Internetdienstanbieter zusammen, um internetabhängige Probleme zu beheben. IP-Adressen für Microsoft-Rechenzentrumsserver zum Hinzufügen Ihrer Liste der zugelassenen oder alle Migration bezogene Datenverkehr von der Netzwerkfirewall umgehen. Weitere Informationen zu den Office 365-IP-Adressbereiche finden Sie unter <a href="#">Office 365-URLs und IP-Adressbereiche</a> .

Eine eingehendere Analyse der Migrationen in Ihrer Umgebung finden Sie in unserem [Blogbeitrag zur Verschiebungsanalyse](#). Der Beitrag umfasst ein Skript, das Sie beim Analysieren von Verschiebungsanforderungen unterstützt.

## Office 365-Einschränkung

In Office 365 werden verschiedene Einschränkungsmechanismen zur Gewährleistung der Sicherheit und Dienstverfügbarkeit eingesetzt. Die drei folgenden Einschränkungstypen können sich auf die Migrationsleistung auswirken:

- Benutzereinschränkung
- Migrationsdiensteinschränkung
- Auf dem Ressourcenstatus basierende Einschränkung

### NOTE

Die drei Arten von Office 365-Einschränkung wirken sich nicht auf alle Migrationsmethoden aus.

### Office 365-Benutzereinschränkung

Die Benutzereinschränkung wirkt sich auf die meisten Migrationstools von Drittanbietern sowie auf die Migrationsmethode zum Hochladen von Clients aus. Diese Migrationsmethoden verwenden Protokolle für den Clientzugriff, z. B. das RPC-über-HTTP-Protokoll, um Postfachdaten zu Office 365-Postfächern zu migrieren. Diese Tools werden zum Migrieren von Daten von Plattformen wie IBM Lotus Domino und Novell GroupWise verwendet.

Die Benutzereinschränkung ist die restriktivste Einschränkungsmethode in Office 365. Da die Benutzereinschränkung für die Verwendung für einen bestimmten Endbenutzer eingerichtet ist, wird bei einer Nutzung auf Anwendungsebene schnell die Einschränkungsrichtlinie überschritten, was eine langsamere Datenmigration zur Folge hat.

### Einschränkungen für den Office 365-Migrationsdienst

Die Migrationsdiensteinschränkung betrifft alle systemeigenen Office 365-Migrationstools. Von der Migrationsdiensteinschränkung werden gleichzeitige Migrationen und die Zuordnung von Dienstressourcen für systemeigene Office 365-Migrationslösungen verwaltet.

Die Migrationsdiensteinschränkung wirkt sich auf Migrationen aus, bei denen folgende Migrationsmethoden zum Einsatz kommen:

- IMAP-Migration
- Exchange-Übernahmemigration
- Mehrstufige Exchange-Migration
- Hybridmigrationen (auf dem MRSProxy-Dienst basierende Verschiebungen in eine Hybridumgebung)

Ein Beispiel für die Migrationsdiensteinschränkung ist das Kontrollieren der Anzahl der Postfächer, die während einfacher Exchange- und IMAP-Migrationen gleichzeitig migriert werden. Der Standardwert ist 10. Dies bedeutet, dass maximal 10 Postfächer aus allen Migrationsbatches zu einem bestimmten Zeitpunkt migriert werden. Sie können die Anzahl der parallelen Postfachmigrationen für einen Migrationsbatch entweder über die Exchange-Systemsteuerung oder über Windows PowerShell erhöhen. Weitere Informationen zum Optimieren dieser Einstellung finden Sie unter [Verwalten von Migrationsbatches in Office 365](#).

### Auf dem Office 365-Ressourcenstatus basierende Einschränkung

Alle Migrationsmethoden unterliegen der Kontrolle durch die Verfügbarkeitseinschränkung. Die Office 365-Diensteinschränkung wirkt sich hingegen nicht so stark wie die zuvor beschriebenen anderen Einschränkungstypen auf Office 365-Migrationen aus.

Die auf dem Ressourcenstatus basierende Einschränkung ist die am wenigsten offensive Einschränkungsmethode. Sie erfolgt, um ein Problem mit der Dienstverfügbarkeit zu verhindern, das die Endbenutzer und wichtige Dienstvorgänge beeinträchtigen könnte.

Bevor sich die Leistung des Dienstes so weit verschlechtert, dass die Leistung des Endbenutzers beeinträchtigt werden könnte, werden Hybridmigrationen verzögert, bis die Leistung wiederhergestellt ist und der Dienst zu einem Niveau unter dem Einschränkungsschwellenwert zurückkehrt.

Nachfolgend finden Sie Beispiele aus einem Exchange-Bericht zur Migrationsstatistik. Sie zeigen die Einträge, die bei Überschreitung des Schwellenwerts für die Diensteinschränkung protokolliert wurden.

```
1/25/2018 12:56:01 AM [BL2PRD0410CA012] Copy progress: 723/1456 messages, 225.8 MB (236,732,045 bytes)/416.5 MB (436,712,733 bytes).
```

```
1/25/2018 12:57:53 AM [BL2PRD0410CA012] Move for mailbox '/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=xxxxxxxxxxxxxxxxxxxxxx' is stalled because DataMoveReplicationConstraint is not satisfied for the database 'NAMPRD04DG031-db081' (agent MailboxDatabaseReplication). Failure Reason: Database edbf0766-1f2a-4552-9115-bb3a53a8380b doesn't satisfy constraint SecondDatacenter. There are no available healthy database copies. Will wait until 1/25/2018 1:27:53 AM.
```

```
1/25/2018 12:58:24 AM [BL2PRD0410CA012] Request is no longer stalled and will continue.
```

```
6/30/2017 00:03:58 [CY4PR19MB0056] Relinquishing job because of large delays due to unfavorable server health or budget limitations with a request throttling state 'StalledDueToTarget_DiskLatency'.
```

### Lösung und Übungsbeispiel

Wenn Sie eine ähnliche Situation auftreten, warten Sie auf die Office 365-Ressourcen verfügbar wird.

## Leistungsfaktoren und bewährte Methoden für die Migration von Nicht-Hybridbereitstellungen

In diesem Abschnitt werden die Faktoren beschrieben, die sich auf Migrationen auswirken, die die IMAP-, Übernahme- oder mehrstufigen Migrationsmethoden verwenden. Darüber hinaus werden die bewährten Methoden zum Optimieren der Migrationsleistung bezeichnet.

## Faktor 1: Datenquelle

In der folgenden Tabelle werden die durch Quellserver in Ihrer aktuellen E-Mail-Organisation verursachten Auswirkungen auf die Migration sowie die bewährten Methoden zum Verringern dieser Auswirkungen beschrieben:

CHECKLISTE	BESCHREIBUNG	BEWÄHRTE METHODEN
Systemleistung	<p>Die Datenextrahierung stellt eine intensive Aufgabe dar. Das Quellsystem muss über geeignete Ressourcen verfügen, z. B. CPU-Zeit und Arbeitsspeicher, um optimale Migrationsleistungen bieten zu können. Während der Migration befindet sich das Quellsystem hinsichtlich der normalen Arbeitsauslastung durch den Endbenutzer häufig am Rande seiner Kapazität. Wenn die Systemressourcen unzureichend sind, kann sich die zusätzliche Arbeitsauslastung, die sich durch die Migration ergibt, auf die Endbenutzer auswirken.</p>	<p>Überwachen Sie die Systemleistung während eines Migrationstests. Wenn das System ausgelastet ist, wird aufgrund potenzieller verringriger Migrationsgeschwindigkeiten und Dienstverfügbarkeitsproblemen empfohlen, einen offensiveren Migrationszeitplan für das System zu vermeiden. Erweitern Sie nach Möglichkeit die Quellsystemleistung durch Hinzufügen von Hardwareressourcen, und verringern Sie die Auslastung des Systems durch Verschieben von Aufgaben und Benutzern auf andere Server, die nicht an der Migration beteiligt sind.</p> <p>Weitere Informationen finden Sie unter:</p> <ul style="list-style-type: none"> <li>• <a href="#">Exchange 2013 Server Health and Performance</a></li> <li>• <a href="#">Grundlegendes zu Exchange 2010-Leistung</a></li> <li>• <a href="#">Exchange 2007: Überwachen von Postfachservern</a></li> </ul> <p>Bei der Migration von einer lokalen Exchange-Organisation, die mehrere Postfachserver umfasst, wird empfohlen, dass Sie eine Liste der Migrationsbenutzer erstellen, die gleichmäßig auf die verschiedenen Postfachserver verteilt wird. Auf Grundlage der jeweiligen Serverleistung kann die Liste weiter optimiert werden, um den Durchsatz zu maximieren.</p> <p>Wenn Server A z. B. über eine um 50 Prozent höhere Ressourcenverfügbarkeit als Server B aufweist, ist es sinnvoll, 50 Prozent mehr Benutzer von Server A in demselben Migrationsbatch zu verwenden. Ähnliche Methoden können auf andere Quellsysteme angewendet werden. Führen Sie die Migrationen aus, wenn die Server eine maximale Ressourcenverfügbarkeit aufweisen, z. B. nach Feierabend oder an Wochenenden oder Feiertagen.</p>

CHECKLISTE	BESCHREIBUNG	BEWÄHRTE METHODEN
Back-End-Aufgaben	Andere Back-End-Aufgaben, die während der Migrationszeit ausgeführt werden. Da es sich als bewährte Methode erweist, die Migration außerhalb der Geschäftszeiten durchzuführen, kommt es häufig vor, dass Migrationen mit Wartungsaufgaben (z. B. Datensicherungen) in Konflikt geraten, die auf den lokalen Servern ausgeführt werden.	Überprüfen Sie andere Systemaufgaben, die möglicherweise während der Migration ausgeführt werden. Es wird empfohlen, dass Sie die Datenmigration ausführen, wenn keine anderen ressourcenintensiven Aufgaben ausgeführt werden. <b>Hinweis:</b> für Kunden mit lokalem Exchange, die Back-End-Aufgaben werden datensicherungslösungen sowie um <a href="#">Wartung der Exchange-Informationsspeicher</a> .
Einschränkungsrichtlinie	Es ist allgemein üblich, E-Mail-Systeme mit einer Einschränkungsrichtlinie zu schützen, die einen bestimmten Grenzwert festlegt, wie schnell und wie viele Daten während einer bestimmten Zeitspanne aus dem System extrahiert werden können.	Überprüfen Sie, welche Einschränkungsrichtlinie auf Ihr E-Mail-System angewendet wird. Google Mail beschränkt z. B. die Datenmenge, die in einem bestimmten Zeitraum extrahiert werden kann.  Je nach Version weist Exchange Richtlinien auf, die den IMAP-Zugriff auf den lokalen E-Mail-Server (verwendet von IMAP-Migrationen) und den RPC-über-HTTP-Protokollzugriff (verwendet von Exchange-Übernahmemigrationen und mehrstufigen Exchange-Migrationen) einschränkt.  Zum Überprüfen der Einschränkungseinstellungen in einer Exchange 2013-Organisation führen Sie das Cmdlet <a href="#">Get-ThrottlingPolicy</a> aus. Weitere Informationen finden Sie unter <a href="#">Verwaltung der Exchange-Arbeitsauslastung</a> .  Weitere Informationen zur IMAP-Einschränkung finden Sie unter <a href="#">Migrieren von IMAP-Postfächern zu Office 365</a>  Weitere Informationen zur Einschränkung des RPC-über-HTTP-Protokolls finden Sie unter: <ul style="list-style-type: none"><li>• <a href="#">Exchange 2013-Arbeitsauslastungsverwaltung</a></li><li>• <a href="#">Exchange 2010: Grundlegendes zu Clienteinschränkung Richtlinien</a></li><li>• <a href="#">Exchange 2007: Grundlegendes zu Clienteinschränkung</a></li></ul>

## Faktor 2: Migrationsserver

IMAP-, Übernahme- und mehrstufige Migrationen sind über die Cloud eingeleitete Migrationsmethoden mit Datenabruft, daher sind keine dedizierten Migrationsserver erforderlich. Die internetfähigen Protokollhosts (IMAP oder RPC-über-HTTP-Protokoll) funktionieren jedoch als Migrationsserver zum Migrieren von Postfächern und Postfachdaten zu Office 365. Daher gelten die Faktoren und bewährten Methoden für die Migrationsleistung, die im vorherigen Abschnitt zum Datenquellserver für Ihre aktuelle E-Mail-Organisation beschrieben wurden, auch für die Internet-Edgeserver. Für Exchange 2007-, Exchange Server 2010- und Exchange 2013-Organisationen

funktionsweise der Clientzugriffsserver als Migrationsserver.

Weitere Informationen finden Sie unter:

- [Verwaltung der Exchange 2013-Arbeitsauslastung](#)
- [Exchange 2010: Indikatoren für Clientzugriffsserver](#)
- [Exchange 2007: Überwachen von Clientzugriffsservern](#)

### Faktor 3: Migrationsmodul

IMAP-, Übernahme- und mehrstufige Exchange-Migrationen werden mithilfe des Migrationsdashboards im Exchange Admin Center durchgeführt. Dies unterliegt der Office 365-Migrationsdiensteinschränkung.

### Lösung und Übungsbeispiel

Kunden können jetzt mithilfe von Windows PowerShell die Migrationsparallelität angeben (z. B. die Anzahl der gleichzeitig zu migrierenden Postfächer). Der Standardwert ist 20 Postfächer. Nachdem Sie einen Migrationsbatch erstellt haben, können Sie diesen Wert mithilfe des folgenden Windows PowerShell-Cmdlets auf maximal 100 erhöhen.

```
Set-MigrationEndPoint <Identity> -MaxConcurrentMigrations <value between 1 and 100>
```

Weitere Informationen finden Sie unter [Verwalten von Migrationsbatches in Office 365](#).

#### NOTE

Wenn Ihre Datenquelle nicht über ausreichend Ressourcen verfügt, um alle Verbindungen zu verwalten, wird empfohlen, die hohe Parallelität zu vermeiden. Beginnen Sie mit einem kleinen Wert für die Parallelität, z. B. mit 10. Erhöhen Sie diesen Wert während der Überwachung der Leistung der Datenquelle, um Probleme beim Endbenutzerzugriff zu vermeiden.

### Faktor 4: Netzwerk

#### Überprüfungstests

Je nach Migrationsmethode können Sie die folgenden Überprüfungstests ausprobieren:

- **IMAP-Migrationen:** Auffüllen einer Quellpostfach mit Beispieldaten. Klicken Sie dann aus dem Internet (außerhalb des lokalen Netzwerks), Herstellen einer Verbindung mit dem Quellpostfach mithilfe einer standard IMAP-e-Mail-Clients wie Microsoft Outlook, und klicken Sie dann messen Sie netzwerkleistung bestimmen, wie lange es dauert, laden Sie alle Daten aus der Quelle Postfach. Der Durchsatz sollte ähnlich, was Kunden mithilfe des IMAP-Migrationstools in Office 365, vorausgesetzt, dass es keine anderen Einschränkungen sind abrufen können.
- **Cutover und mehrstufige Exchange-Migrationen:** Auffüllen einer Quellpostfach mit Beispieldaten. Klicken Sie dann aus dem Internet (außerhalb des lokalen Netzwerks), eine Verbindung zu das Quellpostfach mit Outlook mithilfe von RPC über HTTP-Protokoll. Stellen Sie sicher, dass Sie eine Verbindung herstellen, mithilfe der **Cache-Modus**. Messen der netzwerkleistung überprüfen Sie, wie lange es dauert, um alle Daten aus dem Quellpostfach zu synchronisieren. Der Durchsatz sollte ähnlich, was Kunden mithilfe der einfachen Exchange-Migrationstools in Office 365, vorausgesetzt, dass es keine anderen Einschränkungen sind abrufen können.

Während einer tatsächlichen IMAP-, Übernahme- oder mehrstufigen Exchange-Migration kommt es zu einem gewissen Mehraufwand. Der tatsächliche Durchsatz sollte jedoch den Ergebnissen dieser Überprüfungstest ähnlich sein.

### Faktor 5: Office 365-Dienst

Die auf dem Ressourcenstatus von Office 365 basierende Einschränkung wirkt sich auf Migrationen aus, die die systemeigenen einfachen Office 365-Migrationstools verwenden. Weitere Informationen finden Sie im Abschnitt [Auf dem Office 365-Ressourcenstatus basierende Einschränkung](#).

## Verschiebungsanforderungen im Office 365-Dienst

Allgemeine Informationen zum Abrufen von Statusinformationen für Verschiebungsanforderungen finden Sie unter [Anzeigen der Eigenschaften von Verschiebungsanforderungen](#).

Im Office 365-Dienst werden anders als beim lokalen Exchange Server 2010 die Migrationswarteschlange und Dienstressourcen, die den Migrationen zugeordnet sind, von den Mandanten gemeinsam genutzt. Diese Freigabe wirkt sich darauf aus, wie Verschiebungsanforderungen in den einzelnen Phasen der Verschiebung behandelt werden.

Es gibt zwei Arten von Verschiebungsanforderungen in Office 365:

- **Onboarding verschiebungsanforderungen:** neue Kunden Migrationen Onboarding-verschiebungsanforderungen berücksichtigt werden. Diese Anfragen haben normale Priorität.
- **Interne Datacenter verschiebungsanforderungen:** Hierbei handelt es sich um Postfach verschiebungsanforderungen von Teams, Datacenter-Vorgang initiiert hat. Diese Anfragen haben eine niedrigere Priorität, da durch der Endbenutzer betroffen nicht zur Verfügung, wenn die verschiebungsanforderung verzögert wird.

### Potenzielle Auswirkungen und Verzögerungen für Verschiebungsanforderungen mit dem Status "In der Warteschlange" und "In Bearbeitung"

- **Verschieben von Anforderungen in Warteschlange:** dieser Status gibt an, dass die Verschiebung wurde in die Warteschlange und wartet auf die vom Exchange-Postfach-Replikationsdienst aufgenommene. Für Exchange 2003-verschiebungsanforderungen können Benutzer in dieser Phase weiterhin ihre Postfächer zugreifen.

Zwei Faktoren beeinflussen, welche Anforderung vom Postfachreplikationsdienst ausgewählt wird:

- **Priorität:** in der Warteschlange verschiebungsanforderungen mit einer höheren Priorität werden vor dem Verschieben von Anforderungen niedrigerer Priorität aufgenommene. Dadurch wird sichergestellt, dass verschiebungsanforderungen Customer-Migration vor dem internen Datacenter verschiebungsanforderungen immer verarbeitet.
- **Position in der Warteschlange:** Wenn verschiebungsanforderungen die gleiche Priorität, die zuvor Ruft die Anforderung in die Warteschlange haben, die zuvor es wird ausgewählt werden durch die Mailbox Replication Service. Da es mehrere Kunden Postfachmigrationen zur selben Zeit ausführen könnten, ist es normal, dass neue verschiebungsanforderungen in der Warteschlange bleiben, bevor sie verarbeitet werden.

Häufig wird die Zeit, die Postfachanforderungen vor der Verarbeitung in der Warteschlange warten, während der Migrationsplanung nicht berücksichtigt. Dies führt zu Kunden, für die nicht genügend Zeit reserviert wurde, um alle geplanten Migrationen abzuschließen.

- **In Bearbeitung verschiebungsanforderungen:** dieser Status gibt an, dass die Verschiebung noch ausgeführt wird. Ist dies ein online-Postfach verschieben, wird der Benutzer weiterhin an das Postfach zugegriffen hat sein. Für das Verschieben von Postfächern offline wird das Postfach des Benutzers nicht verfügbar sein.

Nachdem die Verschiebungsanforderung für das Postfach den Status "In Bearbeitung" aufweist, hat die Priorität keine Bedeutung mehr und neue Verschiebungsanforderungen werden nicht verarbeitet, bis eine vorhandene Verschiebungsanforderung mit dem Status "In Bearbeitung" abgeschlossen wird, auch wenn die neue Verschiebungsanforderung eine höhere Priorität aufweist.

## Bewährte Methoden

**Planung:** wie zuvor erwähnt, da Exchange 2003-Benutzer keinen Zugriff während einer hybridmigration Kunden mit Exchange 2003 werden in der Regel mehr betreffenden dazu, wann Sie Migrationen planen und wie lange sie dauern werden.

Bei der Planung der Anzahl der zu migrierenden Postfächer während eines bestimmten Zeitraums, sollten Sie Folgendes berücksichtigen:

- Beziehen Sie die Zeitspanne mit ein, die die Verschiebungsanforderung in der Warteschlange wartet. Diese kann wie folgt berechnet werden:

$$\text{(Gesamtzahl der zu migrierenden Postfächer)} = ((\text{Gesamtzeit}) - (\text{durchschnittliche Wartezeit})) * (\text{Migrationsdurchsatz})$$

Dabei entspricht der Migrationsdurchsatz der Gesamtzahl der Postfächer, die pro Stunde migriert werden können.

Nehmen Sie beispielsweise an, Sie verfügen für die Migration von Postfächern über ein Zeitfenster von sechs Stunden. Wenn die durchschnittliche Zeit in der Warteschlange eine Stunde beträgt, und Sie einen Migrationsdurchsatz von 100 Postfächern pro Stunde erreichen, können Sie innerhalb von sechs Stunden 500 Postfächer migrieren:  $500 = (6 - 1) * 100$ .

- Starten Sie die Migration früher als anfänglich geplant, um die Zeit in der Warteschlange zu verringern. Wenn sich die Postfächer in der Warteschlange befinden, können Exchange 2003-Benutzer weiterhin auf ihre Postfächer zugreifen.

**Determine Zeit in der Warteschlange:** die Zeit in der Warteschlange ist nie konstant, da die Migrationspläne von Kunden nicht von Microsoft verwaltet.

Um die potenzielle Wartezeit zu ermitteln, kann ein Kunde versuchen, mehrere Stunden vor dem Start der eigentlichen Migration eine Testverschiebung zu planen. Der Kunde kann dann auf Grundlage der ermittelten Dauer, die die Anforderung in der Warteschlange verweilt, besser einschätzen, wann die Migration gestartet werden muss. Zudem kann er besser beurteilen, wie viele Postfächer im angegebenen Zeitraum verschoben werden können.

Wenn eine Testmigration z. B. vier Stunden vor dem Start einer geplanten Migration abgeschlossen wurde. Der Kunde hat ermittelt, dass die Warteschlangenzzeit für die Testmigration ungefähr eine Stunde ergibt. Dann sollte der Kunden erwägen, die Migration eine Stunde früher zu starten als ursprünglich geplant, um sicherzustellen, dass ausreichend Zeit zum Abschließen aller Migrationen verfügbar ist.

## Drittanbiertools für Office 365-Migrationen

Drittanbiertools werden hauptsächlich in Migrationsszenarien verwendet, die kein Exchange umfassen, z. B. in Szenarien mit Google Mail, IBM Lotus Domino und Novell GroupWise. Dieser Abschnitt konzentriert sich auf die von Migrationstools von Drittanbietern verwendeten Protokolle, anstatt auf die eigentlichen Produkte und Migrationstools. Die folgende Tabelle enthält eine Liste von Faktoren, die für Migrationstools von Drittanbietern in Office 365-Migrationsszenarien gelten.

### Faktor 1: Datenquelle

CHECKLISTE	BESCHREIBUNG	BEWÄHRTE METHODEN
------------	--------------	-------------------

CHECKLISTE	BESCHREIBUNG	BEWÄHRTE METHODEN
Systemleistung	<p>Die Datenextrahierung stellt eine intensive Aufgabe dar. Das Quellsystem muss über geeignete Ressourcen verfügen, z. B. CPU-Zeit und Arbeitsspeicher, um optimale Migrationsleistungen bieten zu können. Während der Migration befindet sich das Quellsystem hinsichtlich der normalen Arbeitsauslastung durch den Endbenutzer häufig am Rande seiner Kapazität. Wenn die Systemressourcen unzureichend sind, kann sich die zusätzliche Arbeitsauslastung, die sich durch die Migration ergibt, auf die Endbenutzer auswirken.</p>	<p>Überwachen Sie die Systemleistung während eines Migrationstests. Wenn das System ausgelastet ist, wird aufgrund potenzieller verringriger Migrationsgeschwindigkeiten und Dienstverfügbarkeitsproblemen empfohlen, einen offensiveren Migrationszeitplan für das System zu vermeiden. Erhöhen Sie nach Möglichkeit die Leistung des Quellsystems durch Hinzufügen von Hardwareressourcen und Verringern der Arbeitsauslastung des Systems. Die Arbeitsauslastung des Systems kann durch Verschieben von Aufgaben und Benutzern auf andere Server verringert werden, die nicht in die Migration einbezogen sind.</p> <p>Weitere Informationen finden Sie unter:</p> <ul style="list-style-type: none"> <li>• <a href="#">Exchange 2013 Server Health and Performance</a></li> <li>• <a href="#">Grundlegendes zu Exchange 2010-Leistung</a></li> <li>• <a href="#">Exchange 2007: Überwachen von Postfachservern</a></li> </ul> <p>Bei der Migration von einer lokalen Exchange-Organisation, die mehrere Postfachserver umfasst, wird empfohlen, dass Sie eine Liste der Migrationsbenutzer erstellen, die gleichmäßig auf die verschiedenen Postfachserver verteilt wird. Auf Grundlage der jeweiligen Serverleistung kann die Liste weiter optimiert werden, um den Durchsatz zu maximieren.</p> <p>Verfügt Server A beispielsweise über eine um 50 Prozent höhere Ressourcenverfügbarkeit als Server B, bietet es sich an, in einem Migrationsbatch den Benutzeranteil von Server A um 50 Prozent zu erhöhen. Eine ähnliche Methode kann auch für andere Quellsysteme angewendet werden.</p> <p>Die Migration sollte bei maximaler Ressourcenverfügbarkeit des Systems ausgeführt werden, also beispielsweise außerhalb der Geschäftszeiten, an Wochenenden oder an Feiertagen.</p>

CHECKLISTE	BESCHREIBUNG	BEWÄHRTE METHODEN
Back-End-Aufgaben	<p>Andere Back-End-Aufgaben, die in der Regel während der Migrationszeit ausgeführt werden. Da es sich als bewährte Methode erweist, die Migration außerhalb der Geschäftszeiten durchzuführen, kommt es häufig vor, dass Migrationen mit anderen Wartungsaufgaben in Konflikt geraten, die auf den lokalen Servern ausgeführt werden, z. B. Datensicherungen.</p>	<p>Überprüfen Sie andere Systemaufgaben, die während der Migration ausgeführt werden. Es wird empfohlen, dass Sie ein ausschließlich für die Datenmigration vorgesehenes Zeitfenster erstellen, wenn keine anderen ressourcenintensiven Aufgaben ausgeführt werden.</p> <p>Für lokale Exchange-Kunden sind die allgemeinen Aufgaben Sicherungslösungen. Weitere Informationen finden Sie unter <a href="#">Wartung des Exchange-Informationsspeichers</a>.</p>
Einschränkungsrichtlinie	<p>Es ist allgemein üblich, E-Mail-Systeme mit einer Einschränkungsrichtlinie zu schützen, die einen bestimmten Grenzwert festlegt, wie schnell und wie viele Daten während einer bestimmten Zeitspanne und mithilfe einer bestimmten Migrationsmethode aus dem System extrahiert werden können.</p>	<p>Überprüfen Sie, welche Einschränkungsrichtlinie auf Ihr E-Mail-System angewendet wird. Google Mail beschränkt z. B. die Datenmenge, die in einem bestimmten Zeitraum extrahiert werden kann.</p> <p>Je nach Version weist Exchange Richtlinien auf, die den IMAP-Zugriff auf den lokalen E-Mail-Server (verwendet von IMAP-Migrationen) und den RPC-über-HTTP-Protokollzugriff (verwendet von Exchange-Übernahmemigrationen und mehrstufigen Exchange-Migrationen) einschränkt.</p> <p>Weitere Informationen zur IMAP-Einschränkung finden Sie unter <a href="#">Tipps zum Optimieren von IMAP-Migrationen</a>.</p> <p>Weitere Informationen zur Einschränkung des RPC-über-HTTP-Protokolls finden Sie unter:</p> <ul style="list-style-type: none"> <li>• <a href="#">Exchange 2013-Arbeitsauslastungsverwaltung</a></li> <li>• <a href="#">Exchange 2010: Grundlegendes zu Clienteinschränkung Richtlinien</a></li> <li>• <a href="#">Exchange 2007: Grundlegendes zu Clienteinschränkung</a></li> </ul> <p>Weitere Informationen zum Konfigurieren der Einschränkung von Exchange-Webdiensten finden Sie unter <a href="#">Exchange 2010: Informationen zu Richtlinien zur Clienteinschränkung</a>.</p>

## Faktor 2: Migrationsserver

Die meisten Drittanbietertools für Office 365-Migrationen werden vom Client initiiert und verschieben Daten zu Office 365. Diese Tools erfordern in der Regel einen Migrationsserver. Für diese Migrationsserver gelten Faktoren wie Systemleistung, Back-End-Aufgaben und Einschränkungsrichtlinien für die Quellserver.

#### **NOTE**

Einige Migrationslösungen von Drittanbietern werden im Internet als cloudbasierte Dienste gehostet und erfordern keinen lokalen Migrationsserver.

## **Lösung und Übungsbeispiel**

Um die Migrationsleistung bei der Verwendung eines Migrationsservers zu verbessern, wenden Sie dieselben bewährten Methoden an, die auch im Abschnitt [Faktor 1: Datenquelle](#) beschrieben werden.

### **Faktor 3: Migrationsmodul**

Für Migrationstools von Drittanbietern werden am häufigsten die Exchange-Webdienste und das RPC-über-HTTP-Protokoll verwendet.

#### **Exchange-Webdienste**

Exchange-Webdienste ist das empfohlene Protokoll zum Migrieren zu Office 365, da große Datenbatches unterstützt werden und eine bessere dienstorientierte Einschränkung verfügbar ist. In Office 365 (im Identitätswechselmodus) verbrauchen Migrationen, die Exchange-Webdienste verwenden, nicht die veranschlagte Menge an Office 365 Exchange-Webdienstressressourcen, sondern stattdessen eine Kopie der veranschlagten Ressourcen:

- Alle Identitätswechselaufrufe der Exchange-Webdienste, die über dasselbe Administratorkonto getätigter werden, werden separat vom Budget berechnet, das diesem Administratorkonto zugewiesen ist.
- Für jede Identitätswechselsitzung wird eine Schattenkopie des Budgets des tatsächlichen Benutzers erstellt. Alle Migration für diese bestimmte Sitzung verwenden diese Schattenkopie.
- Die Einschränkung bei einem Identitätswechsel ist auf die einzelne Benutzermigrationssitzung begrenzt.

#### **Bewährte Methoden**

- Die Migrationsleistung für Kunden, die Migrationstools von Drittanbietern mit EWA-Identitätswechsel verwenden, konkurriert mit auf Exchange-Webdiensten basierenden Migrationen und der Dienstresssourcennutzung durch andere Mandanten. Daher variiert die Migrationsleistung.
- Kunden sollten nach Möglichkeit Migrationstools von Drittanbietern verwenden, die den Identitätswechsel mit Exchange-Webdiensten verwenden, da diese in der Regel schneller und effizienter sind als die Verwendung von Clientprotokollen, z. B. als das RPC-über-HTTP-Protokoll.

#### **RPC-über-HTTP-Protokoll**

Viele herkömmliche Migrationslösungen verwenden das RPC-über-HTTP-Protokoll. Diese Methode basiert vollständig auf einem Clientzugriffsmodell, z. B. auf dem von Outlook. Skalierbarkeit und Leistung sind beschränkt, da der Office 365-Dienst den Zugriff unter der Annahme einschränkt, dass die Nutzung durch einen Benutzer und nicht durch eine Anwendung erfolgt.

#### **Bewährte Methoden**

- Für Migrationstools, die das RPC-über-HTTP-Protokoll verwenden, ist es üblich, den Migrationsdurchsatz durch Hinzufügen weiterer Migrationsserver und Verwenden mehrerer administrativer Office 365-Benutzerkonten zu erhöhen. Diese Methode kann die Parallelität bei der Dateneinspeisung und einen höheren Datendurchsatz erreichen, da jeder administrative Benutzer der Office 365-Benutzereinschränkung unterliegt. Es liegen entsprechende Berichte vor, dass viele Unternehmenskunden mehr als 40 Migrationsserver einrichten mussten, um einen Migrationsdurchsatz von 20 bis 30 GB pro Stunde zu erreichen.
- In der Entwicklungsphase eines Migrationstools ist es wichtig, die Anzahl der RPC-Vorgänge zu

berücksichtigen, die zum Migrieren einer Nachricht erforderlich sind. Zur Veranschaulichung haben wir die von Office 365-Diensten erfassten Protokolle für zwei Migrationslösungen von Drittanbietern (von Drittanbietern entwickelt) gesammelt, die von Kunden zum Migrieren von Postfächern zu Office 365 verwendet wurden. Wir haben zwei von Drittanbietern entwickelte Migrationslösungen verglichen. Es wurde die Migration von zwei Postfächern für die jeweilige Migrationslösung verglichen. Diese Migrationslösungen wurden ebenfalls mit dem Hochladen einer PST-Datei in Outlook verglichen. Hier folgen die Ergebnisse.

METHODE	POSTFACHGRÖSSE	ELEMENTANZAHL	MIGRATIONSSZEIT	GESAMTE RPC-TRANSAKTIONEN	DURCHSCHNITTLCHE CLIENTWARTEZEIT (MS)	AVGCASRPCPROCESSINGTIME (MS)
Lösung A (Postfach 1)	376,9 MB	4.115	4:24:33	132.040	48.4395	18.0807
Lösung A (Postfach 2)	249,3 MB	12.779	10:50:50	423.188	44.1678	4.8444
Lösung B (Postfach 1)	618,1 MB	4.322	1:54:58	12.196	37.2931	8.3441
Lösung B (Postfach 2)	56,7 MB	2.748	0:47:08	5.806	42.1930	7.4439
Outlook	201,9 MB	3.297	0:29:47	15.775	36.9987	5.6447

Beachten Sie, dass die Client und Dienst Bearbeitungszeiten ähneln Lösung A dauert wesentlich mehr RPC-Vorgänge zum Migrieren von Daten. Da jede Operation Wartezeit auf dem Client und Server-Bearbeitungszeit beansprucht, ist Lösung A niedriger die gleiche Datenmenge im Vergleich zu Lösung B und Outlook migrieren.

#### Faktor 4: Netzwerk

##### Bewährte Methode

Für die Migrationslösungen von Drittanbietern, die das RPC-über-HTTP-Protokoll verwenden, folgt hier eine geeignete Möglichkeit zum Messen der potenziellen Migrationsleistung:

1. Stellen Sie über den Migrationsserver eine Verbindung mit dem Office 365-Postfach mit Outlook über das RPC-über-HTTP-Protokoll her. Stellen Sie sicher, dass Sie die Verbindung nicht im [Cachemodus](#) herstellen.
2. Importieren Sie eine großen PST-Datei mit Beispieldaten in das Office 365-Postfach.
3. Messen Sie die Migrationsleistung, indem Sie die Zeit für das Hochladen der PST-Datei nehmen. Der Migrationsdurchsatz sollte dem ähneln, den Kunden über ein Migrationstool von Drittanbietern erzielen können, das das RPC-über-HTTP-Protokoll verwendet, vorausgesetzt, es gibt keine weiteren Einschränkungen. Während einer tatsächlichen Migration kommt es zu einem Mehraufwand, daher kann der Durchsatz leicht abweichen.

#### Faktor 5: Office 365-Dienst

Die auf dem Ressourcenstatus von Office 365 basierende Einschränkung wirkt sich auf Migrationen aus, die Migrationstools von Drittanbietern verwenden. Weitere Informationen finden Sie unter [Auf dem Office 365-Ressourcenstatus basierende Einschränkung](#).

# Zuweisen von Exchange-Berechtigungen zum Migrieren von Postfächern zu Office 365

18.12.2018 • 10 minutes to read

Beim Migrieren lokaler Exchange-Postfächer zu Office 365 sind bestimmte Berechtigungen erforderlich, um auf diese Postfächer zuzugreifen und sie ggf. zu ändern. Das Benutzerkonto, das während der Migration zum Herstellen einer Verbindung mit der lokalen Exchange-Organisation verwendet wird, benötigt diese Berechtigungen. Das Benutzerkonto, das als Migrationsadministratorkonto bezeichnet wird, dient zum Erstellen eines Migrationsendpunkts zu Ihrer lokalen Organisation.

Der Migrationsadministrator muss über die erforderlichen Administratorrechte in Ihrer lokalen Exchange-Organisation verfügen, um erfolgreich einen Migrationsendpunkt erstellen zu können. Dieselben Administratorrechte sind erforderlich, wenn der Migrationsadministrator einen Migrationsbatch erstellen möchte, falls Ihre Organisation keine Migrationsendpunkte aufweist. Die folgende Liste zeigt die Administratorrechte, die für das Migrationsadministratorkonto erforderlich sind, um Postfächer mithilfe der verschiedenen Migrationsmethoden zu Office 365 zu migrieren:

## • Mehrstufige Exchange-Migration

Für eine mehrstufige Migration muss das Migrationsadministratorkonto folgende Voraussetzungen erfüllen:

- Es muss Mitglied der Gruppe der Domänenadministratoren in Active Directory Domain Services (AD DS) in der lokalen Organisation sein.

oder
- Zugewiesene Berechtigung FullAccess für jedes Postfach und die WriteProperty lokale-Berechtigungen zum Ändern der Eigenschaft *TargetAddress* des lokalen Benutzerkontos.

oder
- Die Berechtigung Receive As für die lokale Postfachdatenbank, die die Benutzerpostfächer und die WriteProperty speichert zugewiesen über Berechtigungen zum Ändern der Eigenschaft *TargetAddress* des lokalen Benutzerkontos.

## • Exchange-Übernahmemigration

Für eine Übernahmemigration muss das Migrationsadministratorkonto folgende Voraussetzungen erfüllen:

- Es muss Mitglied der Gruppe der Domänenadministratoren in Active Directory Domain Services (AD DS) in der lokalen Organisation sein.

oder
- Ihm muss die Berechtigung "FullAccess" für jedes lokale Postfach zugewiesen sein.

oder
- Ihm muss die Berechtigung "Receive As" für die lokale Postfachdatenbank zugeordnet sein, in der die Benutzerpostfächer gespeichert werden.

## • IMAP4 (Internet Message Access Protocol 4)-Migration

Für eine IMAP4-Migration muss die Datei mit durch Kommas getrennten Werten (CSV) für den Migrationsbatch Folgendes enthalten:

- Benutzername und Kennwort für jedes Postfach, das Sie migrieren möchten.  
oder
- Benutzername und Kennwort für ein Konto in Ihrem IMAP4 messaging-System, das über Administratorrechte für den Zugriff alle Benutzerpostfächer auf verfügt. Um zu erfahren, ob der IMAP4-Server unterstützt, diese Vorgehensweise und zum Aktivieren, finden Sie unter Dokumentation für IMAP4-Server.

Exchange Online PowerShell können in Ihrer lokalen Organisation Sie die erforderlichen Berechtigungen zum Migrieren von Postfächern zu Office 365 schnell zuweisen.

#### **NOTE**

Da Exchange Online PowerShell von Exchange Server 2003 nicht unterstützt wird, müssen Sie Active Directory-Benutzer und-Computer verwenden, um die FullAccess zuzuweisen Berechtigung und Exchange Server-Manager die Berechtigung Receive As zuweisen. Weitere Informationen finden Sie unter [wie zuweisen-Dienstkonto den Zugriff auf alle Postfächer in Exchange Server 2003](#).

Informationen zum Migrieren von Postfächern zu Office 365 mithilfe von unterschiedlichen Migrationstypen, finden Sie unter [Möglichkeiten, um mehrere e-Mail-Konten zu Office 365 zu migrieren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Die geschätzte Zeit zum Ausführen der einzelnen Verfahren beträgt 2 Minuten.
- Ihnen müssen Berechtigungen zugewiesen werden, bevor Sie diese Verfahren ausführen können. Informationen zu den benötigten Berechtigungen finden Sie unter dem Thema [Empfängerberechtigungen](#) im Abschnitt "Empfängerbreitstellungsberechtigungen" im Eintrag "Berechtigungen und Delegierung".

## Was möchten Sie tun?

### **Zuweisen der Berechtigung "FullAccess"**

Die folgenden Beispiele zeigen unterschiedliche Möglichkeiten zum Verwenden des Exchange Online PowerShell-**Add-MailboxPermission** -Cmdlets zum migrationsadministratorkonto für Postfächer in Ihrer lokalen Organisation die Berechtigung FullAccess zuweisen.

#### **Beispiel 1**

Die Berechtigung "FullAccess" für das Postfach von Terry Adams wird dem Migrationsadministratorkonto zugewiesen (z. B. "migadmin").

```
Add-MailboxPermission -Identity "Terry Adams" -User migadmin -AccessRights FullAccess -InheritanceType all
```

#### **Beispiel 2**

Die Berechtigung "FullAccess" für alle Mitglieder der Verteilergruppe "MigrationBatch1" wird dem Migrationsadministratorkonto zugewiesen.

```
Get-DistributionGroupMember MigrationBatch1 | Add-MailboxPermission -User migadmin -AccessRights FullAccess -InheritanceType all
```

### Beispiel 3

Berechtigung FullAccess für alle Postfächer mit dem Wert der `MigBatch2` für `CustomAttribute10` dem migrationsadministrator zugewiesen ist.

```
Get-Mailbox -ResultSize unlimited -Filter {((CustomAttribute10 -eq 'MigBatch2'))} | Add-MailboxPermission -User migadmin -AccessRights FullAccess -InheritanceType all
```

### Beispiel 4

Die Berechtigung "FullAccess" für alle Benutzerpostfächer in der lokalen Organisation wird dem Migrationsadministratorkonto zugewiesen.

```
Get-Mailbox -ResultSize unlimited -Filter {((RecipientTypeDetails -eq 'UserMailbox'))} | Add-MailboxPermission -User migadmin -AccessRights FullAccess -InheritanceType all
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter den folgenden Themen:

- [Add-MailboxPermission](#)
- [Filterbare Eigenschaften für den Parameter "-Filter"](#)

**Wie können Sie feststellen, ob die Zuweisung der Berechtigung erfolgreich war?**

Führen Sie einen der folgenden Befehle aus, um zu überprüfen, ob Sie dem Migrationsadministratorkonto die Berechtigung "FullAccess" im jeweiligen Beispiel erfolgreich zugewiesen haben.

```
Get-MailboxPermission -Identity <mailbox> -User migadmin
```

```
Get-DistributionGroupMember MigrationBatch1 | Get-MailboxPermission -User migadmin
```

```
Get-Mailbox -ResultSize unlimited -Filter {((CustomAttribute10 -eq 'MigBatch2'))} | Get-MailboxPermission -User migadmin
```

```
Get-Mailbox -ResultSize unlimited -Filter {((RecipientTypeDetails -eq 'UserMailbox'))} | Get-MailboxPermission -User migadmin
```

### Zuweisen der Berechtigung "Receive As"

Das folgende Beispiel zeigt, wie Sie das Exchange Online PowerShell- **Add-ADPermission** -Cmdlet verwenden, um das Administratorkonto für die Migration zu "Postfachdatenbank 1900992314" die Berechtigung Receive As zuweisen

```
Add-ADPermission -Identity "Mailbox Database 1900992314" -User migadmin -ExtendedRights receive-as
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Add-ADPermission](#).

**Wie können Sie feststellen, ob die Zuweisung der Berechtigung erfolgreich war?**

Überprüfen Sie, ob Sie dem Migrationsadministratorkonto die Berechtigung "Receive As" im Beispiel erfolgreich zugewiesen haben. Führen Sie den folgenden Befehl aus.

```
Get-ADPermission -Identity "Mailbox Database 1900992314" -User migadmin
```

## Zuweisen der Berechtigung "WriteProperty"

Die folgenden Beispiele zeigen verschiedene Arten auf das Exchange Online PowerShell- **Add-ADPermission** - Cmdlet verwenden, um das Administratorkonto für die Migration die Berechtigung WriteProperty zum Ändern der Eigenschaft *TargetAddress* für lokale Benutzer zuweisen Konten. Diese Funktion ist eine mehrstufige Exchange-Migration ausführen, wenn dem migrationsadministrator ein Mitglied der Gruppe Domänen-Admins ist nicht erforderlich.

### Beispiel 1

WriteProperty Berechtigung zum Ändern der *TargetAddress* -Eigenschaft für das Benutzerkonto des Rainer Witte wird das migrationsadministratorkonto ein (beispielsweise Migadmin) zugewiesen.

```
Add-ADPermission -Identity "Rainer Witte" -User migadmin -AccessRights WriteProperty -Properties TargetAddress
```

### Beispiel 2

WriteProperty Berechtigung zum Ändern der Eigenschaft *TargetAddress* für alle Mitglieder der Verteilergruppe stagedbatch1 angezeigt wird das Administratorkonto für die Migration zugewiesen.

```
Get-DistributionGroupMember StagedBatch1 | Add-ADPermission User migadmin -AccessRights WriteProperty -Properties TargetAddress
```

### Beispiel 3

Berechtigung zum Ändern der Eigenschaft *TargetAddress* für alle Benutzerkonten mit dem Wert der WriteProperty `StagedMigration` für das migrationsadministratorkonto ein *CustomAttribute15* zugewiesen ist.

```
Get-User -ResultSize unlimited -Filter {((CustomAttribute15 -eq 'StagedMigration'))} | Add-ADPermission -User migadmin -AccessRights WriteProperty -Properties TargetAddress
```

### Beispiel 4

Administratorkonto für die Migration wird die Berechtigung WriteProperty so ändern Sie die Eigenschaft *TargetAddress* für Benutzerpostfächer in der lokalen Organisation zugewiesen.

```
Get-User -ResultSize unlimited -Filter {((RecipientTypeDetails -eq 'UserMailbox'))} | Add-ADPermission -User migadmin -AccessRights WriteProperty -Properties TargetAddress
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter den folgenden Themen:

- [Add-ADPermission](#)
- [Filterbare Eigenschaften für den Parameter "-Filter"](#)

#### Wie können Sie feststellen, ob die Zuweisung der Berechtigung erfolgreich war?

Überprüfen Sie, ob Sie dem Administratorkonto die Berechtigung "WriteProperty" erfolgreich zugewiesen haben. Führen Sie einen der folgenden Befehle aus, um zu bestätigen, dass die Berechtigung zum Ändern der Eigenschaft "TargetAddress" mithilfe des Befehls im jeweiligen Beispiel erteilt wurde.

```
Get-ADPermission -Identity <mailbox> -User migadmin
```

```
Get-DistributionGroupMember MigrationBatch1 | Get-ADPermission -User migadmin
```

```
Get-Mailbox -ResultSize unlimited -Filter {(CustomAttribute15 -eq 'StagedMigration')} | Get-MailboxPermission  
-User migadmin
```

```
Get-Mailbox -ResultSize unlimited -Filter {(RecipientTypeDetails -eq 'UserMailbox')} | Get-ADPermission -User  
migadmin
```

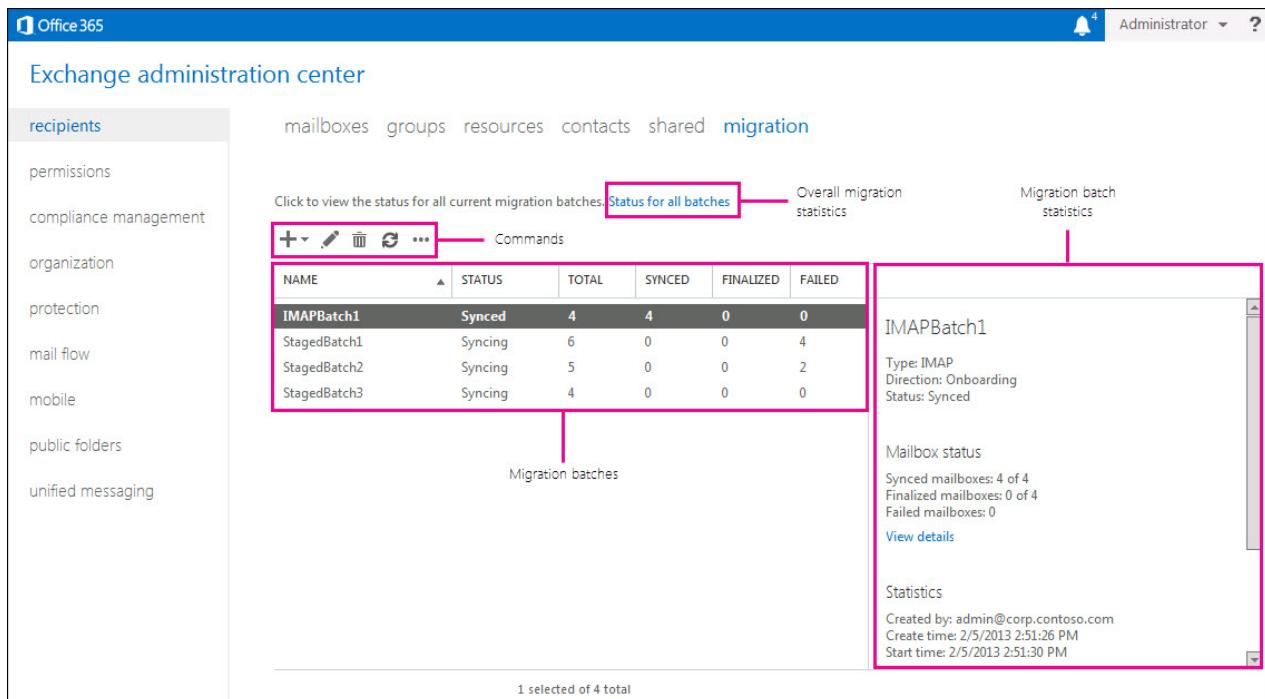
# Verwalten von Migrationsbatches in Office 365

18.12.2018 • 14 minutes to read

Im Office 365 Exchange Admin Center (EAC) können Sie mithilfe des Migrationsdashboards die Postfachmigration zu Office 365 verwalten. Sie können dazu eine Exchange-Übernahmemigration oder eine mehrstufige Exchange-Migration verwenden. Sie können das Migrationsdashboard auch verwenden, um die Inhalte von Benutzerpostfächern von einem lokalen IMAP-Server zu vorhandenen Office 365-Postfächern zu migrieren. Im Migrationsdashboard werden Statistiken zur Gesamtmigration und Statistiken zu einem bestimmten Migrationsbatch angezeigt. Sie können Migrationsbatches erstellen, starten, beenden, anhalten und bearbeiten.

## Migrationsdashboard

Um im EAC auf das Migrationsdashboard zuzugreifen, wählen Sie **Empfänger > Migration** aus. Im folgenden Screenshot sind die verschiedenen Bereiche des Migrationsdashboards dargestellt, in denen Sie Migrationsinformationen abrufen und Migrationsbatches verwalten können.



The screenshot shows the Exchange administration center interface. On the left, there's a navigation menu with links like recipients, mailboxes, groups, resources, contacts, shared, and migration. The migration link is highlighted. In the center, there's a table titled "Migration batches" with columns: NAME, STATUS, TOTAL, SYNCED, FINALIZED, and FAILED. The table contains four rows: IMAPBatch1 (Synced, 4, 4, 0, 0), StagedBatch1 (Syncing, 6, 0, 0, 4), StagedBatch2 (Syncing, 5, 0, 0, 2), and StagedBatch3 (Syncing, 4, 0, 0, 0). Above the table, there's a button labeled "Status for all batches". To the right of the table, there's a detailed view for "IMAPBatch1" which includes its type (IMAP), direction (Onboarding), and status (Synced). It also shows mailbox statistics (Synced mailboxes: 4 of 4, Failed mailboxes: 0) and migration details (Created by: admin@corp.contoso.com, Create time: 2/5/2013 2:51:26 PM, Start time: 2/5/2013 2:51:30 PM).

### Statistiken zur Gesamtmigration

Klicken Sie auf **Status für alle Batches**, um die allgemeinen Statistiken zu allen erstellten Migrationsbatches anzuzeigen. In den folgenden Feldern werden kumulierte Informationen zu allen Migrationsbatches angezeigt.

FELD	BESCHREIBUNG
<b>Postfächer gesamt</b>	Die Gesamtanzahl von Postfächern aus allen aktuellen Migrationsbatches.
<b>Synchronisierte Postfächer</b>	Die Anzahl von Postfächern aus allen Migrationsbatches, die erfolgreich migriert wurden.

FELD	BESCHREIBUNG
<b>Abgeschlossene Postfächer</b>	Die Anzahl von Postfächern aus allen Migrationsbatches, die abgeschlossen wurden. Ein Abschluss erfolgt nur dann, wenn zur Migration von Postfächern zwischen Ihrer lokalen Exchange-Organisation und Office 365 in einer Exchange-Hybridbereitstellung Remoteverschiebungsmigrationen verwendet werden. Postfächer können abgeschlossen werden, nachdem die Erstsynchronisierung erfolgreich abgeschlossen wurde. Weitere Informationen zum Abschluss in Remoteverschiebungsmigrationen finden Sie unter <a href="#">Complete-MigrationBatch</a> .
<b>Postfächer mit Fehlern</b>	Die Anzahl von Postfächern aus allen Migrationsbatches, bei deren Migration ein Fehler aufgetreten ist.

## Migrationsbatches

Die erstellten Migrationsbatches werden in der Migrationswarteschlange aufgelistet. In den folgenden Spalten werden Informationen zu jedem Migrationsbatch angezeigt.

SPALTE	BESCHREIBUNG
<b>Name</b>	Der Name des Migrationsbatches, der beim Erstellen des Migrationsbatches definiert wurde.

SPALTE	BESCHREIBUNG
<b>Status</b>	<p>Der Status des Migrationsbatches. Im Folgenden finden Sie eine Liste mit den unterschiedlichen Statuszuständen von Migrationsbatches sowie Informationen darüber, welche Möglichkeiten Sie bei den einzelnen Statuszuständen der Migrationsbatches haben.</p> <p><b>Beendet:</b> der migrationsbatch erstellt wurde, aber es wurde nicht gestartet. In diesem Status können Sie starten, bearbeiten oder löschen Sie ihn.</p> <p><b>Synchronisiert:</b> der migrationsbatch gestartet wurde, und Postfächer im migrationsbatch aktiv migriert werden. Wenn Sie ein migrationsbatch in diesem Status ist, können Sie ihn stoppen.</p> <p><b>Wird beendet:</b> Unmittelbar nach dem Ausführen des <a href="#">Stop-MigrationBatch</a>-Cmdlets.</p> <p><b>Beendet:</b> der migrationsbatch beendet ist und keine weitere Postfächer aus den Batch migriert werden. Wenn Sie ein migrationsbatch in diesem Status ist, können Sie ihn neu starten.</p> <p><b>Wird gestartet:</b> Unmittelbar nach dem Ausführen des <a href="#">Start-MigrationBatch</a>-Cmdlets.</p> <p><b>Wird abgeschlossen:</b> Unmittelbar nach dem Ausführen des <a href="#">Complete-MigrationBatch</a>-Cmdlets.</p> <p><b>Wird entfernt:</b> Unmittelbar nach dem Ausführen des <a href="#">Remove-MigrationBatch</a>-Cmdlets.</p> <p><b>Synchronisiert:</b> der migrationsbatch abgeschlossen ist, und keine Postfächer aktiv migriert werden. In diesem Status ein migrationsbatches kann Fehler enthalten, wenn Postfächer migriert wurden nicht. Exchange-übernahmemigrationen und IMAP-Migrationen mit diesem Status in der lokalen und der entsprechenden Office 365 Postfächer alle 24 Stunden während der inkrementellen Synchronisierung synchronisiert werden.</p> <p><b>Abgeschlossen:</b> Der Migrationsbatch ist abgeschlossen.</p> <p><b>Synchronisiert mit Fehlern:</b> der migrationsbatch abgeschlossen ist, aber einige Postfächer Fehler bei Migration. Postfächer, die in migrationsbatches mit Fehlern erfolgreich migriert wurden, werden weiterhin alle 24 Stunden während der inkrementellen Synchronisierung synchronisiert.</p>
<b>Gesamt</b>	Gibt die Anzahl von Postfächern im Migrationsbatch an.
<b>Synchronisiert</b>	Gibt die Anzahl von Postfächern an, die erfolgreich migriert wurden.
<b>Abgeschlossen</b>	Die Anzahl von Postfächern im Migrationsbatch, die abgeschlossen wurden. Der Abschluss wird nur für Migrationsbatches bei Remoteverschiebungsmigrationen in einer Exchange-Hybridbereitstellung durchgeführt. Weitere Informationen zum Abschlussvorgang finden Sie unter <a href="#">Complete-MigrationBatch</a> .
<b>Fehler</b>	Die Anzahl von Postfächern im Migrationsbatch, bei deren Migration ein Fehler aufgetreten ist. Sie können Informationen zu bestimmten Postfächern anzeigen, die Migrationsfehler aufweisen. Weitere Informationen finden Sie unter <a href="#">Statusbericht für Migrationsbenutzer</a> .

## IMPORTANT

Migrationsbatches mit dem Status **Synchronisiert**, für die in den letzten 90 Tagen keine vom Administrator initiierte Aktivität vorliegt (beispielsweise wurde kein Migrationsbatch von einem Administrator beendet und neu gestartet oder bearbeitet), werden beendet und dann 30 Tage später gelöscht, wenn vom Administrator keine weitere Aktion ausgeführt wird.

Das Migrationsdashboard enthält eine Reihe von Befehlen zum Verwalten von Migrationsbatches. Nach dem Erstellen eines Migrationsbatches können Sie ihn auswählen und dann auf einen der folgenden Befehle klicken. Befindet sich ein Migrationsbatch in einem Statuszustand, der von einem Befehl nicht unterstützt wird, ist der Befehl nicht verfügbar und wird daher abgeblendet oder nicht angezeigt.

BEFEHL	BESCHREIBUNG
<b>Neue +</b>	Erstellt einen neuen Migrationsbatch. Mit diesem Befehl können Sie lokale Postfächer zu Office 365 migrieren (auch Onboarding genannt) oder Office 365-Postfächer zurück zu Ihrer lokalen Exchange-Organisation in einer Hybridbereitstellung migrieren.
<b>Bearbeiten ↎</b>	Bearbeitet einen vorhandenen Migrationsbatch. Bei mehrstufigen Exchange-Migrationen und IMAP-Migrationen können Sie eine andere CSV-Datei übermitteln. Zudem können Sie den für den Migrationsbatch verwendeten Migrationsendpunkt ändern. Sie können nur einen Migrationsbatch mit dem Status <b>Erstellt</b> bearbeiten.
<b>Starten ►</b>	Startet einen Migrationsbatch, der erstellt wurde. Nachdem der Batch gestartet wurde, wird der Status in <b>Synchronisierung</b> geändert.
<b>Fortsetzen ►</b>	Setzt die Ausführung eines Migrationsbatches fort, der angehalten wurde und den Status <b>Beendet</b> aufweist. Wenn bei einem Migrationsbatch Fehler aufgetreten sind, können Sie ihn mithilfe dieses Befehls neu starten. Office 365 versucht dann, die Postfächer zu migrieren, bei denen Fehler aufgetreten sind.
<b>Anhalten ■</b>	Beendet einen Migrationsbatch, der derzeit ausgeführt wird oder gestartet wurde, allerdings den Status <b>In Warteschlange eingereiht</b> besitzt. Sie haben auch die Möglichkeit, einen Exchange-Übernahmemigrationsbatch oder einen IMAP-Migrationsbatch zu beenden, der die Initiierungssynchronisierungsphase abgeschlossen hat und den Status <b>Synchronisiert</b> aufweist. Inkrementelle Synchronisierungen werden dadurch beendet. Sie können inkrementelle Synchronisierungen fortsetzen, indem Sie den Migrationsbatch auswählen und auf <b>Fortsetzen</b> klicken.
<b>Löschen ━</b>	Löscht einen Migrationsbatch, nachdem Sie überprüft haben, ob alle Postfächer im Migrationsbatch erfolgreich migriert wurden und ob E-Mails direkt an cloudbasierte Postfächer weitergeleitet werden, nachdem Sie den MX-Eintrag so konfiguriert haben, dass er auf Office 365 verweist. Wenn Sie einen Migrationsbatch löschen, bereinigt Office 365 alle zum Migrationsbatch gehörenden Einträge und entfernt den Batch aus der Liste.

BEFEHL	BESCHREIBUNG
<b>Weitere ...</b>	Klicken Sie auf diesen Befehl und anschließend auf <b>Migrationsendpunkte</b> , um neue Migrationsendpunkte zu erstellen oder vorhandene Migrationsendpunkte anzuzeigen und zu bearbeiten.
<b>Aktualisieren</b> 	Aktualisiert das Migrationsdashboard, um die Informationen zu den Gesamt migrationsstatistiken, zur Liste der Migrationsbatches und zu den Statistiken zum ausgewählten Migrationsbatch zu aktualisieren.

## Statistiken zum Migrationsbatch

Im Detailbereich des Migrationsdashboards werden die folgenden Informationen zum ausgewählten Migrationsbatch angezeigt.

FELD	BESCHREIBUNG
<b>Typ</b>	Gibt den Migrationstyp des ausgewählten Migrationsbatches an. Der Wert dieses Felds gibt zudem den Typ des Migrationsendpunkts an, der dem Migrationsbatch zugeordnet wurde. <b>Exchange Outlook Anywhere:</b> der migrationsbatch ist entweder eine Exchange-übernahmemigration oder eine mehrstufige Exchange-Migration. <b>IMAP:</b> der migrationsbatch ist eine IMAP-Migration. <b>Remoteverschiebungsmigration:</b> der migrationsbatch ist entweder eine Onboarding- oder eine Offboarding remoteverschiebungsmigration in einer Exchange-hybridbereitstellung.
<b>Richtung</b>	Gibt an, ob Postfächer zu Office 365 oder zu Ihrer lokalen Exchange-Organisation migriert werden. <b>Onboarding:</b> Gibt an, dass Postfächer zu Office 365 migriert werden. Onboarding Migrationstypen sind mehrstufige Migrationen, Einstufige Migrationen, IMAP-Migrationen und remoteverschiebungsmigrationen Onboarding. <b>Offboarding:</b> Gibt an, dass Office 365-Postfächer zu Ihrer lokalen Exchange-Organisation migriert werden. Offboarding-remoteverschiebungsmigrationen sind die einzige Art von Migration Offboarding.
<b>Status</b>	Der aktuelle Zustand des ausgewählten Migrationsbatches. <b>Beendet</b> <b>Wird synchronisiert</b> <b>Beendet</b> <b>Synchronisiert</b> <b>Synchronisiert mit Fehlern</b> Siehe vorherige Beschreibung zu jedem dieser Zustände.
<b>Angefordert</b>	Die Anzahl der zu migrierenden Postfächer im Migrationsbatch. Diese Anzahl entspricht der Anzahl von Zeilen in der CSV-Migrationsdatei für IMAP-Migrationen, mehrstufige Migrationen oder Remoteverschiebungsmigrationen oder der Anzahl von lokalen Postfächern in einer Exchange-Übernahmemigration.

FELD	BESCHREIBUNG
<b>Synchronisierte Postfächer</b>	Der Anteil an der Gesamtanzahl von Postfächern im Migrationsbatch, bei denen die Erstsynchronisierung erfolgreich abgeschlossen wurde. Dieses Feld wird während der Migration aktualisiert.
<b>Abgeschlossen</b>	Der Anteil an der Gesamtanzahl von Postfächern im Migrationsbatch, die erfolgreich abgeschlossen wurden. Ein Abschluss erfolgt nur in Onboarding- und Offboarding-Remoteverschiebungsmigrationen.
<b>Postfächer mit Fehlern</b>	Die Anzahl von Postfächern, bei deren Erstsynchronisierung ein Fehler aufgetreten ist.
<b>Details anzeigen</b>	Klicken Sie auf <b>Details anzeigen</b> , um Statusinformationen zu den einzelnen Postfächern im Migrationsbatch anzuzeigen. Weitere Informationen finden Sie unter <a href="#">Statusbericht für Migrationsbenutzer</a> .
<b>Erstellt von</b>	Die E-Mail-Adresse des Office 365-Administrators, der den Migrationsbatch erstellt hat.
<b>Erstellungszeit</b>	Datum und Uhrzeit der Erstellung des Migrationsbatches.
<b>Startzeit</b>	Datum und Uhrzeit des Starts des Migrationsbatches.
<b>Zeitpunkt der Erstsynchronisierung</b>	Datum und Uhrzeit, zu denen die Erstsynchronisierung des Migrationsbatches abgeschlossen war.
<b>Dauer der Erstsynchronisierung</b>	Die zum Abschließen der Erstsynchronisierung für alle Postfächer im Migrationsbatch benötigte Zeit.
<b>Letzte Synchronisierungszeit</b>	Der Zeitpunkt, zu dem der Migrationsbatch zuletzt neu gestartet wurde oder zu dem die inkrementelle Synchronisierung für den Batch zuletzt durchgeführt wurde. Wie bereits erwähnt, erfolgt die inkrementelle Synchronisierung für IMAP-Migrationen und Exchange-Übernahmemigrationen alle 24 Stunden.
<b>Zugeordneter Endpunkt</b>	Der Name des Migrationsendpunkts, der vom Migrationsbatch verwendet wird. Klicken Sie auf <b>Details anzeigen</b> , um die Einstellungen des Migrationsendpunkts anzuzeigen. Sie können die Einstellungen auch bearbeiten, wenn aktuell kein Migrationsbatch ausgeführt wird, der diesen Endpunkt verwendet.

# Statusbericht für Migrationsbenutzer

18.12.2018 • 9 minutes to read

■ Sie können das Migrationsdashboard im Exchange Admin Center (EAC) verwenden, um die Migrationsstatusinformationen für alle Benutzer in einem Migrationsbatch anzuzeigen. Sie können auch detaillierte Migrationsinformationen für jeden Benutzer in einem Migrationsbatch anzeigen. Mithilfe dieser Informationen, auch als Migrationsbenutzerstatistiken bezeichnet, können Sie Probleme beheben, die die Migration des Postfachs oder der Postfachelemente eines Benutzers verhindern. Sie können diese Migrationsstatusinformationen für Migrationsbatches anzeigen, die gegenwärtig ausgeführt werden, die beendet wurden oder die abgeschlossen sind.

Exchange Online PowerShell können auch migrationsbenutzerstatistiken anzuzeigen. Weitere Informationen finden Sie unter:

- [Get-MigrationUser](#)
- [Get-MigrationUserStatistics](#)

## Migrationsbenutzerbericht

Um auf den Migrationsbenutzerbericht für einen Migrationsbatch zuzugreifen, wählen Sie **Empfänger > Migration** und anschließend den Migrationsbatch aus. Klicken Sie dann im Detailbereich unter **Postfachstatus** auf **Details anzeigen**.

The screenshot shows the Exchange Admin Center interface. At the top, there's a navigation bar with 'IMAPBatch1' selected. Below it, a table lists migration users: danp@corp.contoso.com (Synced, 15 items), erik@corp.contoso.com (Synced, 15 items), tamaraj@corp.contoso.com (Synced, 15 items), and judyl@corp.contoso.com (Synced, 15 items). A tooltip 'Migration users in the migration batch' points to this table. A modal window titled 'Migration user statistics for selected user' is open over the table, showing details for 'danp@corp.contoso.com': Status: Synced, Skipped item details, Data migrated:, Migration rate:, Error:, Report: Download the report for this user, and Last successful sync date: 2/5/2013 2:55:10 PM. A tooltip '1 selected of 4 total' points to the bottom of the modal. In the background, another part of the interface shows migration batches: StagedBatch3, StagedBatch2, StagedBatch1, and IMAPBatch1 (Synced, 4 items). To the right, a detailed view of IMAPBatch1 is shown, including its type (IMAP), direction (Onboarding), status (Synced), mailbox status (Synced mailboxes: 4 of 4, Finalized mailboxes: 0 of 4, Failed mailboxes: 0), and statistics (Created by: admin@corp.contoso.com, Create time: 2/5/2013 2:51:26 PM, Start time: 2/5/2013 2:51:30 PM, Total item count: 383,012, 3,871,111 DTA).

Der Name des Migrationsbatches und die folgenden Befehle werden oben im Fenster angezeigt.

BEFEHL	BESCHREIBUNG
<b>Löschen</b> 	Löschen des ausgewählten Benutzers aus der Liste der Migrationsbenutzer.
<b>Aktualisieren</b> 	Aktualisieren der Liste der Migrationsbenutzer, um die für die Benutzer im Migrationsbatch angezeigten Informationen zu aktualisieren.

### Spalten in der Liste der Migrationsbenutzer

SPALTE	BESCHREIBUNG
<b>Identität</b>	Die E-Mail-Adresse des Benutzers.
<b>Status</b>	Der Migrationsstatus des Benutzers. Weitere Informationen finden Sie in den Statusbeschreibungen in der Tabelle im nächsten Abschnitt.
<b>Synchronisierte Elemente</b>	Die Anzahl der Elemente im lokalen Postfach des Benutzers, die erfolgreich zum Office 365-Postfach migriert wurden.
<b>Übersprungene Elemente</b>	Die Anzahl der Elemente im lokalen Postfach des Benutzers, die nicht zum Office 365-Postfach migriert wurden.

## Migrationsbenutzerstatistiken für einen bestimmten Benutzer

Zum Anzeigen von Statusinformationen (auch Migrationsbenutzerstatistiken genannt) für ein bestimmtes Postfach, einen bestimmten E-Mail-Kontakt oder eine bestimmte Verteilergruppe klicken Sie auf das Postfach, den Kontakt bzw. die Verteilergruppe in der Liste. Statusinformationen für das ausgewählte E-Mail-Objekt werden im Detailbereich angezeigt. In der folgenden Tabelle werden die einzelnen im Detailbereich angezeigten Felder beschrieben.

FELD	BESCHREIBUNG

FELD	BESCHREIBUNG
<b>Status</b>	<p>Identifiziert für jedes E-Mail-Objekt im Migrationsbatch den genauen Punkt im Migrationsprozess. Dieser Status ist spezifischer als die allgemeine Statuszusammenfassung, die in der Liste der Migrationsbenutzer angezeigt wird. In der folgenden Liste sind die einzelnen Status beschrieben.</p> <ul style="list-style-type: none"> <li>• <b>Warteschlange eingereiht:</b> das Objekt ist in einem migrationsbatch, der ausgeführt wird, aber die Migration des Objekts wurde noch nicht gestartet. Objekte weisen in der Regel einen Status <b>in Warteschlange eingereiht</b>, wenn alle Verbindungen in den migrationsendpunkt zugeordnet migrationsbatch verwendet werden.</li> <li>• <b>Provisioning:</b> der Migrationsprozess wurde für das e-Mail-Objekt gestartet, aber es noch nicht bereitgestellt.</li> <li>• <b>Bereitstellung Aktualisierung:</b> das e-Mail-Objekt verfügt, aber nicht alle Objekteigenschaften migriert wurden. Nach einer Verteilergruppe migriert wurde, tritt dieser Zustand beispielsweise wenn hatte keine Mitglieder der Gruppe noch migriert wurden, oder es ist ein Problem mit dem Migrieren von eines Benutzers ein Mitglied der Gruppe ist. In diesem Fall gibt den Status des Migrationsprozesses Mitglied der Gruppe Update ist nicht möglich, da nicht alle Mitglieder der Gruppe migriert wurden.</li> <li>• <b>Synchronisiert:</b> der Migrationsprozess erfolgreich bereitgestellte Office 365-Postfach und die erstsynchonisierung, in dem alle Postfachelemente in das Cloud-basierte Postfach kopiert wurden. Für Exchange-übernahmemigrationen und IMAP-Migrationen kann dieser Status wird auch, dass die inkrementelle Synchronisierung erfolgreich abgeschlossen angeben.</li> <li>• <b>Fehler:</b> Fehler bei der Bereitstellung oder der ersten Synchronisierung des e-Mail-Objekts. Wenn ein Office 365-Postfach wurde erfolgreich für einen Benutzer erstellt, aber die Migration der Postfachelemente fehlschlägt, wird der Status für den Benutzer <b>fehlgeschlagen</b>.</li> </ul>
<b>Details zu übersprungenen Elementen</b>	<p>Klicken Sie auf <b>Details zu übersprungenen Elementen</b>, um Informationen zu jedem Element anzuzeigen, das für den ausgewählten Benutzer übersprungen wurde. Es werden die folgenden Informationen zu jedem übersprungenen Element angezeigt:</p> <ul style="list-style-type: none"> <li>• <b>Datum:</b> der Zeitstempel des postfachelements.</li> <li>• <b>Betreff:</b> die Betreffzeile der Nachricht.</li> <li>• <b>Art:</b> den Typ des Fehlers an, das Element übersprungen werden soll.</li> <li>• <b>Ordnername:</b> der Ordner, in dem das übersprungene Element befindet.</li> </ul>
<b>Migrierte Daten</b>	<p>Die Gesamtmenge an Daten (in Bytes und Megabytes (MB)) für die Postfachelemente, die zum Office 365-Postfach migriert wurden. Diese Zahl umfasst Elemente, die in der Erstsynchronisierung und in der inkrementellen Synchronisierung migriert wurden. Dieses Feld enthält keinen Wert für IMAP-Migrationen.</p>
<b>Migrationsrate</b>	<p>Die durchschnittliche Übertragungsrate (in Bytes oder MB pro Minute), mit der Daten in das Office 365-Postfach kopiert werden. Dieses Feld enthält keinen Wert für IMAP-Migrationen.</p>

FELD	BESCHREIBUNG
<b>Fehler</b>	Wenn bei der Migration für den Benutzer ein Fehler aufgetreten ist, wird in diesem Feld eine Beschreibung des Fehlers angezeigt. Diese Fehlerbeschreibung ist auch im Fehlerbericht für die Migration enthalten.
<b>Bericht</b>	Klicken Sie auf <b>Bericht für diesen Benutzer herunterladen</b> , um einen detaillierten Migrationsbericht zu öffnen oder zu speichern, der Diagnoseinformationen über den Migrationsstatus des Benutzers enthält. Sie bzw. der Microsoft-Support können anhand der Informationen in diesem Bericht fehlgeschlagene Migrationen beheben.
<b>Datum der letzten erfolgreichen Synchronisierung</b>	Der letzte Zeitpunkt, an dem neue Elemente im lokalen Postfach in das cloudbasierte Postfach kopiert wurden.

Klicken Sie auf **Weitere Details**, um die folgenden zusätzlichen Informationen zu dem ausgewählten Migrationsbenutzer anzuzeigen.

FELD	BESCHREIBUNG
<b>Dauer in Warteschlange</b>	Die Zeitspanne, während der der Benutzer im Status "In Warteschlange eingereiht" befand.
<b>Bearbeitungsdauer</b>	Die Zeitspanne, während der der Benutzer aktiv migriert wurde.
<b>Synchronisierungsdauer</b>	Die Zeitspanne, während der der Migrationsbenutzer im Status "Synchronisiert" befand.
<b>Verzögerte Dauer</b>	Die Zeitspanne, während der der Migrationsprozess für den Benutzer verzögert wurde.

## Migrationsphasen

Damit Sie die in den vorherigen Abschnitten beschriebenen Migrationsstatus besser verstehen, sollten Sie sich mit den Phasen des Migrationsprozesses vertraut machen. In der folgenden Tabelle sind diese Phasen beschrieben, und es ist angegeben, ob die Phase Bestandteil aller Migrationstypen ist.

MIGRATIONSPHASE	EXCHANGE-ÜBERNAHMEMIGRATION	MEHRSTUFIGE EXCHANGE-MIGRATION	IMAP-MIGRATION
<b>Provisioning:</b> der Migrationsprozess erstellt das neue Office 365-Postfach.	Ja (einschließlich der Verteilergruppen und E-Mail-Kontakte)	Ja (einschließlich der E-Mail-Kontakte)	Nein
<b>Anfängliche Synchronisierung:</b> nach Office 365-Postfächern werden bereitgestellt, der Migrationsprozess Postfachelemente zu den neu bereitgestellten cloudbasierten Postfächern migriert.	Ja (einschließlich der Kalenderzeiten und Kontakte)	Ja (einschließlich der Kalenderzeiten und Kontakte)	Ja

MIGRATIONSPHASE	EXCHANGE-ÜBERNAHMEMIGRATION	MEHRSTUFIGE EXCHANGE-MIGRATION	IMAP-MIGRATION
<b>Inkrementelle Synchronisierung:</b> der Migrationsprozess synchronisiert das lokale und das entsprechende Office 365-Postfach alle 24 Stunden.	Ja	Nein	Ja

# CSV-Dateien für die Migration von Postfächern

18.12.2018 • 12 minutes to read

Sie können eine Datei durch Kommas getrennten Werten (CSV) Massen eine große Anzahl von Postfächern zu migrieren. Sie können eine CSV-Datei angeben, wenn Sie die Exchange-Verwaltungskonsole (EAC) oder das Cmdlet [New-MigrationBatch](#) in Exchange Online verwenden PowerShell, um einen migrationsbatch zu erstellen. Verwenden eine CSV-Datei an mehrere Benutzer um einen migrationsbatch zu migrieren, wird in den folgenden Migrationsszenarien unterstützt:

- **Onboarding und Offboarding in Office 365**

- **Onboarding remote verschieben Migration:** In einer hybriden Exchange-Bereitstellung können Sie Postfächer aus einer lokalen Exchange-Organisation verschieben, zu Office 365. Dies ist auch bekannt als ein Onboarding-remoteverschiebungsmigration, da Sie integrierte Postfächer zu Office 365.
- **Offboarding remote verschieben Migration:** Sie können auch ausführen eine Offboarding-remoteverschiebungsmigration, in dem Sie Office 365-Postfächer zur lokalen Exchange-Organisation migrieren.

**NOTE**

Sowohl Onboarding- als auch Offboarding-Remoteverschiebungsmigrationen werden über Ihre Office 365-Organisation eingeleitet.

- **Mehrstufige Exchange-Migration:** können Sie auch eine Teilmenge von Postfächern aus einer lokalen Exchange-Organisation zu Office 365 migrieren. Dies ist eine andere Art von Onboarding-Migration. Sie können nur Exchange 2003- und Exchange 2007-Postfächer mithilfe einer mehrstufigen Exchange-Migrations migrieren. Migrieren von Exchange 2010 und Exchange 2013-Postfächer wird die Verwendung einer mehrstufigen Migration nicht unterstützt. Vor dem Ausführen einer mehrstufigen Migrations, müssen Sie Directory-Synchronisierung oder eine andere Methode zum Bereitstellen e-Mail-Benutzer in Office 365-Organisation verwenden.
- **IMAP-Migration:** Diese Onboarding Migrationstyp Postfachdaten von einem IMAP-Server (einschließlich Exchange) zu Office 365 migriert. Bei einer IMAP-Migration müssen Sie Postfächer in Office 365 bereitstellen, bevor Sie Postfachdaten migrieren können.

**NOTE**

Eine Exchange-Übernahmemigration unterstützt nicht die Verwendung einer CSV-Datei, weil alle lokalen Benutzerpostfächer in einem einzigen Batch zu Office 365 migriert werden.

## Unterstützte Attribute für CSV-Dateien für Massenverschiebungen oder -migrationen

In der ersten Zeile (Überschriftenzeile) einer CSV-Datei, die für die Migration von Benutzern verwendet wird, werden die Namen der Attribute (Felder) aufgelistet, die in den darauffolgenden Zeilen angegeben sind. Die einzelnen Attributnamen sind durch ein Komma getrennt. Jede Zeile unter der Überschriftenzeile stellt einen einzelnen Benutzer dar und liefert die für die Migration erforderlichen Informationen. Die Attribute in jeder

einzelnen Benutzerzeile müssen dieselbe Reihenfolge wie die Attributnamen in der Überschriftenzeile aufweisen. Die einzelnen Attributwerte sind durch ein Komma getrennt. Wenn der Attributwert für einen bestimmten Datensatz "0" (null) lautet, geben Sie für dieses Attribut nichts ein. Vergessen Sie jedoch nicht, den Nullwert mithilfe des Kommas vom nächsten Attribut zu trennen.

Attributwerte in der CSV-Datei den Wert des entsprechenden Parameters außer Kraft setzen, wenn diese derselbe Parameter beim Erstellen eines migrationsbatches mit der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell verwendet wird. Weitere Informationen und Beispiele finden Sie im Abschnitt [Attributwerte in der CSV-Datei überschreiben Sie die Werte für den migrationsbatch](#).

#### TIP

Sie können die CSV-Datei mit einem beliebigen Texteditor erstellen. Wenn Sie dazu jedoch eine Anwendung wie Microsoft Excel verwenden, können Sie Daten einfacher importieren sowie CSV-Dateien konfigurieren und organisieren. Achten Sie aber darauf, CSV-Dateien als CSV- oder TXT-Datei zu speichern.

In den nachstehenden Abschnitten werden die unterstützten Attribute für die Überschriftenzeile einer CSV-Datei für jeden Migrationstyp beschrieben. Jeder Abschnitt enthält eine Tabelle, in der jedes unterstützte Attribut aufgelistet wird, mit der Angabe, ob es erforderlich ist, einem Beispiel für einen Wert, der für das Attribut zu verwenden ist, und einer Beschreibung.

#### NOTE

In den nachstehenden Abschnitten bezeichnet Quellumgebung den aktuellen Speicherort eines Benutzerpostfachs oder einer Datenbank. Zielumgebung bezeichnet den Speicherort, zu dem das Postfach migriert wird, oder die Datenbank, in die das Postfach verschoben wird.

## Mehrstufige Exchange-Migrationen

Sie müssen eine CSV-Datei verwenden, um die Gruppe von Benutzern für einen Migrationsbatch zu identifizieren, wenn Sie lokale Exchange 2003- und Exchange 2007-Postfächer mithilfe einer mehrstufigen Exchange-Migration zu Office 365 migrieren möchten. Die Anzahl der Postfächer, die Sie mithilfe einer mehrstufigen Exchange-Migration in die Cloud migrieren können, ist nicht begrenzt. Die CSV-Datei für einen Migrationsbatch kann dagegen maximal 2.000 Zeilen enthalten. Zur Migration von mehr als 2.000 Postfächern müssen Sie zusätzliche CSV-Dateien erstellen und dann jede davon zum Erstellen eines neuen Migrationsbatches verwenden. Weitere Informationen zu mehrstufigen Exchange-Migrationen finden Sie unter [Wichtige Informationen zur mehrstufigen E-Mail-Migration zu Office 365](#).

In der nachstehenden Tabelle werden die unterstützten Attribute für eine CSV-Datei für eine mehrstufige Exchange-Migration beschrieben.

ATTRIBUT	ERFORDERLICH ODER OPTIONAL	ZULÄSSIGE WERTE	BESCHREIBUNG
----------	----------------------------	-----------------	--------------

ATTRIBUT	ERFORDERLICH ODER OPTIONAL	ZULÄSSIGE WERTE	BESCHREIBUNG
EmailAddress	Erforderlich	SMTP-Adresse für den Benutzer	Gibt die e-Mail-Adresse für den e-Mail-aktivierten Benutzer (oder ein Postfach, wenn Sie die Migration erneut sind) in Office 365, die das Benutzerpostfach an lokalen entspricht, die migriert werden. E-Mail-aktivierte Benutzer werden in Office 365 als Ergebnis einer Directory-Synchronisierung oder eine andere Bereitstellungsprozess erstellt. Die e-Mail-Adresse des e-Mail-aktivierten Benutzers muss die <i>WindowsEmailAddress</i> - Eigenschaft für das entsprechende lokalen Postfach übereinstimmen.
Password	Optional	Ein Kennwort muss eine Mindestlänge von acht Zeichen haben und eventuelle Kennwortschränkungen erfüllen, die auf Ihre Office 365-Organisation angewendet werden.	Dieses Kennwort wird für das Benutzerkonto festgelegt, wenn der entsprechende E-Mail-aktivierte Benutzer in Office 365 während der Migration in ein Postfach konvertiert wird.
ForceChangePassword	Optional	True oder False	Gibt an, ob ein Benutzer das Kennwort bei der ersten Anmeldung an seinem Office 365-Postfach ändern muss. <b>Hinweis:</b> Wenn Sie eine Lösung für einmaliges Anmelden (SSO) durch die Bereitstellung von Active Directory Federation Services 2.0 (AD FS 2.0) in Ihrer lokalen Organisation implementiert haben, können Sie mit False für den Wert dieses Attributs.

## IMAP-Migrationen

Eine CSV-Datei für einen IMAP-Migrationsbatch kann maximal 50.000 Zeilen enthalten. Es empfiehlt sich jedoch, Benutzer in mehreren kleineren Batches zu migrieren. Weitere Informationen zu IMAP-Migrationen finden Sie unter den folgenden Themen:

- [Migrieren von IMAP-Postfächern zu Office 365](#)
- [CSV-Dateien für IMAP-Migrationsbatches](#)

In der nachstehenden Tabelle werden die unterstützten Attribute für eine CSV-Datei für eine IMAP-Migration beschrieben.

ATTRIBUT	ERFORDERLICH ODER OPTIONAL	ZULÄSSIGE WERTE	BESCHREIBUNG
EmailAddress	Erforderlich	SMTP-Adresse für den Benutzer	Gibt die Benutzer-ID für das Office 365-Postfach des Benutzers an.
UserName	Erforderlich	Zeichenfolge zur Identifizierung des Benutzers im IMAP-Messaging-System in einem vom IMAP-Server unterstützten Format	Gibt den Anmeldenamen für das Konto des Benutzers im IMAP-Messagingsystem (der Quell-Umgebung). Zusätzlich zu den Benutzernamen können Sie die Anmeldeinformationen eines Kontos, die die erforderlichen Berechtigungen zum Zugriff auf Postfächer auf dem IMAP-Server zugewiesen wurde. Weitere Informationen finden Sie unter <a href="#">CSV-Dateien für IMAP-migrationsbatches</a> .
Password	Erforderlich	Kennwortzeichenfolge	Gibt das Kennwort für das Benutzerkonto an, das durch das Attribut "UserName" festgelegt wurde.

## Die Attributwerte in der CSV-Datei setzen die Werte für den Migrationsbatch außer Kraft

Attributwerte in der CSV-Datei den Wert des entsprechenden Parameters außer Kraft setzen, wenn diese derselbe Parameter beim Erstellen eines migrationsbatches mit der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell verwendet wird. Wenn Sie den Migration Batch Wert auf einen Benutzer angewendet werden soll, würden Sie diese Zelle in der CSV-Datei weglassen. Auf diese Weise können Sie das Mischen und bestimmte Attributwerte für ausgewählte Benutzer in einem migrationsbatch übereinstimmen.

Nehmen Sie in diesem Beispiel an, dass Sie einen Batch für eine Onboarding-Remoteverschiebungsmigration in einer Hybridbereitstellung erstellen, um Archivpostfächer mit dem folgenden [New-MigrationBatch](#)-Befehl zu Office 365 zu verschieben:

```
New-MigrationBatch -Name OnBoarding1 -SourceEndpoint RemoteEndpoint1 -TargetDeliveryDomain cloud.contoso.com -  
CSVData ([System.IO.File]::ReadAllBytes("C:\Users\Administrator\Desktop\OnBoarding1.csv")) -MailboxType  
ArchiveOnly -AutoStart
```

Da Sie aber auch die primären Postfächer für ausgewählte Benutzer verschieben möchten, würde ein Teil der Datei "OnBoarding1.csv" für diesen Migrationsbatch so aussehen:

```
EmailAddress,MailboxType  
user1@contoso.com,  
user2@contoso.com,  
user3@cloud.contoso.com,PrimaryAndArchive  
user4@cloud.contoso.com,PrimaryAndArchive  
...
```

Da der Wert für die Postfachtyp in der CSV-Datei die Werte für den Parameter *MailboxType* in den Befehl zum Erstellen des Stapels überschreibt, wird nur für das Archivpostfach user1 und user2 zu Office 365 migriert. Aber

die primäre und archivpostfächer für user3 und user4 in Office 365 verschoben werden.

# Zusammenarbeit in Exchange Online

18.12.2018 • 8 minutes to read

Office 365 und Exchange Online bietet verschiedene Features, die Ihre Endbenutzer auf einfache Weise der Zusammenarbeit per e-Mail helfen kann.

Jedes dieser Features, die in den folgenden Abschnitten beschrieben hat eine andere benutzererfahrung und Feature festgelegt und sollte verwendet werden, basierend auf was Ihre Benutzer ausführen müssen, und was Ihrer Organisation bereitstellen kann. Beispielsweise bieten websitepostfächer umfangreiche Dokumentation Features für die Zusammenarbeit. Jedoch verlassen von websitepostfächern in SharePoint, sodass Sie Sie bei der Planung werden nicht zum Abonnieren von SharePoint, Öffentliche Ordner Gemeinsame Nutzung von Dokumenten verwenden können.

In diesem Thema werden diese Funktionen für die Zusammenarbeit verglichen, um Sie bei der Entscheidung zu unterstützen, was Sie Ihren Benutzern anbieten möchten.

## Websitepostfächer

Ein Websitepostfach setzte sich funktionell aus der Mitgliedschaft in einer SharePoint-Website (Besitzer und Mitglieder), aus einem gemeinsamen Speicher in Form eines Exchange-Postfachs für E-Mails und aus einer SharePoint-Website für Speicherung und Freigabe zusammen. In einem Websitepostfach werden im Wesentlichen Exchange-E-Mail und SharePoint-Dokumente zusammengeführt. Für Benutzer dient ein Websitepostfach als zentrale Projektablage, die einen Speicherort für Projekt-E-Mails und -dokumente bereitstellt, die nur von Websitemitgliedern aufgerufen und bearbeitet werden können. Außerdem haben Websitepostfächer einen bestimmten Lebenszyklus und sind für Projekte optimiert, die ein Start- und Enddatum aufweisen. Endnutzer müssen Outlook 2013 verwenden, um Websitepostfächer vollständig zu implementieren.

Weitere Informationen finden Sie unter [Vorbereiten der Verwendung von Websitepostfächern in Office 365](#).

## Öffentliche Ordner

Öffentliche Ordner ermöglichen den gemeinsamen Zugriff und stellen ein einfaches und effektives Mittel zum Erfassen, Organisieren und Freigeben von Informationen für andere Personen in der Arbeitsgruppe oder Organisation dar.

Dieser Inhalt wird mithilfe öffentlicher Ordner in einer Hierarchie angeordnet, die einfach zu durchsuchen ist. Benutzer können interessante und relevante Inhalte finden, indem Sie die für sie relevanten Unterordner dieser Hierarchie durchsuchen. Den Benutzern wird immer die vollständige Hierarchie in ihrer Outlook-Ordneransicht angezeigt. Öffentliche Ordner sind eine großartige Möglichkeit zur Archivierung von Verteilergruppen. Öffentliche Ordner können E-Mail-aktiviert und als Mitglied der Verteilergruppe hinzugefügt werden. Die an die Verteilergruppe gesendeten E-Mails werden automatisch für den späteren Zugriff zum öffentlichen Ordner hinzugefügt. Öffentliche Ordner bieten außerdem eine einfache Dokumentfreigabe und setzen nicht die Installation von SharePoint in Ihrer Organisation voraus. Schließlich können Endbenutzer öffentliche Ordner mit den folgenden unterstützten Outlook-Clients nutzen: Outlook 2007, Outlook 2010, Outlook 2013 und Outlook Web App, allerdings mit einigen Einschränkungen.

Weitere Informationen finden Sie unter [Öffentliche Ordner in Office 365 und Exchange Online](#).

## Freigegebene Postfächer

Ein freigegebenes Postfach ist ein Postfach, auf das mehrere vorgesehene Benutzer zum Lesen und Senden von E-

Mail-Nachrichten zugreifen und das sie zum Freigeben eines gemeinsamen Kalenders nutzen können. Freigegebene Postfächer können eine allgemeine E-Mail-Adresse (wie "info@contoso.com" oder "vertrieb@contoso.com") bereitstellen, über die Kunden Anfragen an das Unternehmen senden können. Wenn dem freigegebenen Postfach die Berechtigung "Senden als" zugewiesen ist, wenn ein angegebener Benutzer auf die E-Mail-Nachricht antwortet, kann es so aussehen, als ob das Postfach (z. B. "vertrieb@contoso.com") und nicht der eigentliche Benutzer antwortet.

Weitere Informationen finden Sie unter [Shared Mailboxes](#).

## Gruppen

Gruppen, auch Verteilergruppen genannt, sind eine Zusammenstellung von mindestens zwei Personen, die im freigegebenen Adressbuch angezeigt wird. Wenn eine E-Mail-Nachricht an eine Gruppe gesendet wird, wird sie von allen Mitgliedern der Gruppe empfangen. Verteilergruppen können nach einem bestimmten Diskussionsthema wie "Tierfreunde" oder nach Benutzern mit einer gemeinsamen Arbeitsstruktur angeordnet werden, die eine regelmäßige Kommunikation untereinander erfordert.

Weitere Informationen finden Sie unter [Empfänger in Exchange Online](#).

## Auswahl der richtigen Option

Die folgende Tabelle bietet einen schnellen Überblick über die einzelnen Funktionen für die Zusammenarbeit, um Ihnen die Auswahl der richtigen Option zu erleichtern.

	WEBSITEPOSTFÄCHER	ÖFFENTLICHE ORDNER	FREIGEGBENE POSTFÄCHER	GRUPPEN
<b>Art der Gruppe</b>	Zusammenarbeit als Team an einem bestimmten Projekt mit konkretem Start- und Enddatum.	Bei entsprechenden Berechtigungen können alle Personen in Ihrer Organisation auf öffentliche Ordner zugreifen und diese durchsuchen. Öffentliche Ordner eignen sich ideal für die Verwaltung des Verlaufs oder von Unterhaltungen in Verteilergruppen.	Stellvertretungen, die im Namen einer virtuellen Identität arbeiten und als diese freigegebene Postfachidentität auf E-Mails antworten können. Beispiel: support@tailspintoy.com	Benutzer, die E-Mails an eine Gruppe von Empfängern mit gemeinsamen Interessen oder Merkmalen senden müssen.
<b>Ideale Gruppengröße</b>	Klein	Groß	Klein	Groß
<b>Zugriff</b>	Websitepostfachbesitzer und -mitglieder.	Der Zugriff ist allen Benutzern in Ihrer Organisation möglich.	Benutzern können Berechtigungen für den Vollzugriff und/oder zum Senden erteilt werden. Wenn Benutzer die Berechtigungen für den Vollzugriff erhalten, müssen Sie das freigegebene Postfach auch zu ihrem Outlook-Profil hinzufügen, um darauf zugreifen zu können.	Für Verteilergruppen müssen Mitglieder manuell hinzugefügt werden. Für dynamische Verteilergruppen werden die Mitglieder anhand von Filterkriterien hinzugefügt.

	WEBSITEPOSTFÄCHER	ÖFFENTLICHE ORDNER	FREIGEGEBENE POSTFÄCHER	GRUPPEN
<b>Freigegebener Kalender?</b>	Nein	Ja	Ja	Nein
<b>E-Mail-Eingang im persönlichen Posteingang des Benutzers?</b>	Nein, E-Mails gehen im Websitepostfach ein.	Nein, E-Mails gehen im öffentlichen Ordner ein.	Nein, E-Mails gehen im Posteingang des freigegebenen Postfachs ein.	Ja. Ja, E-Mails gehen im Posteingang des Mitglieds einer Verteilergruppe ein.
<b>Unterstützte Clients</b>	Outlook 2013 SharePoint Online	Outlook 2013 Outlook Web App Outlook 2010 Outlook 2007	Outlook 2013 Outlook Web App Outlook 2010 Outlook 2007	Outlook 2013 Outlook Web App Outlook 2010 Outlook 2007

# Öffentliche Ordner in Office 365 und Exchange Online

18.12.2018 • 14 minutes to read

Öffentliche Ordner ermöglichen den gemeinsamen Zugriff und stellen ein einfaches und effektives Mittel zum Erfassen, Organisieren und Freigeben von Informationen für andere Personen in der Arbeitsgruppe oder Organisation dar. Dieser Inhalt wird mithilfe öffentlicher Ordner in einer Hierarchie angeordnet, die einfach zu durchsuchen ist. Benutzern wird die vollständige Hierarchie in Outlook angezeigt, sodass sie sie leicht nach den Inhalten durchsuchen können, an denen sie interessiert sind.

## NOTE

Öffentliche Ordner sind in der folgenden Outlook-Clients zur Verfügung: Outlook Web App für Exchange, Outlook 2007, Outlook 2010, Outlook 2013 und Outlook für Mac

Öffentliche Ordner können auch als Archivierungsmethode für Verteilergruppen verwendet werden. Wenn Sie einen öffentlichen Ordner für E-Mail aktivieren und der Verteilergruppe hinzufügen, werden an die Gruppe gesendete E-Mails automatisch dem öffentlichen Ordner hinzugefügt, damit sie später zur Verfügung stehen.

Öffentliche Ordner sind zu folgenden Zwecken nicht geeignet:

- **Datenarchivierung.** Benutzer, die Postfachbeschränkungen beachten müssen, verwenden manchmal öffentliche Ordner anstelle von Postfächern zum Archivieren von Daten. Diese Vorgehensweise wird nicht empfohlen, da dadurch Speicherplatz in öffentlichen Ordnern belegt wird und Postfachbeschränkungen ihren Sinn verlieren. Stattdessen wird die Verwendung von [In-Place Archiving](#) als Archivierungslösung empfohlen.
- **Gemeinsame Nutzung von Dokumenten und Zusammenarbeit.** Öffentliche Ordner stellen keine Versionsverwaltung oder andere Dokumentverwaltungsfeatures wie z. B. gesteuerte Eincheck- und Auscheckfunktionen oder automatische Benachrichtigungen bei Inhaltsänderungen zur Verfügung. Stattdessen empfiehlt sich die Verwendung von [SharePoint Online](#) als Lösung für die Dokumentfreigabe.

Weitere Informationen zu öffentlichen Ordnern und anderen Methoden zur Zusammenarbeit in Office 365 und Exchange Online finden Sie unter [Zusammenarbeit in Exchange Online](#).

Eine Liste häufig gestellter Fragen zu öffentlichen Ordnern in Office 365 und Exchange Online finden Sie unter [FAQ: Public folders](#).

Weitere Informationen über Kontingente für öffentliche Ordner in Office 365 und Exchange Online finden Sie in den Dienstbeschreibungsthemen [Freigabe und Zusammenarbeit](#) und [Exchange Online-Begrenzungen](#).

Eine Liste der Verwaltungsaufgaben für öffentliche Ordner finden Sie unter [Öffentliche Ordnerprozeduren in Office 365 und Exchange Online](#).

Weitere Informationen über Begrenzungen für öffentliche Ordner in Office 365 und Exchange Online finden Sie unter [Exchange Online-Begrenzungen](#).

Suchen Sie die Exchange Server-Version dieses Themas? Finden Sie unter [Public Folders](#).

## Architektur für öffentliche Ordner

Die Architektur für öffentliche Ordner verwendet speziell entworfene Postfächer, um sowohl die Hierarchie

öffentlicher Ordner als auch ihren Inhalt zu speichern. Die wichtigsten Architekturkomponenten von öffentlichen Ordnern sind die Postfächer für öffentliche Ordner.

## Postfächer für öffentliche Ordner

Es gibt zwei Arten von Postfächern für öffentliche Ordner: das primäre Hierarchiepostfach und die sekundären Hierarchiepostfächer. Beide Arten von Postfächern können Inhalte enthalten:

- **Hierarchie der primären Postfach:** das Postfach des primären Hierarchie der eine schreibbare Kopie der die Hierarchie Öffentlicher Ordner ist. Diese werden schreibgeschützte Kopien, jedoch wird die Hierarchie Öffentlicher Ordner in allen anderen Postfächer für Öffentliche Ordner kopiert.
- **Sekundäre hierarchiepostfächer:** sekundäre hierarchiepostfächer enthalten ebenfalls Inhalte Öffentlicher Ordner und eine schreibgeschützte Kopie der Hierarchie für Öffentliche Ordner.

Es gibt zwei Möglichkeiten, Postfächer öffentlicher Ordner zu verwalten:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Öffentliche Ordner > Postfächer für den öffentlichen Ordner**.
- Verwenden Sie in Exchange Online PowerShell den \*\* \*-Postfach\*\* Gruppe von Cmdlets.

## Hierarchie öffentlicher Ordner

Die Hierarchie öffentlicher Ordner enthält die Eigenschaften der Ordner sowie organisatorische Informationen einschließlich der Baumstruktur. Jedes Postfach für öffentliche Ordner enthält eine Kopie der Hierarchie öffentlicher Ordner. Es gibt nur eine schreibbare Kopie der Hierarchie. Diese befindet sich im primären Postfach für öffentliche Ordner. Für einen bestimmten Ordner werden die Hierarchiedaten zum Identifizieren der folgenden Informationen verwenden:

- Berechtigungen für den Ordner
- Die Position des Ordners in der Struktur für öffentliche Ordner einschließlich der über- und untergeordneten Ordner

### NOTE

In der Hierarchie werden keine Informationen zu E-Mail-Adressen für E-Mail-aktivierte öffentliche Ordner gespeichert. E-Mail-Adressen werden im Verzeichnis gespeichert.

## Hierarchiesynchronisierung

Beim Synchronisierungsvorgang für die Hierarchie öffentlicher Ordner wird ICS (Incremental Change Synchronization) verwendet. So wird ein Mechanismus für die Überwachung und Synchronisierung von Änderungen an einer Exchange-Speicherhierarchie oder an Inhalten bereitgestellt. Die Änderungen umfassen das Erstellen, Ändern und Löschen von Ordner und Nachrichten. Wenn Benutzer Verbindungen zu Inhaltspostfächern hergestellt haben und diese verwenden, tritt die Synchronisierung alle 15 Minuten auf. Wenn keine Benutzer über eine Verbindung zu einem Inhaltspostfach verfügen, wird die Synchronisierung weniger häufig ausgelöst (alle 24 Stunden). Wenn ein Schreibvorgang, wie die Erstellung eines Ordners, in der primären Hierarchie durchgeführt wird, wird die Synchronisierung zum Inhaltspostfach sofort (synchron) ausgelöst.

### IMPORTANT

Da nur eine schreibbare Kopie der Hierarchie vorhanden ist, wird die Ordnererstellung durch das Inhaltspostfach, mit dem Benutzer verbunden sind, an das Hierarchiepostfach weitergegeben.

Weitere Informationen finden Sie unter [der Hierarchie Öffentlicher Ordner aktualisieren](#).

### Inhalte öffentlicher Ordner

Inhalte öffentlicher Ordner können E-Mails, Beiträge, Dokumente und eForms einschließen. Die Inhalte werden im Postfach des öffentlichen Ordners gespeichert, werden jedoch nicht in mehrere Postfächer öffentlicher Ordner repliziert. Alle Benutzer greifen auf dasselbe Postfach für öffentliche Ordner zu, um dieselben Inhalte abzurufen. Zwar steht eine Volltextsuche im Inhalt eines öffentlichen Ordners zur Verfügung; Inhalte sind jedoch nicht über öffentliche Ordner hinweg durchsuchbar und werden nicht von der Exchange-Suche indiziert.

## Überlegungen

Während die Verwendung öffentlicher Ordner in Office 365 und Exchange Online zahlreiche Vorteile bietet, sollten Sie auch einige Einschränkungen überdenken, bevor Sie sie in Ihrer Organisation implementieren:

- Outlook Web App wird unterstützt, aber mit Einschränkungen. Sie können öffentliche Ordner als Favoriten hinzufügen und entfernen und Vorgänge auf Elementebene durchführen, wie das Erstellen, Bearbeiten, Löschen und Beantworten von Beiträgen. Sie können jedoch öffentliche Ordner nicht über Outlook Web App erstellen oder löschen.
- Zwar steht eine Volltextsuche im Inhalt eines öffentlichen Ordners zur Verfügung; Inhalte sind jedoch nicht über öffentliche Ordner hinweg durchsuchbar und werden nicht von der Exchange-Suche indiziert.
- Zum Zugreifen auf öffentliche Ordner in Office 365 und Exchange Online müssen Sie Outlook 2007 oder höher verwenden.
- Aufbewahrungsrichtlinien werden für Postfächer öffentlicher Ordner nicht unterstützt.

## Migration von öffentlichen Ordnern zu Office 365 und Exchange Online

Wenn Sie Ihre öffentlichen Ordner migrieren, verwenden Sie einen Prozess mit der Bezeichnung Batchmigration des öffentlichen Ordners. Bei der Batchmigration des öffentlichen Ordners (oder einfach nur Batchmigration) wird eine Postfachmigrationsanforderung für jedes Postfach des öffentlichen Ordners erstellt, das in Exchange Online vorhanden sein wird. Das Verwenden mehrerer Anforderungen bedeutet, dass die Migration viel schneller erfolgt, da die verfügbare Netzwerkbandbreite effizienter genutzt werden kann. Diese Vorgehensweise ist auch zuverlässiger, da die Möglichkeit einer einzelnen Störung oder eines Engpasses, die bzw. der sich auf die gesamte Migration auswirkt, verringert wird.

Während Migrationen Batch mithilfe des **New-MigrationBatch**-Cmdlets in Exchange Online PowerShell gestartet werden müssen, können den Fortschritt und den Abschluss der Migration angezeigt und in der Exchange-Verwaltungskonsole verwaltet werden. Da das Cmdlet **New-MigrationBatch** eine Postfachmigrationsanforderung für jedes Postfach für Öffentliche Ordner initiiert, können Sie den Status der diese Anforderungen mithilfe der Seite Postfach Migration anzeigen. Sie erhalten Sie auf der Seite Mailbox Migration und Migrationsberichte, die an Sie gesendet werden können, von der Exchange-Verwaltungskonsole in Exchange Online öffnen, und Navigieren zum **Postfach** erstellen können > **Migration**.

Um die Batchmigration zum Migrieren Ihrer öffentlichen Ordner zu Exchange Online zu verwenden, muss der Exchange-Legacyserver die Anforderungen in der folgenden Liste erfüllen. Wenn dies der Fall ist und Sie beginnen können, checken Sie [Verwenden der Stapelmigration zum Migrieren von öffentlichen Ordnern einer Vorgängerversion zu Office 365 und Exchange Online](#) aus.

Exchange unterstützt das Verschieben Ihrer öffentlichen Ordner von den folgenden Legacyversionen von Exchange Server zu Office 365 und Exchange Online:

- Exchange Server 2010 SP3 RU8 oder höher

Finden Sie unter [Verwendung Batch Migration zu Exchange 2013 öffentlicher Ordner zu Exchange Online migrieren](#) Ihrer öffentlichen Ordner von Exchange Server zu migrieren.

Es wird empfohlen, statt des PST-Exportfeatures von Outlook die Batchmigration zum Migrieren öffentlicher Ordner zu Office 365 und Exchange Online zu verwenden. Das Anwachsen des Postfachs für öffentliche Ordner in Office 365 und Exchange Online wird über ein Feature zur automatischen Aufteilung verwaltet, welches das Postfach für öffentliche Ordner aufteilt, wenn Größenkontingente überschritten werden. Das plötzliche Anwachsen der Postfächer für öffentliche Ordner kann nicht von der automatischen Aufteilung verwaltet werden, wenn Sie öffentliche Ordner über den PST-Export migrieren. Sie müssen dann möglicherweise bis zu zwei Wochen warten, bis die Daten durch automatische Aufteilung aus dem primären Postfach verschoben werden. Anweisungen für die Batchmigration finden Sie in [Verwenden der Stapelmigration zum Migrieren von öffentlichen Ordner einer Vorgängerversion zu Office 365 und Exchange Online](#) und [Use batch migration to migrate Exchange 2013 public folders to Exchange Online](#). Wenn Sie jedoch bereits eine PST-Migration gestartet haben und ein Problem aufgetreten ist, weil das primäre Postfach voll ist, können Sie die PST-Migration auf zwei Arten wiederherstellen:

1. Warten, bis die Daten von der automatischen Aufteilung aus dem primären Postfach verschoben werden. Dies kann bis zu zwei Wochen dauern. Allerdings können alle Öffentlichen Ordner in einem vollständig gefüllten Postfach für Öffentliche Ordner keine neuen Inhalte empfangen, bis die automatische Aufteilung abgeschlossen ist.
2. [Erstellen eines Postfachs für Öffentliche Ordner](#) und dann verwenden Sie das Cmdlet **[New-PublicFolder]** mit dem Parameter *Mailbox* die verbleibenden Öffentlichen Ordner im Postfach sekundären Öffentlichen Ordner zu erstellen. Dieses Beispiel erstellt einen neuen öffentlichen Ordner mit dem Namen PF201 im sekundären Öffentlichen Ordner-Postfach.

```
New-PublicFolder -Name PF201 -Mailbox SecondaryPFMbx
```

# Öffentliche Ordnerprozeduren in Office 365 und Exchange Online

18.12.2018 • 2 minutes to read

[Verwenden der Stapelmigration zum Migrieren von öffentlichen Ordnern einer Vorgängerversion zu Office 365 und Exchange Online](#)

[Migrieren von Exchange 2013-basierten öffentlichen Ordnern zu Exchange Online mithilfe einer Batchmigration](#)

[Configure legacy on-premises public folders for a hybrid deployment](#)

[Konfigurieren von öffentlichen Ordnern von Exchange Server für eine hybridbereitstellung](#)

[Konfigurieren öffentlicher Exchange Online-Ordner für eine Hybridbereitstellung](#)

[Einrichten von öffentlichen Ordnern in einer neuen Organisation](#)

[Zugreifen auf öffentliche Ordner mit Outlook 2016 für Mac](#)

[\(Erstellen eines Postfachs für öffentliche Ordner\)](#)

[Erstellen eines öffentlichen Ordners](#)

[Wiederherstellen eines gelöschten Postfachs für öffentliche Ordner](#)

[Verwenden bevorzugter öffentlicher Ordner in Outlook im Web](#)

[E-Mail-Aktivierung oder E-Mail-Deaktivierung von öffentlichen Ordnern](#)

[Update the public folder hierarchy](#)

[Remove a public folder](#)

[Anzeigen von Statistiken für öffentliche Ordner und Elemente öffentlicher Ordner](#)

# Verwenden der Stapelmigration zum Migrieren von öffentlichen Ordner einer Vorgängerversion zu Office 365 und Exchange Online

18.12.2018 • 49 minutes to read

**Zusammenfassung:** Verwenden Sie diese Verfahren, um Ihre öffentlichen Ordner von Exchange 2010 nach Office 365 zu verschieben.

In diesem Thema wird beschrieben, wie Ihre öffentlichen Ordner in einer einstufigen oder mehrstufigen Migration von Updaterollup 8 für Exchange Server 2010 Service Pack 3 (SP3) in Office 365 oder Exchange Online migrieren.

Dieses Thema bezieht sich auf dem Exchange 2010 SP3 RU8 Server als Exchange-Legacyserver. Darüber hinaus gelten die Schritte in diesem Thema zu Exchange Online und Office 365. Die Begriffe können in diesem Thema synonym verwendet werden.

## NOTE

In diesem Artikel beschriebenen Batch Migration-Methode ist die einzige unterstützte Methode für das Migrieren von öffentlichen Legacyordnern zu Office 365 und Exchange Online. Die alte seriellen Migrationsmethode für die Migration Öffentlicher Ordner wird von Microsoft nicht mehr unterstützt.

Es wird empfohlen, nicht das PST-Exportfeature von Outlook zum Migrieren öffentlicher Ordner zu Office 365 oder Exchange Online zu verwenden. Das Anwachsen des Postfachs für öffentliche Ordner in Office 365 und Exchange Online wird über ein Feature zur automatischen Aufteilung verwaltet, welches das Postfach für öffentliche Ordner aufteilt, wenn Größenkontingente überschritten werden. Das plötzliche Anwachsen der Postfächer für Öffentliche Ordner kann nicht von der automatischen Aufteilung verwaltet werden, wenn Sie Öffentliche Ordner über den PST-Export migrieren. Sie müssen dann möglicherweise bis zu zwei Wochen warten, bis die Daten durch automatische Aufteilung aus dem primären Postfach verschoben werden. Es wird empfohlen, den Cmdlet-basierten Anweisungen in diesem Dokument zu folgen, um öffentliche Ordner zu Office 365 und Exchange Online zu migrieren. Wenn Sie sich dennoch dafür entscheiden, Öffentliche Ordner per PST-Export zu migrieren, sollten Sie den Abschnitt [Migrieren von Öffentlichen Ordner zu Office 365 mit PST-Export von Outlook](#) weiter unten in diesem Thema lesen.

Die Migration wird mit den Cmdlets **\*-MigrationBatch** sowie mit den folgenden PowerShell-Skripts ausgeführt:

- `Export-PublicFolderStatistics.ps1` : Dieses Skript erstellt die Datei zur Zuordnung von Ordner Namen zu Ordnergrößen. Dieses Skript führen Sie auf dem Exchange-Legacyserver.
- `Export-PublicFolderStatistics.psd1` : Diese Unterstützungsdatei wird von der `Export-PublicFolderStatistics.ps1` Skript und sollte an denselben Speicherort heruntergeladen werden.
- `PublicFolderToMailboxMapGenerator.ps1` : Dieses Skript erstellt die Datei zur Zuordnung von öffentlichen Ordner zu Postfächern anhand der Ausgabe aus der `Export-PublicFolderStatistics.ps1` Skript. Dieses Skript führen Sie auf dem Exchange-Legacyserver.
- `PublicFolderToMailboxMapGenerator.strings.psd1` : Diese Unterstützungsdatei wird von der `PublicFolderToMailboxMapGenerator.ps1` Skript und sollte an denselben Speicherort heruntergeladen werden.

- `Create-PublicFolderMailboxesForMigration.ps1` : Dieses Skript erstellt die Postfächer für Öffentliche Ordner Ziel für die Migration. Dieses Skript berechnet darüber hinaus die Anzahl der Postfächer, die erforderlich sind, um die geschätzte Benutzerlast, basierend auf die Richtlinien für die Anzahl der benutzeranmeldungen pro Postfach für Öffentliche Ordner empfohlen, [Grenzwerte für Öffentliche Ordner](#) zu behandeln.
- `Create-PublicFolderMailboxesForMigration.strings.ps1` : Diese Unterstützungsdatei wird von dem Skript erstellen `PublicFolderMailboxesForMigration.ps1` verwendet und sollte an denselben Speicherort heruntergeladen werden.
- `Sync-MailPublicFolders.ps1` : Mit diesem Skript werden e-Mail-aktivierte Öffentliche Ordner-Objekte zwischen Ihrer lokalen Exchange-Bereitstellung und Office 365 synchronisiert. Dieses Skript führen Sie auf dem Exchange-Legacyserver.
- `SyncMailPublicFolders.strings.ps1` : Dies ist eine Unterstützungsdatei, die durch die `Sync-MailPublicFolders.ps1` Skript und an den gleichen Speicherort wie die vorhergehenden Skripts kopiert werden sollte.

[Schritt 1: Herunterladen der Migrationsskripts](#) enthält nähere Informationen dazu, wo Sie diese Skripts herunterladen können. Stellen Sie sicher, dass alle Skripts unter demselben Speicherort heruntergeladen werden.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Öffentliche Ordner finden Sie unter [Public Folder Procedures](#).

## Welche Versionen von Exchange werden für die Migration öffentlicher Ordner zu Office 365 und Exchange Online unterstützt?

Exchange unterstützt das Verschieben Ihrer öffentlichen Ordner von den folgenden Legacyversionen von Exchange Server zu Office 365 und Exchange Online:

- Exchange 2010 SP3 RU8 oder höher

Wenn Ihre lokalen Server werden nicht die minimale Unterstützung Versionen von Exchange 2010 ausführen, jedoch Sie Ihre öffentlichen Ordner zu Exchange Online verschieben müssen, wird dringend empfohlen, dass Sie Ihre lokalen Server aktualisieren und Verwendung Batch Migration, der den einzigen unterstützten Öffentlichen Ordner-Migration-Methode.

Öffentliche Ordner können nicht direkt von Exchange 2003 migriert werden. Wenn Sie Exchange 2003 in Ihrer Organisation ausführen, müssen Sie alle Datenbanken für Öffentliche Ordner und Replikate auf Exchange 2010 SP3 RU8 oder höher zu verschieben. Keine Replikate Öffentlicher Ordner können auf Exchange 2003 verbleiben. Darüber hinaus kann nicht für einen öffentlichen Ordner von Exchange 2013 gesendeten Nachrichten über einen Exchange 2003-Server weitergeleitet werden.

## Was sollten Sie wissen, bevor Sie beginnen?

- Auf dem Exchange 2010-Server muss Exchange 2010 SP3 RU8 oder höher ausgeführt werden.
- In Office 365 und Exchange Online müssen Sie ein Mitglied der Rollengruppe "Organisationsverwaltung" sein. Diese Rollengruppe unterscheidet sich von den Berechtigungen, die Ihnen zugewiesen wurden, als Sie Office 365 oder Exchange Online abonniert haben. Weitere Informationen dazu, wie Sie die Rollengruppe "Organisationsverwaltung" aktivieren können, finden Sie unter [Manage Role Groups](#).
- Sie müssen in Exchange 2010 ein Mitglied der Rollengruppe "Organisationsverwaltung" oder "Serververwaltung RBAC" sein. Nähere Informationen finden Sie unter [Hinzufügen von Mitgliedern zu einer Rollengruppe](#).

- Wenn es in Ihrer Organisation Öffentliche Ordner gibt, die größer als 2 GB sind, empfehlen wir, vor der Migration entweder Inhalte aus diesem Ordner zu löschen oder ihn in mehrere Öffentliche Ordner aufzuteilen. Wenn keine dieser Möglichkeiten infrage kommt, wird empfohlen, die öffentlichen Ordner nicht zu Office 365 und Exchange Online zu verschieben.
- In Office 365 und Exchange Online können Sie maximal 1.000 Postfächer für öffentliche Ordner erstellen.
- Bevor Sie Ihre öffentlichen Ordner migrieren, empfehlen wir, zuerst alle Benutzerpostfächer zu Office 365 und Exchange Online zu verschieben. Weitere Informationen finden Sie unter [Methoden zum Migrieren mehrerer E-Mail-Konten zu Office 365](#).
- Outlook Anywhere auf dem Exchange-Legacyserver aktiviert werden muss. Ausführliche Informationen zum Aktivieren von Outlook Anywhere auf Exchange 2010-Servern finden Sie unter [Outlook Anywhere aktivieren](#).
- Dieses Verfahren kann nicht mithilfe des Exchange Admin Centers (EAC) oder der Exchange-Verwaltungskonsole (EMC) ausgeführt werden. Sie müssen auf den Exchange-Legacyservern die Exchange-Verwaltungsshell verwenden. Für Exchange Online müssen Sie die Exchange Online PowerShell verwenden. Weitere Informationen finden Sie unter [Herstellen einer Verbindung mit Exchange Online mithilfe der Remote-PowerShell](#).
- Sie müssen einen einzelnen migrationsbatch verwenden, um alle Daten Ihrer öffentlichen Ordner zu migrieren. Exchange kann nur einen migrationsbatch zu einem Zeitpunkt erstellen. Wenn Sie versuchen, die gleichzeitig mehrere migrationsbatch zu erstellen, wird das Ergebnis ein Fehler.
- Bevor Sie beginnen, sollten Sie dieses Thema vollständig lesen, da für einige Schritte Ausfallzeiten erforderlich sind.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Schritt 1: Herunterladen der Migrationsskripts

1. Laden Sie alle Skripts und unterstützenden Dateien unter [Public Folders Migration Scripts](#) herunter.
2. Speichern Sie die Skripts auf dem lokalen Computer, auf dem Sie PowerShell ausführen. Verwenden Sie als Speicherort beispielsweise C:\PFSscripts. Stellen Sie sicher, dass alle Skripts unter demselben Speicherort gespeichert werden.
3. Laden Sie die folgenden Dateien von [E-Mail-aktivierten öffentlichen Ordnern - Skript für die Verzeichnissynchronisierung](#) herunter:
  - `Sync-MailPublicFolders.ps1`
  - `SyncMailPublicFolders.strings.psd1`
4. Speichern Sie die Skripts am gleichen Speicherort, den Sie unter Schritt 2 verwendet haben, z. B. C:\PFSscripts.

## Schritt 2: Vorbereiten der Migration

Führen Sie vor Beginn der Migration die folgenden erforderlichen Schritte durch.

## Allgemeine erforderliche Schritte

- Stellen Sie sicher, dass keine verwaisten E-Mail-Objekte für öffentliche Ordner in Active Directory vorhanden sind, also Objekte in Active Directory ohne ein entsprechendes Exchange-Objekt.
- Vergewissern Sie sich, dass die SMTP-E-Mail-Adresse, die für öffentliche Ordner in Active Directory konfiguriert wird, mit den SMTP-E-Mail-Adressen für die Exchange-Objekte übereinstimmt.
- Stellen Sie sicher, dass keine doppelten Objekte für öffentliche Ordner in Active Directory vorhanden sind, um eine Situation zu vermeiden, bei der zwei oder mehrere Active Directory-Objekte auf den gleichen E-Mail-aktivierten öffentlichen Ordner verweisen.

## Erforderliche Schritte auf dem Exchange-Legacyserver

1. Stellen Sie auf dem Exchange-Legacyserver sicher, dass das Routing zu den E-Mail-aktivierten öffentlichen Ordnern, die für Exchange Online vorgesehen sind, weiterhin funktioniert, bis alle DNS-Caches über das Internet so aktualisiert wurden, dass sie auf den Exchange Online-DNS verweisen, auf dem sich Ihre Organisation nun befindet. Führen Sie dazu den folgenden Befehl aus, um eine akzeptierte Domäne mit einem bekannten Namen zu konfigurieren, die E-Mail-Nachrichten korrekt zur Exchange Online-Domäne routet.

```
New-AcceptedDomain -Name "PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99" -DomainName contoso.onmicrosoft.com -DomainType InternalRelay
```

Wenn der Name eines öffentlichen Ordners mit einen umgekehrten Schrägstrich enthält (\) oder einen Schrägstrich (/), die öffentlichen Ordner möglicherweise im übergeordneten öffentlichen Ordner erstellt werden, wenn Migration auftritt. Bevor Sie migrieren, wird empfohlen, dass Sie Öffentliche Ordner umbenennen, die einen umgekehrten Schrägstrich oder einen Schrägstrich im Namen aufweisen.

Führen Sie in Exchange 2010 den folgenden Befehl aus, um Öffentliche Ordner zu finden, deren Name einen Schrägstrich aufweist:

```
Get-PublicFolderStatistics -ResultSize Unlimited | Where {($_.Name -like "*\*") -or ($_.Name -like "*/*") } | Format-List Name,Identity
```

2. Wenn Öffentliche Ordner zurückgegeben werden, können Sie sie durch Ausführung des folgenden Befehls umbenennen:

```
Set-PublicFolder -Identity <public folder identity> -Name <new public folder name>
```

3. Stellen Sie sicher, dass es kein vorherigen Datensatz, der eine erfolgreiche Migration. Wenn vorhanden ist, müssen Sie legen Sie diesen Wert auf \$false . Wenn der Wert, um festgelegt ist \$true , die migrationsanforderung schlägt fehl.

Im folgenden Beispiel wird der Migrationsstatus der Öffentlichen Ordner überprüft.

```
Get-OrganizationConfig | Format-List PublicFoldersLockedforMigration,PublicFolderMigrationComplete
```

4. Wenn der Status der Eigenschaften *PublicFoldersLockedforMigration* oder *PublicFolderMigrationComplete* \$true , führen Sie den folgenden Befehl aus, um den Wert festzulegen \$false .

```
Set-OrganizationConfig -PublicFoldersLockedforMigration:$false -PublicFolderMigrationComplete:$false
```

Nachdem Sie diese Eigenschaften zurückgesetzt haben, müssen Sie warten, bis Exchange die neuen Einstellungen erkennt. Dies kann bis zu zwei Stunden dauern.

5. Zur Überprüfung am Ende der Migration sollten Sie zuerst die folgenden Exchange-Verwaltungsshell-Befehle auf dem Exchange-Legacyserver ausführen, um Momentaufnahmen der aktuellen Bereitstellung öffentlicher Ordner zu erstellen:

Führen Sie den folgenden Befehl aus, um eine Momentaufnahme der ursprünglichen Quellordnerstruktur zu erstellen.

```
Get-PublicFolder -Recurse | Export-CliXML C:\PFMigration\Legacy_PFStructure.xml
```

Führen Sie den folgenden Befehl aus, um eine Momentaufnahme der Statistikdaten von Öffentlichen Ordnern (wie Anzahl von Elementen, Größe und Besitzer) zu erstellen.

```
Get-PublicFolderStatistics -ResultSize Unlimited | Export-CliXML C:\PFMigration\Legacy_PFStatistics.xml
```

Führen Sie den folgenden Befehl aus, um eine Momentaufnahme der Berechtigungen zu erstellen.

```
Get-PublicFolder -Recurse | Get-PublicFolderClientPermission | Select-Object Identity,User -ExpandProperty AccessRights | Export-CliXML C:\PFMigration\Legacy_PFPerms.xml
```

Speichern Sie die Informationen aus den oben aufgeführten Befehlen, um am Ende der Migration einen Vergleich durchführen zu können.

6. Wenn Sie Microsoft Azure Active Directory Connect (Azure AD Connect) zum Synchronisieren Ihrer lokalen Verzeichnisse mit Azure Active Directory verwenden, müssen Sie Folgendes ausführen (wenn Sie nicht Azure AD Connect verwenden, können Sie diesen Schritt überspringen):

a. auf einem lokalen Computer öffnen Sie Microsoft Azure Active Directory verbinden, und wählen Sie dann auf **Konfigurieren**.

b. Klicken Sie auf dem Bildschirm **zusätzliche Aufgaben** wählen Sie **Anpassen Synchronisierungsoptionen aus**, und klicken Sie dann auf **Weiter**.

c. Klicken Sie auf dem Bildschirm **Verbindung mit Azure AD** Geben Sie die entsprechenden Anmeldeinformationen ein, und klicken Sie dann auf **Weiter**. Nachdem die Verbindung hergestellt ist, lassen Sie klicken auf **Weiter**, bis Sie auf dem Bildschirm **Optionale Features** sind.

d. stellen sicher, dass **Exchange Öffentliche E-Mail-Ordner** nicht aktiviert ist. Wenn sie nicht ausgewählt ist, können Sie mit dem nächsten Abschnitt, *in Office 365 oder Exchange Online erforderliche Schritte* fortfahren. Wenn es aktiviert ist, deaktivieren Sie das Kontrollkästchen, und klicken Sie dann auf **Weiter**.

#### NOTE

Wenn Sie **Öffentliche Exchange-E-Mail-Ordner** nicht als Option auf dem Bildschirm **Optionale Features** sehen, können Sie Microsoft Azure Active Directory Connect beenden und mit dem nächsten Abschnitt, *Erforderliche Schritte in Office 365 oder Exchange Online*, fortfahren.

7. Nachdem Sie die Option **Öffentliche Exchange-E-Mail-Ordner** deaktiviert haben, klicken Sie weiter auf **Weiter**, bis Sie sich auf dem Bildschirm **Bereit zur Konfiguration** befinden, und klicken Sie dann auf **Konfigurieren**.

Ausführliche Informationen zu Syntax und Parametern finden Sie in den folgenden Themen:

- [Neue AcceptedDomain](#)
- [Get-PublicFolder](#)
- [Get-PublicFolderDatabase](#)
- [Set-PublicFolder](#)
- [Get-publicfolderstatistics können](#)
- [Get-PublicFolderClientPermission](#)
- [Get-OrganizationConfig](#)
- [Set-OrganizationConfig](#)

**Erforderliche Schritte in Office 365 oder Exchange Online**

1. Stellen Sie sicher, dass keine Migrationsanforderungen für öffentliche Ordner vorhanden sind. Wenn sie vorhanden sind, löschen Sie sie, da es sonst zu einem Fehler mit Ihrer eigenen Migrationsanforderung kommt. Dieser Schritt ist nicht in allen Fällen erforderlich. Er ist nur erforderlich, wenn Sie glauben, dass in der Pipeline möglicherweise bereits eine Migrationsanforderung vorhanden ist.

Eine vorhandene Migrationsanforderung kann einen von zwei Typen haben: Batchmigration oder serielle Migration. Die Befehle zum Erkennen von Anforderungen für die einzelnen Typen und zum Entfernen von Anforderungen der einzelnen Typen sind nachfolgend aufgeführt.

**IMPORTANT**

Bevor Sie eine Migrationsanforderung entfernen, ist es wichtig zu verstehen, warum eine solche Anforderung vorhanden war. Durch das Ausführen der folgenden Befehle können Sie bestimmen, wann eine frühere Anforderung erstellt wurde. Dies ist nützlich, um möglicherweise aufgetretenen Probleme zu diagnostizieren. Sie müssen möglicherweise mit anderen Administratoren in Ihrer Organisation sprechen, um herauszufinden, warum die Änderung vorgenommen wurde.

Im folgenden Beispiel werden vorhandene serielle Migrationsanforderungen ermittelt.

```
Get-PublicFolderMigrationRequest | Get-PublicFolderMigrationRequestStatistics -IncludeReport | Format-List
```

Im folgenden Beispiel werden alle vorhandenen seriellen Migrationsanforderungen für öffentliche Ordner entfernt.

```
Get-PublicFolderMigrationRequest | Remove-PublicFolderMigrationRequest
```

Im folgenden Beispiel werden vorhandene Batchmigrationsanforderungen ermittelt.

```
$batch = Get-MigrationBatch | ?{$_MigrationType.ToString() -eq "PublicFolder"}
```

Im folgenden Beispiel werden alle vorhandenen Batchmigrationsanforderungen für öffentliche Ordner entfernt.

```
$batch | Remove-MigrationBatch -Confirm:$false
```

2. Stellen Sie sicher, dass in Office 365 keine öffentlichen Ordner oder öffentliche Ordner-Postfächer vorhanden sind.

#### IMPORTANT

Wenn in Office 365 öffentliche Ordner angezeigt werden, ist es wichtig herauszufinden, warum sie vorhanden sind, und wer in Ihrer Organisation eine öffentliche Ordner-Hierarchie gestartet hat, bevor Sie die öffentlichen Ordner oder öffentliche Ordner-Postfächer entfernen.

1. Führen Sie in Office 365 oder Exchange Online PowerShell den folgenden Befehl aus, um zu sehen, ob öffentliche Ordner-Postfächer vorhanden sind.

```
Get-Mailbox -PublicFolder
```

2. Wenn der Befehl keine Öffentlichen Ordner-Postfächer zurückgibt, fahren Sie mit [Schritt 3: Generieren der CSV-Dateien](#) fort. Wenn der Befehl Öffentliche Ordner-Postfächer zurückgibt, führen Sie den folgenden Befehl aus, um herauszufinden, ob Öffentliche Ordner vorhanden sind:

```
Get-PublicFolder
```

3. Wenn in Office 365 oder Exchange Online öffentliche Ordner vorhanden sind, entfernen Sie diese, indem Sie den folgenden PowerShell-Befehl ausführen. Stellen Sie sicher, dass Sie alle Informationen gespeichert haben, die sich in den öffentlichen Ordnern in Office 365 befanden. Alle in den öffentlichen Ordnern enthaltenen Informationen werden endgültig gelöscht, wenn Sie die öffentlichen Ordner entfernen.

```
Get-MailPublicFolder | where {$_.EntryId -ne $null} | Disable-MailPublicFolder -Confirm:$false  
Get-PublicFolder -GetChildren \ | Remove-PublicFolder -Recurse -Confirm:$false
```

4. Führen Sie, nachdem die öffentlichen Ordner entfernt wurden, die folgenden Befehle aus, um alle Postfächer für öffentliche Ordner zu entfernen.

```
$hierarchyMailboxGuid = $(Get-OrganizationConfig).RootPublicFolderMailbox.HierarchyMailboxGuid  
Get-Mailbox -PublicFolder:$true | Where-Object {$_.ExchangeGuid -ne $hierarchyMailboxGuid} | Remove-  
Mailbox -PublicFolder -Confirm:$false  
Get-Mailbox -PublicFolder:$true | Where-Object {$_.ExchangeGuid -eq $hierarchyMailboxGuid} | Remove-  
Mailbox -PublicFolder -Confirm:$false
```

Ausführliche Informationen zu Syntax und Parametern finden Sie in den folgenden Themen:

- [Get-MigrationBatch](#)
- [Get-PublicFolderMigrationRequest](#)
- [Remove-PublicFolderMigrationRequest](#)
- [Get-Mailbox](#)
- [Get-PublicFolder](#)
- [Get-MailPublicFolder](#)
- [Disable-MailPublicFolder](#)
- [Remove-PublicFolder](#)

- Remove-Mailbox

## Schritt 3: Generieren der CSV-Dateien

1. Führen Sie auf dem Exchange-Legacyserver die `Export-PublicFolderStatistics.ps1` Skript zum Erstellen der Ordner Namen zu Ordnergrößen Mapping-Datei. Dieses Skript muss immer durch einen lokalen Administrator ausgeführt werden. Die Datei enthält zwei Spalten: **FolderName** und **FolderSize**. Die Werte für die Spalte **FolderSize** werden in Bytes angezeigt. Beispielsweise `\PublicFolder01,10000`.

```
.\Export-PublicFolderStatistics.ps1 <Folder to size map path> <FQDN of source server>
```

- *FQDN of source server* entspricht dem vollqualifizierten Domänennamen des Postfachservers, auf dem die Hierarchie Öffentlicher Ordner gehostet wird.
- *Folder to size map path* entspricht dem Dateinamen und dem Pfad im freigegebenen Netzwerkordner, in dem Sie die CSV-Datei speichern möchten. Weiter unten in diesem Thema müssen Sie über die Exchange Online PowerShell auf diese Datei zugreifen. Wenn Sie nur den Dateinamen angeben, wird die Datei auf dem lokalen Computer im aktuellen PowerShell-Verzeichnis generiert.
- Falls erforderlich, entfernen Sie alle E-Mail-aktivierten Systemordner aus der Skriptausgabe, bevor Sie fortfahren.

2. Führen Sie die `PublicFolderToMailboxMapGenerator.ps1` Skript zum Erstellen der Öffentliche Ordner-Postfach-Zuordnungsdatei. Diese Datei wird verwendet, um die richtige Anzahl der Postfächer für Öffentliche Ordner in Exchange Online zu berechnen.

```
.\PublicFolderToMailboxMapGenerator.ps1 <Maximum mailbox size in bytes> <Folder to size map path>
<Folder to mailbox map path>
```

### IMPORTANT

Die Datei zur Zuordnung von öffentlichen Ordner zu Postfächern sollte 1.000 Zeilen nicht überschreiten. Wenn diese Datei 1.000 Zeilen überschreitet, muss die Struktur des öffentlichen Ordners vereinfacht werden. Das Fortfahren mit einer Datei von als 1.000 Zeilen wird nicht empfohlen, dabei kann es zu Migrationsfehlern kommen.

- Verwenden Sie vor dem Ausführen des Skripts den folgenden Befehl, um die aktuelle Begrenzungen für Öffentliche Ordner in Exchange Online-Mandanten zu überprüfen. Notieren Sie die aktuellen Kontingentwerte für Öffentliche Ordner an.

```
Get-OrganizationConfig | Format-List *quota*
```

Der Standardwert in Exchange Online ist 1,7 GB für **DefaultPublicFolderIssueWarningQuota** und 2 GB für **DefaultPublicFolderProhibitPostQuota**.

- *Maximum mailbox size in bytes* entspricht der maximalen Größe, die Sie für neue Postfächer für öffentliche Ordner festlegen möchten. Die maximale Größe von Postfächern für öffentliche Ordner in Exchange Online beträgt 100 GB. Es wird empfohlen, diese Einstellung auf 15 GB festzulegen, sodass das Anwachsen aller Öffentliche Ordner-Postfächer unterstützt wird. Exchange Online verfügt über ein Standardkontingent „Bereitstellen verbieten“ von 2 GB. Wenn Sie einzelne öffentliche Ordner besitzen, die größer als 2 GB sind, können Sie eine der folgenden Optionen verwenden, um dieses Problem zu beheben:

- Bevor Sie den migrationsbatch zu starten, erhöhen Sie das standardmäßige Kontingent für Öffentliche Ordner "Bereitstellen verbieten" mithilfe des folgenden Befehls:

```
Set-OrganizationConfig -DefaultPublicFolderProhibitPostQuota <size value> -
DefaultPublicFolderIssueWarningQuota <size value>
```

- Vor dem Start des Migrationsbatches löschen Sie die Inhalte des öffentlichen Ordners, um die Inhaltsgröße auf 2 GB oder weniger zu reduzieren.
- Teilen Sie vor dem Start des Migrationsbatches den öffentlichen Ordner in mehrere öffentliche Ordner auf, die jeweils maximal 2 GB groß sind.

**NOTE**

Wenn der öffentliche Ordner größer als 30 GB ist und das Löschen von Inhalten oder das Aufteilen in mehrere öffentliche Ordner nicht möglich ist, wird empfohlen, die öffentlichen Ordner nicht zu Exchange Online zu verschieben.

- *Folder to Size Map Path* entspricht den Dateipfad der CSV-Datei, die Sie erstellt haben, bei der Ausführung der `Export-PublicFolderStatistics.ps1` Skript.
- *Folder to mailbox map path* entspricht dem Dateinamen und -pfad der .csv-Datei für die Zuordnung von Ordnern zu Postfächern, die Sie in diesem Schritt erstellen. Wenn Sie nur den Dateinamen angeben, wird die Datei auf dem lokalen Computer im aktuellen PowerShell-Verzeichnis generiert.

**NOTE**

Nachdem die Skripts ausgeführt und die csv.-Dateien erstellt wurden, werden keine neuen öffentlichen Ordner oder Updates für vorhandene öffentliche Ordner erfasst.

## Schritt 4: Erstellen der Öffentliche Ordner-Postfächer in Exchange Online

Führen Sie den folgenden Befehl zum Ziel Postfächer für Öffentliche Ordner zu erstellen. Das Skript erstellt eine Zielpostfach für jedes Postfach in der CSV-Datei, die Sie zuvor in Schritt 3 durch Ausführen von generiert die `PublicFoldertoMailboxMapGenerator.ps1` Skript.

```
.\Create-PublicFolderMailboxesForMigration.ps1 -FolderMappingCsv Mapping.csv -
EstimatedNumberOfConcurrentUsers:<estimate>
```

*Mapping.csv* ist die Datei generiert von der `PublicFoldertoMailboxMapGenerator.ps1` Skript in Schritt 3. Die geschätzte Anzahl der gleichzeitigen benutzerverbindungen Durchsuchen einer Hierarchie Öffentlicher Ordner ist in der Regel kleiner als die Gesamtzahl der Benutzer in einer Organisation.

## Schritt 5: Starten der Migrationsanforderung

1. Führen Sie auf dem älteren Exchange-Server den folgenden Befehl zum Synchronisieren von für E-Mail aktivierten öffentlichen Ordnern vom lokalen Active Directory mit Exchange Online aus.

```
.\Sync-MailPublicFolders.ps1 -Credential (Get-Credential) -CsvSummaryFile:sync_summary.csv
```

`Credential` ist Office 365-Benutzernamen und Ihr Kennwort ein. `CsvSummaryFile` ist der Dateipfad an, in dem Sie darüber melden möchten. CSV-Format, Synchronisierungsvorgänge und Fehler.

#### NOTE

Es wird empfohlen, dass Sie zuerst die Aktionen simulieren, der das Skript vor der tatsächlich Ausführung, was Sie durch Ausführen des Skripts mit möglich führt eine `-WhatIf` Parameter.

2. Rufen Sie auf dem Exchange-Legacyserver die folgenden Informationen ab, die zur Ausführung der Migrationsanforderung erforderlich sind:

- a. Hier finden Sie die `LegacyExchangeDN` von das Konto des Benutzers, der ein Mitglied der Administratorrolle für Öffentliche Ordner ist. Dies ist derselbe Benutzer wird, dessen Anmeldeinformationen, die Sie in Schritt 3 dieses Verfahrens benötigen.

```
Get-Mailbox <PublicFolder_Administrator_Account> | Select-Object LegacyExchangeDN
```

- b. Suchen Sie nach der `LegacyExchangeDN` eines Postfachservers, der Öffentliche Ordner-Datenbank verfügt.

```
Get-ExchangeServer <public folder server> | Select-Object -Expand ExchangeLegacyDN
```

- c. Suchen Sie den FQDN des Outlook Anywhere-Hostnamens. Wenn Sie mehrere Instanzen von Outlook Anywhere haben, wird empfohlen, die Instanz auszuwählen, die dem Migrationsendpunkt oder den Replikaten Öffentlicher Order in der Legacy-Exchange-Organisation am nächsten ist. Mit dem folgenden Befehl werden alle Instanzen von Outlook Anywhere gefunden:

```
Get-OutlookAnywhere | Format-Table Identity,ExternalHostName
```

3. Führen Sie in der Office 365 PowerShell die folgenden Befehle aus, um die im vorherigen Schritt zurückgegebenen Informationen an Variablen weiterzugeben, die dann in der Migrationsanforderung verwendet werden.

- a. Übergeben Sie die Anmeldeinformationen eines Benutzers mit auf dem Exchange-Legacyserver in die Variable Administratorrechten `$Source_Credential`. Die migrationsanforderung, die in Exchange Online ausgeführt hat wird dieser Anmeldeinformationen verwenden, um Zugriff auf Ihre Exchange-Legacyservern, über den Inhalt zu kopieren.

```
$Source_Credential = Get-Credential <source_domain\PublicFolder_Administrator_Account>
```

- b. Verwendung der `ExchangeLegacyDN` des Migrationsbenutzers auf dem Exchange-Legacyserver, dass Sie in Schritt 2a gefunden haben, und geben Sie ihn an die Variable `$Source_RemoteMailboxLegacyDN`.

```
$Source_RemoteMailboxLegacyDN = "<paste the value here>"
```

- c. Verwendung der `ExchangeLegacyDN` des öffentlichen ordnerservers, dass Sie in Schritt 2 b oben gefunden haben, und geben Sie ihn an die Variable `$Source_RemotePublicFolderServerLegacyDN`.

```
$Source_RemotePublicFolderServerLegacyDN = "<paste the value here>"
```

- d. Verwenden Sie die externen Host von Outlook Anywhere, dass Sie in Schritt 2c oben gefunden haben, und geben Sie ihn an die Variable `$Source_OutlookAnywhereExternalHostName`.

```
$Source_OutlookAnywhereExternalHostName = "<paste the value here>"
```

4. Führen Sie abschließend in der Exchange Online PowerShell die folgenden Befehle aus, um die Migrationsanforderung zu erstellen.

**NOTE**

Die Authentifizierungsmethode im folgenden Exchange-Verwaltungsshell-Beispiel muss mit Ihren Outlook Anywhere-Einstellungen übereinstimmen. Andernfalls tritt beim Ausführen des Befehls ein Fehler auf.

```
$PfEndpoint = New-MigrationEndpoint -PublicFolder -Name PublicFolderEndpoint -RPCProxyServer $Source_OutlookAnywhereExternalHostName -Credentials $Source_Credential -SourceMailboxLegacyDN $Source_RemoteMailboxLegacyDN -PublicFolderDatabaseServerLegacyDN $Source_RemotePublicFolderServerLegacyDN -Authentication Basic [byte[]]$bytes = Get-Content -Encoding Byte <folder_mapping.csv> New-MigrationBatch -Name PublicFolderMigration -CSVData $bytes -SourceEndpoint $PfEndpoint.Identity - NotificationEmails <email addresses for migration notifications>
```

In dem die `< folder_mapping.csv >` ist die Datei, die bei generiert wurde [Schritt 3: generieren die CSV-Dateien](#).

5. Starten Sie die Migration mit dem folgenden Befehl:

```
Start-MigrationBatch PublicFolderMigration
```

Obwohl die Batchmigrationen mit dem **New-MigrationBatch**-Cmdlet in der Exchange-Verwaltungsshell erstellt werden müssen, können Status und Fertigstellung der Migration in EAC angezeigt und verwaltet werden. Da das **New-MigrationBatch**-Cmdlet eine Postfachmigrationsanforderung für jedes Postfach für öffentliche Ordner initiiert, können Sie den Status dieser Anforderungen mithilfe der Seite für die Postfachmigration anzeigen. Sie können zur Seite für die Postfachmigration wechseln und Migrationsberichte erstellen, die Ihnen per E-Mail gesendet werden können, indem Sie Folgendes vornehmen:

1. Melden Sie sich bei Exchange Online an, und öffnen Sie EAC.
2. Navigieren Sie zu **Postfach > Migration**.
3. Wählen Sie die soeben erstellte Migrationsanforderung aus, und klicken Sie im Bereich **Details** auf **Details anzeigen**.

Ausführliche Informationen zu Syntax und Parametern finden Sie in den folgenden Themen:

- [Get-Mailbox](#)
- [Get-ExchangeServer](#)
- [Get-OutlookAnywhere](#)
- [New-PublicFolderMigrationRequest](#)
- [Get-PublicFolderDatabase](#)
- [Get-PublicFolderMigrationRequest](#)
- [Get-PublicFolderMigrationRequestStatistics](#)

## Schritt 6: Sperren der Öffentlichen Ordner auf dem Exchange-Legacyserver für die endgültige Migration (Ausfallzeit erforderlich)

Bis zu diesem Zeitpunkt im Migrationsprozess konnten Benutzer auf Öffentliche Ordner zugreifen. In den nächsten Schritten werden die Benutzer von den älteren Öffentlichen Ordner abgemeldet, und die Ordner werden gesperrt, bis die abschließende Synchronisierung im Rahmen des Migrationsvorgangs beendet ist. Während dieses Vorgangs können die Benutzer nicht auf Öffentliche Ordner zugreifen. Außerdem werden alle E-Mails, die an E-Mail-aktivierte Öffentliche Ordner gesendet werden, in die Warteschlange gestellt und erst nach Abschluss der Öffentlichen Ordner-Migration übermittelt.

Vor dem Ausführen der `Set-OrganizationConfig -PublicFoldersLockedForMigration $true` Befehl wie unten beschrieben, stellen Sie sicher, dass alle Aufträge im Zustand **synchronisiert** werden. Hierzu können Sie mit der `Get-PublicFolderMailboxMigrationRequest` Befehl. Fahren Sie mit diesen Schritt nur aus, nachdem Sie sichergestellt haben, dass alle Aufträge im Zustand **synchronisiert** werden.

Führen Sie auf dem Exchange-Legacyserver den folgenden Befehl aus, um die älteren Öffentlichen Ordner bis zum Abschluss des Vorgangs zu sperren.

```
Set-OrganizationConfig -PublicFoldersLockedForMigration:$true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [set-OrganizationConfig](#).

Wenn Ihre Organisation mehrere Datenbanken für Öffentliche Ordner verfügt, müssen Sie warten, bis die Replikation Öffentlicher Ordner zu bestätigen, dass alle Datenbanken für Öffentliche Ordner aufgenommene haben abgeschlossen ist die `Set-OrganizationConfig -PublicFoldersLockedForMigration $true` Flag und alle ausstehenden Änderungen, die Benutzer auf Ordner kürzlich vorgenommen haben in der gesamten Organisation zusammengeführt. Dies kann mehrere Stunden dauern.

## Schritt 7: Schließen Sie die Migration öffentlicher Ordner ab (Ausfallzeit erforderlich)

Führen Sie zum Abschließen der Migration für öffentliche Ordner den folgenden Befehl aus:

```
Complete-MigrationBatch PublicFolderMigration
```

Nach Abschluss die Migration führt Exchange eine endgültige Synchronisierung zwischen dem Legacy-Exchange-Server und Exchange Online durch. Ist die abschließende Synchronisierung erfolgreich, werden die öffentlichen Ordner auf dem Exchange Online-Server entsperrt, und der Status des Migrationsbatches wird in **Wird abgeschlossen** und dann in **Abgeschlossen** geändert. In der Regel dauert es einige Stunden, bis der Status des Migrationsbatches von **Synchronisiert** in **Wird abgeschlossen** geändert wird. Erst dann beginnt die abschließende Synchronisierung.

Wenn Sie eine Hybridbereitstellung zwischen Ihren lokalen Exchange-Servern und Office 365 konfiguriert haben, müssen Sie den folgenden Befehl in Exchange Online PowerShell ausführen, nachdem die Migration abgeschlossen ist:

```
Set-OrganizationConfig -RemotePublicFolderMailboxes $Null -PublicFoldersEnabled Local
```

## Schritt 8: Testen und Entsperren der Migration Öffentlicher Ordner

Nachdem Sie die Migration Öffentlicher Ordner abgeschlossen haben, sollten Sie den folgenden Test durchführen und so sicherstellen, dass die Migration erfolgreich war. Dadurch können Sie die Hierarchie der

migrierten öffentlichen Ordner testen, bevor Sie auf die Verwendung von öffentlichen Ordnern in Office 365 oder Exchange Online umstellen.

1. Weisen Sie in Office 365 oder Exchange Online PowerShell einige Testpostfächer so zu, dass sie als das Standardpostfach für öffentliche Ordner ein neu migriertes Postfach für öffentliche Ordner verwenden.

```
Set-Mailbox -Identity <Test User> -DefaultPublicFolderMailbox <Public Folder Mailbox Identity>
```

2. Melden Sie sich auf Outlook 2010 oder höher mit dem im vorherigen Schritt identifizierten Testbenutzer, und führen Sie die folgenden Tests für Öffentliche Ordner durch:

- Zeigen Sie die Hierarchie an.
- Prüfen Sie die Berechtigungen.
- Erstellen und löschen Sie Öffentliche Ordner.
- Veröffentlichen Sie Inhalte in einem Öffentlichen Ordner, und löschen Sie diese.

3. Wenn Probleme auftreten, lesen Sie [Durchführen eines Rollbacks der Migration](#) weiter unten in diesem Thema. Wenn der Inhalt und die Hierarchie des öffentlichen Ordners akzeptabel sind und wie erwartet funktionieren, fahren Sie mit dem nächsten Schritt fort.

4. Führen Sie auf dem Exchange-Legacyserver den folgenden Befehl aus, um anzugeben, dass die Migration der Öffentlichen Ordner abgeschlossen ist.

```
Set-OrganizationConfig -PublicFolderMigrationComplete:$true
```

5. Nachdem Sie sichergestellt haben, dass die Migration abgeschlossen ist, führen Sie den folgenden Befehl in Exchange Online PowerShell, um sicherzustellen, dass der Parameter *PublicFoldersEnabled* gibt für **Set-OrganizationConfig**, um festgelegt ist `Local` :

```
Set-OrganizationConfig -PublicFoldersEnabled Local
```

Ausführliche Informationen zu Syntax und Parametern finden Sie in den folgenden Themen:

[Set-Mailbox](#)

[Get-Mailbox](#)

[Set-OrganizationConfig](#)

## Woher weiß ich, dass der Vorgang erfolgreich war?

Unter [Schritt 2: Vorbereiten der Migration](#) wurden Sie aufgefordert, Momentaufnahmen der Struktur Öffentlicher Ordner, der Statistikdaten und der Berechtigungen vor der Migration zu erstellen. Mit den folgenden Schritten können Sie überprüfen, ob die Migration Öffentlicher Ordner erfolgreich war, indem Sie die gleichen Momentaufnahmen nach Abschluss der Migration erstellen. Sie können dann die Daten in beiden Dateien vergleichen, um den Erfolg zu überprüfen.

1. Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um eine Momentaufnahme der neuen Ordnerstruktur zu erstellen.

```
Get-PublicFolder -Recurse | Export-CliXML C:\PFMigration\Cloud_PFStructure.xml
```

2. Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um eine Momentaufnahme der Statistikdaten von Öffentlichen Ordnern (wie Anzahl von Elementen, Größe und Besitzer) zu erstellen.

```
Get-PublicFolderStatistics -ResultSize Unlimited | Export-CliXML C:\PfMigration\Cloud_PFStatistics.xml
```

3. Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um eine Momentaufnahme der Berechtigungen zu erstellen.

```
Get-PublicFolder -Recurse | Get-PublicFolderClientPermission | Select-Object Identity,User -ExpandProperty AccessRights | Export-CliXML C:\PfMigration\Cloud_PFPerms.xml
```

## Entfernen von Datenbanken für Öffentliche Ordner von den Exchange-Legacyservern

Nachdem die Migration abgeschlossen wurde und Sie sichergestellt haben, dass die Öffentlichen Exchange Online-Ordner erwartungsgemäß funktionieren, sollten Sie die Datenbanken für Öffentliche Ordner auf den Exchange-Legacyservern entfernen.

### IMPORTANT

Da all Ihre Postfächer vor der Migration der öffentlichen Ordner in Office 365 migriert wurden, wird dringend empfohlen, den Datenverkehr über Office 365 (dezentraler E-Mail-Verkehr) statt zentral über Ihre lokale Umgebung zu leiten. Wenn Sie den zentralen E-Mail-Verkehr beibehalten möchten, kann es zu Zustellproblemen bei Ihren öffentlichen Ordner kommen, da Sie die Postfachdachtenbanken des öffentlichen Ordners aus Ihrer lokalen Organisation entfernt haben.

- Nähere Informationen zum Entfernen von Öffentliche Ordner-Datenbanken von Exchange 2010-Servern finden Sie unter [Entfernen von Öffentliche Ordner-Datenbanken](#).

## Durchführen eines Rollbacks der Migration

Wenn bei der Migration Probleme auftreten und Sie die Öffentlichen Ordner von einem Exchange-Legacyserver erneut aktivieren müssen, führen Sie die folgenden Schritte aus.

### Caution

Wenn Sie ein Rollback der Migration auf die Exchange-Legacyserver durchführen, gehen alle E-Mails verloren, die an E-Mail-aktivierte Öffentliche Ordner gesendet wurden, sowie Inhalte, die nach der Migration in Öffentlichen Ordnern bereitgestellt wurden. Um diese Inhalte zu speichern, müssen Sie die Inhalte der öffentlichen Ordner in einer PST-Datei speichern und diese dann nach Abschluss des Rollbacks in die älteren öffentlichen Ordner importieren.

1. Führen Sie auf dem Exchange-Legacyserver den folgenden Befehl aus, um die älteren Öffentlichen Exchange-Ordner zu entsperren. Dieser Vorgang kann mehrere Stunden in Anspruch nehmen.

```
Set-OrganizationConfig -PublicFoldersLockedForMigration:$False
```

2. Führen Sie in Exchange Online PowerShell die folgenden Befehle aus, um alle Öffentlichen Exchange Online-Ordner zu entfernen.

```
$hierarchyMailboxGuid = $(Get-OrganizationConfig).RootPublicFolderMailbox.HierarchyMailboxGuid  
Get-Mailbox -PublicFolder:$true | Where-Object {$_._ExchangeGuid -ne $hierarchyMailboxGuid} | Remove-  
Mailbox -PublicFolder -Confirm:$false -Force  
Get-Mailbox -PublicFolder:$true | Where-Object {$_._ExchangeGuid -eq $hierarchyMailboxGuid} | Remove-  
Mailbox -PublicFolder -Confirm:$false -Force
```

3. Führen Sie auf dem Exchange-Legacyserver den folgenden Befehl zum Festlegen der `PublicFolderMigrationComplete` flag auf `$false`.

```
Set-OrganizationConfig -PublicFolderMigrationComplete:$False
```

## Migrieren von Öffentlichen Ordnern zu Office 365 mit PST-Export von Outlook

Es wird empfohlen, nicht das PST-Exportfeature von Outlook zum Migrieren öffentlicher Ordner zu Office 365 oder Exchange Online zu verwenden, wenn die Hierarchie der öffentlichen Ordner mehr als 30 GB umfasst. Das Anwachsen des Postfachs für öffentliche Ordner in Office 365 wird über ein Feature zur automatischen Aufteilung verwaltet, welches das Postfach für öffentliche Ordner aufteilt, wenn Größenkontingente überschritten werden. Das plötzliche Anwachsen der Postfächer für Öffentliche Ordner kann nicht von der automatischen Aufteilung verwaltet werden, wenn Sie Öffentliche Ordner über den PST-Export migrieren. Sie müssen dann möglicherweise bis zu zwei Wochen warten, bis die Daten durch automatische Aufteilung aus dem primären Postfach verschoben werden. Zudem sollten Sie Folgendes bedenken, bevor Sie den PST-Export von Outlook verwenden, um öffentliche Ordner zu Office 365 oder Exchange Online zu exportieren:

- Berechtigungen für Öffentliche Ordner gehen während dieses Vorgangs verloren. Erfassen Sie die aktuellen Berechtigungen vor der Migration, und fügen Sie sie nach der Migration manuell hinzu.
- Wenn Sie komplexe Berechtigungen verwenden oder viele Ordner zu migrieren haben, sollten Sie die Cmdlet-Methode zur Migration verwenden.
- Alle Änderungen an Elementen und Ordnern, die während der PST-Exportmigration an den Öffentlichen Quellordnern vorgenommen werden, gehen verloren. Daher wird empfohlen, die Cmdlet-Methode zu verwenden, wenn diese Export- und Importvorgänge lange dauern.

Wenn Sie Ihre Öffentlichen Ordner dennoch mithilfe von PST-Dateien migrieren möchten, sollten Sie die folgenden Schritte ausführen, um eine erfolgreiche Migration sicherzustellen.

1. Verwenden Sie die Anweisungen in [Schritt 1: Herunterladen der Migrationsskripts](#) zum Herunterladen der Migrationsskripts. Sie müssen nur zum Herunterladen der `PublicFolderToMailboxMapGenerator.ps1` Datei.
2. Führen Sie Schritt 2 von [Schritt 3: Generieren der CSV-Dateien](#) aus, um die Datei zur Zuordnung von Öffentlichen Ordnern zu Postfächern zu erstellen. Diese Datei wird verwendet, um die richtige Anzahl von Postfächern für Öffentliche Ordner in Exchange Online zu berechnen.
3. Erstellen Sie die Postfächer für Öffentliche Ordner, die Sie benötigen, basierend auf die Datei zur Zuordnung. Weitere Informationen finden Sie unter [Erstellen eines Postfachs für Öffentliche Ordner](#).
4. Verwenden Sie das Cmdlet **[New-PublicFolder]**, öffentlichen Ordner den obersten mithilfe des Parameters `Mailbox` aller Postfächer für Öffentliche Ordner zu erstellen.
5. Exportieren und importieren Sie die PST-Dateien mithilfe von Outlook.
6. Legen Sie die Berechtigungen für die öffentlichen Ordner mithilfe der Exchange-Verwaltungskonsole. Weitere Informationen finden Sie [Schritt 3: Zuweisen von Berechtigungen auf den öffentlichen Ordner](#) im Thema [Einrichten öffentlicher Ordner in einer neuen Organisation](#).

#### **Caution**

Wenn Sie bereits eine PST-Migration gestartet haben ausgeführt, und haben ein Problem, in dem das primäre Postfach voll ist, haben Sie zwei Optionen für die Wiederherstellung der PST-Migrations: > warten, bis die automatische Split-Daten aus dem Hauptpostfach verschieben. Dies kann bis zu zwei Wochen dauern. Jedoch werden nicht alle öffentlichen Ordner in einem Postfach vollständig gefüllten Öffentliche Ordner neuen Inhalte empfangen, bis die Auto-Teilung abgeschlossen ist. > [Erstellen eines Postfachs für Öffentliche Ordner](#) und dann verwenden Sie das Cmdlet **[New-PublicFolder]** mit dem Parameter *Mailbox* die verbleibenden Öffentlichen Ordner im Postfach sekundären Öffentliche Ordner zu erstellen. Dieses Beispiel erstellt einen neuen öffentlichen Ordner mit dem Namen PF201 im sekundären Öffentliche Ordner-Postfach.

# Migrieren von Exchange 2013-basierten öffentlichen Ordnern zu Exchange Online mithilfe einer Batchmigration

18.12.2018 • 51 minutes to read

**Zusammenfassung:** In diesem Artikel erfahren Sie, wie Sie moderne öffentliche Ordner von Exchange 2013 nach Office 365 verschieben.

Migrieren von Exchange 2013 öffentlicher Ordner zu Exchange Online erfordert Exchange Server 2013 CU15 oder höher, in Ihrer lokalen Umgebung ausgeführt.

## NOTE

Wenn Sie Exchange 2013 und Exchange 2016 Öffentliche Ordner in Ihrer Organisation haben, und Sie alle zu Exchange Online verschieben möchten, verwenden Sie [die Exchange-2016-Version dieses Artikels](#) zur Planung und Durchführung der Migrations. Exchange 2013-Servern müssen weiterhin CU15 haben oder höher installiert sein.

## Was sollten Sie wissen, bevor Sie beginnen?

- Wenn Sie auf Exchange Server 2013 CU15 oder höher aktualisieren, müssen Sie auch Active Directory vorbereiten. Ansonsten schlägt die Migration Ihrer öffentlichen Ordner fehl. Durch die Active Directory-Vorbereitung wird sichergestellt, dass alle relevanten PowerShell-Cmdlets und -Parameter verfügbar sind, die Sie zur Vorbereitung und Durchführung der Migration benötigen. Weitere Informationen finden Sie unter [Prepare Active Directory and Domains](#).
- In Exchange Online müssen Sie Mitglied der Rollengruppe "Organisationsverwaltung" sein. Dieser Rollengruppe unterscheidet sich von den Berechtigungen, die Ihnen zugewiesen werden, wenn Sie Office 365 oder Exchange Online abonnieren. Ausführliche Informationen zum Aktivieren der Rollengruppe "Organisationsverwaltung" finden Sie unter [Manage Role Groups](#).
- In Exchange müssen Server 2013, Sie ein Mitglied der Organization Management oder Server Management RBAC-Rollengruppen sein. Weitere Informationen hierzu finden Sie unter [Hinzufügen von Mitgliedern zu einer Rollengruppe](#).
- Vor Beginn der Migration Ihrer öffentlichen Ordner empfehlen wir Folgendes: Falls ein öffentlicher Ordner in Ihrer Organisation größer als 25 GB ist, sollten Sie Inhalte aus diesem Ordner löschen, um ihn zu verkleinern, oder seine Inhalte auf mehrere kleinere öffentliche Ordner verteilen. Beachten Sie, dass der hier genannte Grenzwert von 25 GB nur für den öffentlichen Ordner selbst gilt, nicht für möglicherweise vorhandene untergeordnete Ordner oder Unterordner des Ordners. Wenn keine dieser Möglichkeiten infrage kommt, empfehlen wir Ihnen, von einer Verschiebung Ihrer öffentlichen Ordner nach Exchange Online abzusehen. Weitere Informationen finden Sie unter [Exchange Online-Begrenzungen](#).

## NOTE

Wenn Ihre aktuellen Kontingente für öffentliche Ordner in Exchange Online kleiner als 25 GB sind, können Sie sie mithilfe der Parameter „DefaultPublicFolderIssueWarningQuota“ und „DefaultPublicFolderProhibitPostQuota“ des Cmdlets [Set-OrganizationConfig](#) vergrößern.

- In Office 365 und Exchange Online können Sie maximal 1.000 Postfächer für öffentliche Ordner erstellen.
- Wenn Sie Benutzer zu Office 365 migrieren möchten, sollten Sie die Benutzermigration vor der Migration Ihrer öffentlichen Ordner abschließen. Weitere Informationen finden Sie unter [Methoden zum Migrieren mehrerer E-Mail-Konten zu Office 365](#).
- MRS-Proxy muss auf mindestens ein Exchange-Server einen Server aktiviert werden, die auch Postfächer für Öffentliche Ordner gehostet wird. Einzelheiten finden Sie unter [Aktivieren der Endpunkt des Anwendungsproxys MRS für Remote verschiebt](#).
- Zum Ausführen der Migrationsverfahren in diesem Artikel nicht im Exchange Administrationscenter (EAC) verwendet werden. Stattdessen müssen Sie die Exchange-Verwaltungsshell auf Ihren Exchange 2013 Servern zu verwenden. In Exchange Online müssen Sie Exchange Online PowerShell verwenden. Weitere Informationen finden Sie unter [Connect to Exchange Online PowerShell](#).
- Die Migration gelöschter Elemente und gelöschter Ordner von Exchange 2013 zu Exchange Online wird unterstützt. Wir empfehlen Ihnen, vor Beginn der Migration alle gelöschten Ordner und Ordnerelemente zu überprüfen und alle Ordner und Elemente, die Sie in Exchange Online nicht benötigen, endgültig zu löschen. Beachten Sie: Sobald ein Element endgültig gelöscht wurde, kann es nicht wiederhergestellt werden.

Mithilfe der folgenden Befehle können Sie eine Liste aller gelöschten öffentlichen Ordner im Exchange-Dumpster (in Ihrer lokalen Exchange-Umgebung) aufrufen:

```
Get-PublicFolder \NON_IPM_SUBTREE\DUMPSTER_ROOT -Recurse | ?{$_._FolderClass -ne "$null"} | ft name,foldersize
```

Zum endgültigen Löschen eines bestimmten Ordners (in diesem Beispiel ein Ordner namens „Calendar2“) können Sie den folgenden Befehl verwenden:

```
Get-PublicFolder \NON_IPM_SUBTREE\DUMPSTER_ROOT -Recurse | ?{$_._FolderClass -ne "$null" -and $_._Name -eq "Calendar2"} | Remove-PublicFolder
```

- Sie müssen einen einzelnen migrationsbatch verwenden, um alle Daten Ihrer öffentlichen Ordner zu migrieren. Exchange kann nur einen migrationsbatch zu einem Zeitpunkt erstellen. Wenn Sie versuchen, die gleichzeitig mehrere migrationsbatch zu erstellen, wird das Ergebnis ein Fehler.
- Lesen Sie sich diesen Artikel vollständig durch, bevor Sie beginnen. Einige Schritte erfordern Downtime. Während dieser Downtime kann niemand auf die öffentlichen Ordner zugreifen.

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Schritt 1: Herunterladen der Migrationsskripts

1. Laden Sie alle Skripts und Unterstützungsdateien unter [Exchange 2013/2016 Public Folders Migration Scripts](#) herunter.
2. Speichern Sie die Skripts auf dem lokalen Computer, auf dem Sie PowerShell ausführen. Verwenden Sie als Speicherort beispielsweise C:\PFSscripts. Stellen Sie sicher, dass alle Skripts unter demselben Speicherort gespeichert werden.

Es werden folgende Skripts und Dateien heruntergeladen:

- `Sync-ModernMailPublicFolders.ps1` : Mit diesem Skript werden e-Mail-aktivierte Öffentliche Ordner-Objekte zwischen Ihrer lokalen Umgebung Exchange und Office 365 synchronisiert. Sie müssen dieses Skript auf einem Exchange 2013-Server ausführen.
- `SyncModernMailPublicFolders.strings.psd1` : Diese Unterstützungsdatei wird durch das Sync-ModernMailPublicFolders.ps1 Skript verwendet und sollte an denselben Speicherort heruntergeladen werden.
- `Export-ModernPublicFolderStatistics.ps1` : Dieses Skript erstellt die Größe des Ordners Ordner Name und gelöschte Elemente Größe Zuordnungsdatei. Sie müssen dieses Skript auf dem Exchange 2013-Server ausführen.
- `Export-ModernPublicFolderStatistics.strings.psd1` : Diese Unterstützungsdatei wird vom Export-ModernPublicFolderStatistics.ps1 Skript verwendet und sollte an denselben Speicherort heruntergeladen werden.
- `ModernPublicFolderToMailboxMapGenerator.ps1` : Dieses Skript erstellt die Datei zur Zuordnung von öffentlichen Ordner zu Postfächern anhand der Ausgabe des Skripts Export-ModernPublicFolderStatistics.ps1. Sie müssen dieses Skript auf einem Exchange 2013-Server ausführen.
- `ModernPublicFolderToMailboxMapGenerator.strings.psd1` : Diese Unterstützungsdatei wird vom ModernPublicFolderToMailboxMapGenerator.ps1 Skript verwendet und sollte an denselben Speicherort heruntergeladen werden.
- `SetMailPublicFolderExternalAddress.ps1` : Aktualisiert dieses Skript `ExternalEmailAddress` der e-Mail-aktivierten Öffentlichen Ordner in Ihrer lokalen Umgebung, die von den entsprechenden Exchange Online. Dadurch wird sichergestellt, dass nach der Migration-e-Mails an e-Mail-aktivierten Öffentlichen Ordner adressiert ordnungsgemäß zu Exchange Online weitergeleitet werden. Sie müssen dieses Skript auf einem Exchange 2013-Server ausgeführt.
- `SetMailPublicFolderExternalAddress.strings.psd1` : Diese Unterstützungsdatei wird vom SetMailPublicFolderExternalAddress.ps1 Skript verwendet und sollte an denselben Speicherort heruntergeladen werden.

## Schritt 2: Vorbereiten der Migration

Führen Sie alle erforderlichen Schritte durch, die in den folgenden Abschnitten beschrieben sind, bevor Sie mit der Migration Ihrer öffentlichen Ordner beginnen.

### Allgemeine erforderliche Schritte

Damit Ihre Migration gelingt, sollten Sie Folgendes tun:

- Stellen Sie sicher, dass in Active Directory keine verwaisten E-Mail-Objekte aus öffentlichen Ordnern vorhanden sind (d. h. Objekte in Active Directory, die kein Exchange-Objekt als Gegenstück haben).
- Vergewissern Sie sich, dass die für die öffentlichen Ordner in Active Directory konfigurierten SMTP-E-Mail-Adressen mit den SMTP-E-Mail-Adressen der Exchange-Objekte übereinstimmen.
- Stellen Sie sicher, dass keine doppelten Objekte des Typs „Öffentlicher Ordner“ in Active Directory vorhanden sind. Das ist nötig, damit nicht zwei oder mehr Active Directory-Objekte auf denselben E-Mail-aktivierten öffentlichen Ordner verweisen.

### Erforderliche Schritte in der lokalen Exchange 2013-Serverumgebung

In der Exchange-Verwaltungsshell (lokal) führen Sie die folgenden Schritte aus:

1. Nach Abschluss die Migration dauert eine Weile DNS-Caches über das Internet auf direkte Nachrichten auf Ihre e-Mail-aktivierten Öffentlichen Ordner in die neue Position im Exchange Online es. Sie können

sicherstellen, dass Ihre neu migrierte e-Mail-aktivierten Öffentlichen Ordner diesem Zeitraum Übergang DNS-Nachrichten empfangen, durch Erstellen einer akzeptierten Domäne mit einem bekannten Namen. Zu diesem Zweck führen Sie den folgenden Befehl in Ihrer lokalen Exchange-Umgebung. In diesem Beispiel `<target domain>` ist Ihre Office 365 oder Exchange Online-Domäne, für die ein Sendeconnector bereits mithilfe des Assistenten für die Hybridkonfiguration konfiguriert wurde.

```
New-AcceptedDomain -Name PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99 -DomainName <target domain> -DomainType InternalRelay
```

### Beispiel:

```
New-AcceptedDomain -Name PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99 -DomainName "contoso.mail.onmicrosoft.com" -DomainType InternalRelay
```

Wenn die akzeptierte Domäne bereits in Ihrer lokalen Umgebung vorhanden ist, benennen Sie sie in `PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99` und behalten Sie die anderen Attribute bei.

Mit diesem Befehl können Sie prüfen, ob die akzeptierte Domäne bereits in Ihrer lokalen Umgebung existiert:

```
Get-AcceptedDomain | Where {$_.DomainName -eq "<target domain>"}
```

So benennen Sie die akzeptierte Domäne an, um

`PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99`, führen Sie Folgendes:

```
Get-AcceptedDomain | Where {$_.DomainName -eq "<target domain>} | Set-AcceptedDomain -Name PublicFolderDestination_78c0b207_5ad2_4fee_8cb9_f373175b3f99
```

#### NOTE

Wenn Sie Ihre e-Mail-aktivierten Öffentlichen Ordner in Exchange Online zum externe e-Mail-Nachrichten aus dem Internet empfangen erwarten, müssen Sie Directory basierend Edge-Blockierung (DBEB) in Exchange Online und Exchange Online Protection (EOP) zu deaktivieren. Weitere Informationen finden Sie unter [Use Directory Based Edge Blocking ablehnen von Nachrichten an ungültige Empfänger gesendet](#).

2. Wenn der Name eines öffentlichen Ordners mit einem umgekehrten Schrägstrich enthält \ oder einen Schrägstrich /, es kann nicht an die vorgesehenen Postfach migriert erhalten möchten, während des Migrationsprozesses. Bevor Sie migrieren, benennen Sie alle solchen Ordner, um diese Zeichen zu entfernen.

a. Führen Sie den folgenden Befehl aus, um öffentliche Ordner zu suchen, deren Name einen umgekehrten Schrägstrich enthält:

```
Get-PublicFolder -Recurse -ResultSize Unlimited | Where {$_.Name -like "*\*" -or $_.Name -like "*/*"} | Format-List Name, Identity, EntryId
```

b. Wenn Öffentliche Ordner zurückgegeben werden, können Sie sie durch Ausführung des folgenden Befehls umbenennen:

```
Set-PublicFolder -Identity "<public folder EntryId>" -Name "<new public folder name>"
```

3. Führen Sie die folgenden Schritte aus, um zu bestätigen, dass es kein Eintrag zu einer vorherigen und erfolgreiche Migration in Ihrer Organisation. Wenn vorhanden ist, müssen Sie diesen Wert festlegen `$false`.

Vergewissern Sie sich vor einer Änderung der Werte, dass der vorherige Migrationsversuch verworfen werden kann, damit Sie nicht versehentlich eine zweite Migration durchführen.

- a. Führen Sie den folgenden Befehl aus, um frühere Migrationen zu finden und den Status dieser Migrationen abzurufen:

```
Get-OrganizationConfig | Format-List PublicFoldersLockedforMigration,  
PublicFolderMigrationComplete, PublicFolderMailboxesLockedForNewConnections,  
PublicFolderMailboxesMigrationComplete
```

**NOTE**

Wenn entweder der `PublicFoldersLockedforMigration` oder `PublicFolderMigrationComplete` Parameter sind `$true`, sie bedeutet, dass Sie zu einem bestimmten Zeitpunkt ältere öffentliche Ordner migriert haben. Stellen Sie sicher, dass alle ältere öffentliche Ordner-Datenbanken außer Betrieb gesetzt wurde haben, bevor Sie mit Schritt 3 fortfahren.

- b. Wenn eine der oben genannten wird zurückgegeben, dessen Wert festgelegt `$true`, stellen sie `$false` durch ausführen:

```
Set-OrganizationConfig -PublicFoldersLockedforMigration:$false -  
PublicFolderMigrationComplete:$false -PublicFolderMailboxesLockedForNewConnections:$false -  
PublicFolderMailboxesMigrationComplete:$false
```

4. Wir empfehlen Ihnen, die nachfolgend aufgeführten Befehle auf allen betreffenden Exchange 2013-Servern auszuführen, damit Sie nach Abschluss der Migration den Migrationserfolg überprüfen können. Die Befehle erstellen Momentaufnahmen Ihrer aktuell bereitgestellten öffentlichen Ordner, die Sie später mit den migrierten öffentlichen Ordner vergleichen können.

**NOTE**

Abhängig von der Größe Ihrer Exchange-Organisation kann die Ausführung dieser Befehle einige Zeit dauern.

- Führen Sie den folgenden Befehl aus, um eine Momentaufnahme der ursprünglichen Quellordnerstruktur zu erstellen.

```
Get-PublicFolder -Recurse -ResultSize Unlimited | Export-CliXML OnPrem_PFStructure.xml
```

- Führen Sie den folgenden Befehl aus, um eine Momentaufnahme der Statistikdaten von Öffentlichen Ordner (wie Anzahl von Elementen, Größe und Besitzer) zu erstellen.

```
Get-PublicFolderStatistics -ResultSize Unlimited | Export-CliXML OnPrem_PFStatistics.xml
```

- Führen Sie den folgenden Befehl aus, um eine Momentaufnahme der Berechtigungen der öffentlichen Ordner zu erstellen:

```
Get-PublicFolder -Recurse -ResultSize Unlimited | Get-PublicFolderClientPermission | Select-Object Identity,User -ExpandProperty AccessRights | Export-CliXML OnPrem_PFPerms.xml
```

- Führen Sie den folgenden Befehl aus, um eine Momentaufnahme Ihrer E-Mail-aktivierten öffentlichen Ordner zu erstellen:

```
Get-MailPublicFolder -ResultSize Unlimited | Export-CliXML OnPrem_MEPM.xml
```

- Speichern Sie die von den oben beschriebenen Befehlen generierten Dateien an einem sicheren Ort, um sie nach der Migration für einen Vergleich heranziehen zu können.

5. Wenn Sie Microsoft Azure Active Directory verbinden (Azure AD-Connect) verwenden die lokalen Verzeichnisse mit Azure Active Directory synchronisiert, müssen Sie die folgenden Aktionen ausführen (Wenn Sie nicht Azure AD-Verbindung verwenden, Sie können diesen Schritt überspringen):

- a. Öffnen Sie auf einem lokalen Computer Microsoft Azure Active Directory Connect, und wählen Sie dann **Konfigurieren** aus.
- b. Wählen Sie auf dem Bildschirm **Weitere Aufgaben** die Option **Synchronisierungsoptionen prüfen oder anpassen** aus, und klicken Sie dann auf **Weiter**.
- c. Geben Sie auf dem Bildschirm **Mit Azure AD verbinden** die entsprechenden Anmeldeinformationen ein, und klicken Sie dann auf **Next**. Nachdem eine Verbindung hergestellt wurde, klicken Sie weiter auf **Weiter**, bis Sie sich auf dem Bildschirm **Optionale Features** befinden.
- d. Vergewissern Sie sich, dass **Öffentliche Exchange-E-Mail-Ordner** nicht aktiviert ist. Wenn die Option nicht aktiviert ist, können Sie mit dem nächsten Abschnitt, *Erforderliche Schritte in Exchange Online*, fortfahren. Wenn die Option aktiviert ist, deaktivieren Sie das Kontrollkästchen, und klicken Sie dann auf **Weiter**.

#### NOTE

Wenn Sie **Öffentliche Exchange-E-Mail-Ordner** nicht als Option auf dem Bildschirm **Optionale Features** sehen, können Sie Microsoft Azure Active Directory Connect beenden und mit dem nächsten Abschnitt, *Erforderliche Schritte in Exchange Online*, fortfahren.

- e. Nachdem Sie die Option **Öffentliche Exchange-E-Mail-Ordner** deaktiviert haben, klicken Sie weiter auf **Weiter**, bis Sie sich auf dem Bildschirm **Bereit zur Konfiguration** befinden, und klicken Sie dann auf **Konfigurieren**.

#### Erforderliche Schritte in Exchange Online

Führen Sie die folgenden Schritte in Exchange Online PowerShell durch:

1. Stellen Sie sicher, dass aktuell keine Migrationsanforderungen für öffentliche Ordner vorhanden sind. Falls welche vorhanden sind, müssen Sie sie löschen; andernfalls wird Ihre eigene Migrationsanforderung fehlgeschlagen. Dieser Schritt ist nur erforderlich, wenn Sie glauben, dass in der Pipeline möglicherweise bereits eine Migrationsanforderung vorhanden ist (eine Anforderung, die fehlgeschlagen ist oder die Sie abbrechen möchten).

Eine bereits vorhandene Migrationsanforderung kann eine Anforderung für einen von zwei Migrationstypen sein: eine Batchmigration oder eine serielle Migration. Unten sehen Sie die Befehle, mit denen Sie die verschiedenen Anforderungstypen erkennen und entfernen können.

Mit diesem Beispielbefehl können Sie alle vorhandenen Anforderungen für eine serielle Migration

ermitteln:

```
Get-PublicFolderMigrationRequest | Get-PublicFolderMigrationRequestStatistics
```

Mit diesem Beispielbefehl entfernen Sie alle vorhandenen Anforderungen für eine serielle Migration öffentlicher Ordner:

```
Get-PublicFolderMigrationRequest | Remove-PublicFolderMigrationRequest
```

Mit diesem Beispielbefehl können Sie alle vorhandenen Anforderungen für eine Batchmigration ermitteln:

```
Get-MigrationBatch | ?{$_._MigrationType.ToString() -eq "PublicFolder"}
```

Mit diesem Beispielbefehl entfernen Sie alle vorhandenen Anforderungen für eine Batchmigration öffentlicher Ordner:

```
Remove-MigrationBatch <name of migration batch> -Confirm:$false
```

2. Die Migrationsfunktion **PAW** muss für Ihren Office 365-Mandanten aktiviert sein. Führen Sie den folgenden Befehl in Exchange Online PowerShell aus, um dies zu überprüfen:

```
Get-MigrationConfig
```

Wenn in der Ausgabe unter **Features** der Eintrag **PAW** aufgeführt ist, ist die Funktion aktiviert, und Sie können mit dem nächsten Schritt fortfahren.

Wenn KRALLE noch nicht für Ihre Mandanten aktiviert, es sein kann, da stehen Ihnen einige vorhandenen migrationsbatches, batches Öffentliche Ordner Batches oder Benutzer. Diese Batches konnte in jeder Zustand, einschließlich abgeschlossen sein. Wenn dies der Fall ist, schließen Sie, und entfernen Sie alle migrationsbatches bis keine Datensätze zurückgegeben werden, bei der Ausführung `Get-MigrationBatch`. Nachdem alle vorhandenen Stapel entfernt werden, KRALLE sollte automatisch aktiviert worden. Notiz, die entsprechend der Änderung in möglicherweise nicht `Get-MigrationConfig` sofort, aber das ist OK. Im Fall von Benutzermigrationen können Sie weiterhin neue Stapel erstellen, sobald dieser Schritt abgeschlossen ist.

3. Stellen Sie sicher, dass in Exchange Online weder öffentliche Ordner noch Postfächer für öffentliche Ordner vorhanden sind. Sollten in Exchange Online nach Durchführung der unten beschriebenen Schritte noch öffentliche Ordner existieren, müssen Sie auf jeden Fall herausfinden, warum sie vorhanden sind und wer in Ihrer Organisation eine Hierarchie für öffentliche Ordner angelegt hat, bevor Sie irgendwelche öffentlichen Ordner oder Postfächer für öffentliche Ordner entfernen.

- a. Führen Sie in Office 365 oder Exchange Online PowerShell den folgenden Befehl aus, um zu sehen, ob öffentliche Ordner-Postfächer vorhanden sind.

```
Get-Mailbox -PublicFolder
```

- b. Falls der Befehl keine Postfächer für öffentliche Ordner zurückgibt, fahren Sie fort mit [Schritt 3: Generieren der CSV-Dateien](#). Gibt der Befehl Postfächer für öffentliche Ordner zurück, müssen Sie den folgenden Befehl ausführen, um nach öffentlichen Ordnern zu suchen:

```
Get-PublicFolder -Recurse
```

- c. Falls öffentliche Ordner in Office 365 oder Exchange Online vorhanden sind, müssen Sie sie mit dem PowerShell-Befehl unten entfernen (sofern sie nicht benötigt werden). Speichern Sie vor dem Löschen auf jeden Fall alle Informationen, die in diesen öffentlichen Ordnern vorhanden sind. Wenn Sie die öffentlichen Ordner entfernen, werden alle Informationen in ihnen endgültig gelöscht.

```
Get-MailPublicFolder -ResultSize Unlimited | where {$_.EntryId -ne $null} | Disable-MailPublicFolder -Confirm:$false  
Get-PublicFolder -GetChildren \ -ResultSize Unlimited | Remove-PublicFolder -Recurse -Confirm:$false
```

- d. Sobald Sie die öffentlichen Ordner entfernt haben, können Sie mithilfe der folgenden Befehle alle Postfächer für öffentliche Ordner entfernen:

```
$hierarchyMailboxGuid = $(Get-OrganizationConfig).RootPublicFolderMailbox.HierarchyMailboxGuid  
Get-Mailbox -PublicFolder | Where-Object {$_.ExchangeGuid -ne $hierarchyMailboxGuid} | Remove-Mailbox -PublicFolder -Confirm:$false -Force  
Get-Mailbox -PublicFolder | Where-Object {$_.ExchangeGuid -eq $hierarchyMailboxGuid} | Remove-Mailbox -PublicFolder -Confirm:$false -Force  
Get-Mailbox -PublicFolder -SoftDeletedMailbox | Remove-Mailbox -PublicFolder -PermanentlyDelete:$true
```

## Schritt 3: Generieren der CSV-Dateien

Verwenden Sie die zuvor heruntergeladenen Skripts, um die während der Migration zu verwendenden CSV-Dateien zu generieren.

- Führen Sie über die Exchange-Verwaltungsshell (lokal), die `Export-ModernPublicFolderStatistics.ps1` Skript zum Erstellen der Ordner Namen zu Ordnergrößen Mapping-Datei. Benötigen Sie Lokaler Administrator-Berechtigungen zum Ausführen dieses Skripts ein. Die resultierende Datei enthält drei Spalten: **FolderName**, **FolderSize** und **DeletedItemSize**. Die Werte für die Spalten **FolderSize** und **DeletedItemSize** werden in Bytes angezeigt. Beispielsweise `\PublicFolder01,10240 100` bedeutet, dass der Öffentliche Ordner im Stamm Hierarchie der mit dem Namen PublicFolder01 ist 10240 Bytes oder 10.240 MB groß, und 100 Bytes wiederherstellbare Elemente darin vorhanden sind. <<<<<< Kopf

=====

```
[ ] [ ] [ ] [ ] master .\Export-ModernPublicFolderStatistics.ps1 <Folder-to-size map path> [ ] [ ] [ ] [ ]
```

### Beispiel:

```
...  
.\\Export-ModernPublicFolderStatistics.ps1 stats.csv  
...
```

- Führen Sie die `ModernPublicFolderToMailboxMapGenerator.ps1` Skript zum Erstellen einer CSV-Datei, die Postfächer für Öffentliche Ordner in Exchange Online Ziel Quelle Öffentliche Ordner zugeordnet ist. Diese Datei wird verwendet, um die richtige Anzahl der Postfächer für Öffentliche Ordner in Exchange Online zu berechnen.

#### NOTE

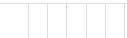
Die Datei, die vom generierten `ModernPublicFolderToMailboxMapGenerator.ps1` enthält nicht den Namen eines jeden öffentlichen Ordner in Ihrer Organisation. Enthält Verweise auf die übergeordneten Ordner größerer Ordner-Strukturen oder die Namen der Ordner, die selbst sind wesentlich groß. Sie können dieser Datei vorstellen, wie eine „Ausnahmedatei verwendet, um sicherzustellen, dass bestimmte Ordner-Strukturen und größerer Ordner in bestimmten Öffentlichen Postfächern gesetzt. Es ist normal, nicht für jede Komponente der öffentlichen Ordner in dieser Datei finden Sie unter. Untergeordneten Ordner eines beliebigen Ordners, die in dieser Datei zur Zuordnung aufgelistet werden auch die gleichen Postfach für Öffentliche Ordner als den übergeordneten Ordner (es sei denn, die explizit auf einer anderen Position in die Datei zur Zuordnung, die sie an eine andere Öffentliche Ordner-Mailbox weist erwähnten) migriert.

```
.\\ModernPublicFolderToMailboxMapGenerator.ps1 <Maximum mailbox size in bytes><Maximum mailbox recoverable item size in bytes><Folder-to-size map path><Folder-to-mailbox map path>
```

- <Maximum mailbox size in bytes> ist die Datenmenge, die Sie maximal zu einem einzelnen Postfach für öffentliche Ordner in Exchange Online migrieren möchten. Die Maximalgröße für dieses Feld liegt derzeit bei 50 GB. Wir empfehlen Ihnen jedoch, einen kleineren Wert zu verwenden (z. B. 50 % der Maximalgröße), um zukünftigem Wachstum Rechnung zu tragen.

<<<<< HEAD

- <Maximale Postfach wiederherstellbare Elemente, Größe in Bytes> wird das Kontingent wiederherstellbare Elemente auf Ihrem Exchange Online-Postfächern. Die maximale Größe der Postfächer für Öffentliche Ordner In Exchange Online ist derzeit 50 GB. Es wird empfohlen, `RecoverableItemsQuota` festlegen ' \_ auf 15 GB oder weniger. =====
- <Maximale Postfach wiederherstellbare Elemente, Größe in Bytes> wird das Kontingent wiederherstellbare Elemente auf Ihrem Exchange Online-Postfächern. Die maximale Größe der Postfächer für Öffentliche Ordner In Exchange Online ist derzeit 50 GB. Es wird empfohlen, `RecoverableItemsQuota` bis 15 GB oder weniger festlegen.

 master 

- <Ordnergröße-Karte Pfad> ist der Dateipfad der CSV-Datei, die Sie erstellt haben, bei der Ausführung der `Export-ModernPublicFolderStatistics.ps1` Skript.
- <Folder-to-mailbox map path> ist der Dateipfad der Datei mit den Ordner-Postfach-Zuordnungen, die Sie in diesem Schritt erstellen. Wenn Sie nur einen Dateinamen angeben, wird die Datei im aktuellen PowerShell-Verzeichnis auf dem lokalen Computer generiert.

#### Beispiel:

```
.\\ModernPublicFolderToMailboxMapGenerator.ps1 -MailboxSize 25GB -MailboxRecoverableItemSize 1GB - ImportFile .\\stats.csv -ExportFile map.csv
```

#### NOTE

Migrieren von öffentlichen Ordner zu Exchange Online nicht unterstützt werden, wenn die Anzahl der eindeutigen Öffentlichen Postfächer in Exchange Online mit mehr als 100 ist.

## Schritt 4: Erstellen der Postfächer für öffentliche Ordner in Exchange

# Online

Im nächsten Schritt erstellen Sie in Exchange Online PowerShell die Zielpostfächer für öffentliche Ordner, die Ihre migrierten öffentlichen Ordner enthalten sollen.

Führen Sie das folgende Skript aus, um die Ziel-Postfächer für Öffentliche Ordner zu erstellen. Das Skript erstellt eine Zielpostfach für jedes Postfach in der CSV-Datei, die Sie zuvor in generiert *Schritt 3: generieren die CSV-Dateien*, bei der Ausführung der `ModernPublicFoldertoMailboxMapGenerator.ps1` Skript.

```
$mappings = Import-Csv <Folder-to-mailbox map path>
$primaryMailboxName = ($mappings | Where-Object FolderPath -eq "\").TargetMailbox
New-Mailbox -HoldForMigration:$true -PublicFolder -IsExcludedFromServingHierarchy:$false $primaryMailboxName
($mappings | Where-Object TargetMailbox -ne $primaryMailboxName).TargetMailbox | Sort-Object -unique |
ForEach-Object { New-Mailbox -PublicFolder -IsExcludedFromServingHierarchy:$false $_ }
```

`Folder-to-mailbox map path` ist der Dateipfad der Postfach-Ordner CSV-Datei, die von generiert wurde die `ModernPublicFoldertoMailboxMapGenerator.ps1` Skript in *Schritt 3: generieren die CSV-Dateien*.

## Schritt 5: Starten der Migrationsanforderung

Nun müssen Sie einige Befehle in Ihrer lokalen Exchange 2013-Umgebung und in Exchange Online ausführen.

1. Führen Sie von einem Exchange 2013 Servern Postfächer für Öffentliche Ordner das folgende Skript aus. Mit diesem Skript werden e-Mail-aktivierte Öffentliche Ordner aus der lokalen Active Directory zu Exchange Online synchronisiert. Stellen Sie sicher, dass Sie die neueste Version von dieses Skript heruntergeladen haben und dass Sie über die Exchange-Verwaltungsshell ausführen.

```
.\Sync-ModernMailPublicFolders.ps1 -Credential (Get-Credential) -CsvSummaryFile:sync_summary.csv
```

- Sie sind für Exchange Online administrative Benutzername und Kennwort aufgefordert.
- `CsvSummaryFile` ist der Dateipfad, unter dem die Protokolldatei mit den Synchronisierungsvorgängen und Synchronisierungsfehlern gespeichert werden soll. Das Protokoll wird im CSV-Format gespeichert.

2. Suchen Sie auf dem Exchange 2013-Server den MRS-Proxyendpunktserver, und notieren Sie sich seinen Namen. Sie benötigen diese Information, um die Migrationsanforderung ausführen zu können. Speichern Sie die Information für Schritt 3b unten.
3. Führen Sie in Exchange Online PowerShell die folgenden Befehle aus, um die Anmeldeinformationen und die MRS-Informationen aus dem vorherigen Schritt an die Cmdlet-Variablen zu übergeben, die in der Migrationsanforderung verwendet werden:

- a. Übergeben Sie die Anmeldeinformationen eines Benutzers mit Administratorberechtigungen in der lokalen Umgebung Exchange 2013 in die Variable `$Source_Credential`. Die migrationsanforderung, dass Sie in Exchange Online ausgeführt wird dieser Anmeldeinformationen verwenden, um Zugriff auf Ihre lokalen Exchange 2013-Server zum Kopieren des Content über öffentlichen Ordners zu Exchange Online verwendet werden soll.

```
$Source_Credential = Get-Credential <source_domain>\<PublicFolder_Administrator_Account>
```

- b. Übergeben Sie die Informationen zum MRS-Proxyserver in der Exchange 2013-Umgebung, die Sie in Schritt 2 oben ermittelt haben, an die Variable:

```
$Source_RemoteServer = "<paste the value here>"
```

4. Führen Sie die folgenden Befehle in Exchange Online PowerShell aus, um den Endpunkt für die Migration der öffentlichen Ordner und die Migrationsanforderung für die öffentlichen Ordner zu erstellen:

```
$PFEEndpoint = New-MigrationEndpoint -PublicFolder -Name PublicFolderEndpoint -RemoteServer $Source_RemoteServer -Credentials $Source_Credential  
[byte[]]$bytes = Get-Content -Encoding Byte <folder_mapping.csv>  
New-MigrationBatch -Name PublicFolderMigration -CSVData $bytes -SourceEndpoint $PFEEndpoint.Identity -NotificationEmails <email addresses for migration notifications>
```

#### NOTE

Trennen Sie mehrere E-Mail-Adressen durch Kommata.

Wobei `folder_mapping.csv` ist die Zuordnungsdatei, die in generiert wurde *Schritt 3: Erstellen Sie die CSV-Dateien*. Achten Sie darauf, dass Sie den vollständigen Dateipfad bereitstellen. Wenn die Zuordnungsdatei aus irgendeinem Grund verschoben wurde, müssen Sie den neuen Speicherort.

5. Führen Sie nun den folgenden Befehl in Exchange Online PowerShell aus, um die Migration zu starten:

```
Start-MigrationBatch PublicFolderMigration
```

Zwar müssen Batchmigrationen mithilfe des Cmdlets „New-MigrationBatch“ in Exchange Online PowerShell erstellt werden; Sie können den Fortschritt und den Abschluss der Migration jedoch im EAC oder mithilfe des Cmdlets „Get-MigrationBatch“ nachverfolgen und verwalten. Das Cmdlet „New-MigrationBatch“ initiiert eine Migrationsanforderung für Postfächer für jedes Postfach für öffentliche Ordner. Den Status dieser Anforderungen können Sie auf der Seite der Postfachmigration sehen.

So rufen Sie die Seite der Postfachmigration auf:

1. Melden Sie sich bei Exchange Online an, und öffnen Sie das EAC.
2. Navigieren Sie zu **Empfänger**, und wählen Sie **Migration** aus.
3. Wählen Sie die soeben erstellte Migrationsanforderung aus, und klicken Sie im Bereich **Details** auf **Details anzeigen**.

Bevor Sie fortfahren mit *Schritt 6: Sperren der öffentlichen Ordner in der Exchange 2013-Umgebung*, müssen Sie sicherstellen, dass alle Daten kopiert worden sind und keine Fehler bei der Migration aufgetreten sind. Sobald Sie sich vergewissert haben, dass der Batch den Status **Synchronisiert** hat, erstellen Sie mithilfe der Befehle aus *Schritt 2: Vorbereiten der Migration* (letzter Schritt unter **Erforderliche Schritte in der lokalen Exchange 2013-Serverumgebung**) eine Momentaufnahme der lokalen öffentlichen Ordner. Nachdem Sie diese Befehle ausgeführt haben, können Sie mit dem nächsten Schritt fortfahren. Beachten Sie, dass es je nach Anzahl der Ordner eine Weile dauern kann, bis die Befehle abgeschlossen werden.

## Schritt 6: Sperren der öffentlichen Ordner in der Exchange 2013-Umgebung während der endgültigen Migration (Downtime der öffentlichen Ordner erforderlich)

Bis zu diesem Zeitpunkt im Migrationsprozess wurden Benutzer auf Ihre lokale Öffentliche Ordner zugreifen. Die folgenden Schritte werden jetzt melden Benutzer deaktiviert aus öffentlichen Ordner von Exchange 2013 und

dann die Ordner sperren, während des Migrationsprozesses die letzte Synchronisierung abgeschlossen ist. Benutzer werden nicht in der Lage, während dieser Zeit auf Öffentliche Ordner zugreifen, und alle an diese e-Mail-aktivierten Öffentlichen Ordner gesendeten Nachrichten in einer Warteschlange gespeichert werden und nicht zugestellt bleiben, bis zum Abschluss der Migrations öffentlicher Ordner.

Vor dem Ausführen der `PublicFolderMailboxesLockedForNewConnections` Befehl wie unten beschrieben, stellen Sie sicher, dass alle Aufträge im Zustand **synchronisiert** werden. Hierzu können Sie mit der `Get-PublicFolderMailboxMigrationRequest` Befehl. Fahren Sie mit diesen Schritt nur aus, nachdem Sie sichergestellt haben, dass alle Aufträge im Zustand **synchronisiert** werden.

Führen Sie den folgenden Befehl in Ihrer lokalen Umgebung aus, um die öffentlichen Ordner in Exchange 2013 während des Abschlusses der Migration zu sperren:

```
Set-OrganizationConfig -PublicFolderMailboxesLockedForNewConnections $true
```

#### NOTE

Wenn Sie nicht für den Zugriff auf können die `-PublicFolderMailboxesLockedForNewConnections` -Parameter möglicherweise, weil die Active Directory nicht während der Aktualisierung CU vorbereitet wurde wie wir oben in besser *Was möchten Sie wissen, bevor Sie beginnen?* Weitere Informationen finden Sie unter [Vorbereiten von Active Directory und Domänen](#). > Beachten Sie, dass alle Benutzer, die Zugriff auf Öffentliche Ordner benötigen sollte auch migriert zuerst, **vor dem** Migrieren von öffentlichen Ordner selbst.

Wenn Ihre Organisation Postfächer für Öffentliche Ordner auf mehreren Exchange 2013 Servern verfügt, müssen Sie warten, bis die Active Directory-Replikation abgeschlossen ist. Nach Abschluss des Vorgangs können Sie bestätigen, dass alle Postfächer für Öffentliche Ordner aufgenommene haben die `PublicFolderMailboxesLockedForNewConnections` -Flag, und alle ausstehenden Änderungen Benutzer zuletzt versucht, ihre öffentlichen Ordner in der gesamten Organisation zusammengeführt haben. All dies kann mehrere Stunden dauern.

## Schritt 7: Abschließen der Migration der öffentlichen Ordner (Downtime der öffentlichen Ordner erforderlich)

Bevor Sie Ihre Migration öffentlicher Ordner abschließen können, müssen Sie bestätigen, dass es keine anderen Postfach für Öffentliche Ordner verschiebt oder Verschieben Öffentlicher Ordner Wechsel zu auf in Ihrer lokalen Exchange-Umgebung. Verwenden Sie dazu die `Get-MoveRequest` und `Get-PublicFolderMoveRequest` Cmdlets so Listen Sie alle vorhandenen öffentlichen Ordner verschoben. Wenn alle Verschiebungen ausgeführt wird, oder den Status **abgeschlossen** sind, entfernen Sie sie.

Führen Sie als Nächstes zum Abschließen der Migration der öffentlichen Ordner den folgenden Befehl in Exchange Online PowerShell aus:

```
Complete-MigrationBatch PublicFolderMigration
```

Wenn Sie diesen Befehl ausführen, geschieht Exchange eine abschließende Synchronisierung zwischen Ihrer lokalen Exchange-Organisation und Exchange Online. Während dieser Phase der Status des migrationsbatches von **synchronisiert** in geändert **wird abgeschlossen**, und schließlich auf **abgeschlossen**. Wenn die abschließende Synchronisierung erfolgreich ist, werden der Öffentliche Ordner in Exchange Online aufgehoben werden.

In der Regel dauert es einige Stunden, bis der Status des migrationsbatches von **Synchronisiert** in **Wird abgeschlossen** geändert wird. Erst dann beginnt die abschließende Synchronisierung.

## Schritt 8: Testen und Entsperren der öffentlichen Ordner in Exchange Online

Führen Sie nach Abschluss der Migration der öffentlichen Ordner die folgenden Schritte durch, um den Erfolg der Migration zu testen und den Abschluss offiziell zu bestätigen. Im Rahmen dieser abschließenden Aufgaben testen Sie die migrierte Hierarchie der öffentlichen Ordner, bevor Sie Ihre Organisation endgültig auf öffentliche Ordner in Exchange Online umstellen.

1. Weisen Sie in Exchange Online PowerShell einigen Testbenutzerpostfächern eines Ihrer gerade migrierten Postfächer für öffentliche Ordner als Standardpostfach für öffentliche Ordner zu:

```
Set-Mailbox -Identity <test user> -DefaultPublicFolderMailbox <public folder mailbox identity>
```

Stellen Sie sicher, dass Ihre Testbenutzer die erforderlichen Berechtigungen zum Erstellen von öffentlichen Ordnern haben.

2. Melden Sie sich mit dem Testbenutzer, den Sie im vorherigen Schritt festgelegt, den und schalten Sie die folgenden Tests für Öffentliche Ordner, in Outlook an. Beachten Sie, dass es 15 bis 30 Minuten, damit die Änderungen wirksam werden dauern kann. Nachdem Outlook die Änderungen bekannt sind, kann sie mehrmals neu starten aufgefordert.
  - a. Zeigen Sie die Hierarchie an.
  - b. Prüfen Sie die Berechtigungen.
  - c. Erstellen Sie einige öffentliche Ordner, und löschen Sie sie anschließend wieder.
  - d. Veröffentlichen Sie Inhalte in einem öffentlichen Ordner, und löschen Sie Inhalte aus einem öffentlichen Ordner.

Wenn Sie auf Probleme stoßen, und bestimmen, dass Sie nicht vollständig zu Exchange Online Öffentliche Ordner in Ihrer Organisation wechseln möchten, finden Sie unter [Zurücksetzen einer Migration öffentlicher Ordner von Exchange 2013 zu Exchange Online](#).

3. Führen Sie den folgenden Befehl im Exchange Online PowerShell zum Entsperren Ihre öffentlichen Ordner in Exchange Online. Nach der Ausführung des Befehls dauert es etwa 15 bis 30 Minuten, damit die Änderungen wirksam werden. Nachdem Outlook sollten Sie die Änderungen wird, fordert es möglicherweise Ihre Benutzer die Anwendung mehrmals neu starten.

```
Set-OrganizationConfig -RemotePublicFolderMailboxes $Null -PublicFoldersEnabled Local
```

## Schritt 9: Lokales Abschließen der Migration

Gehen Sie folgendermaßen vor, um e-Mails an e-Mail-aktivierte Öffentliche Ordner Lokale zu aktivieren:

1. Führen Sie in Ihrer lokalen Umgebung ab das folgende Skript aus, um sicherzustellen, dass alle e-Mails an e-Mail-aktivierten Öffentlichen Ordner zu Exchange Online ordnungsgemäß weitergeleitet werden. Das Skript wird Stempeln e-Mail-aktivierten Öffentlichen Ordner mit einer `ExternalEmailAddress`, um den entsprechenden Exchange Online zeigt:

```
.\SetMailPublicFolderExternalAddress.ps1 -ExecutionSummaryFile:mepf_summary.csv
```

2. Wenn der Test erfolgreich war, führen Sie nun in Ihrer lokalen Umgebung den folgenden Befehl aus, um zu bestätigen, dass die Migration der öffentlichen Ordner abgeschlossen ist:

```
Set-OrganizationConfig -PublicFolderMailboxesMigrationComplete:$true -PublicFoldersEnabled Remote
```

## Woher weiß ich, dass der Vorgang erfolgreich war?

In [Schritt 2: Vorbereiten der Migration](#) haben Sie Momentaufnahmen der Struktur Ihrer lokalen öffentlichen Ordner sowie ihrer Kennzahlen und Berechtigungen erstellt. Mit den folgenden Schritten erstellen Sie nun nach der Migration dieselben Momentaufnahmen in Exchange Online. So können Sie überprüfen, ob die Migration Ihrer öffentlichen Ordner erfolgreich war. Vergleichen Sie einfach die Daten in den beiden Dateien.

1. Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um eine Momentaufnahme der neuen Ordnerstruktur zu erstellen:

```
Get-PublicFolder -Recurse -ResultSize Unlimited | Export-CliXML Cloud_PFStructure.xml
```

2. Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um eine Momentaufnahme der Kennzahlen der öffentlichen Ordner zu erstellen, einschließlich Elementanzahl, Größe und Besitzer:

```
Get-PublicFolder -Recurse -ResultSize Unlimited | Get-PublicFolderStatistics | Export-CliXML Cloud_PFSStatistics.xml
```

3. Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um eine Momentaufnahme der Berechtigungen zu erstellen:

```
Get-PublicFolder -Recurse -ResultSize Unlimited | Get-PublicFolderClientPermission | Select-Object Identity,User, AccessRights | Export-CliXML Cloud_PFPerms.xml
```

4. Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um eine Momentaufnahme der E-Mail-aktivierten öffentlichen Ordner zu erstellen:

```
Get-MailPublicFolder -ResultSize Unlimited | Export-CliXML Cloud_MEPF.xml
```

## Bekannte Probleme

Im folgenden werden häufige Migrationsprobleme für Öffentliche Ordner, die in Ihrer Organisation auftreten können.

- Migrieren von öffentlichen Ordner zu Exchange Online nicht unterstützt werden, wenn die Anzahl der eindeutigen Öffentlichen Ordner-Postfächer in Exchange Online mit mehr als 100 ist.
- Die Berechtigungen für den als Stammordner fungierenden öffentlichen Ordner und den Ordner EFOMS REGISTRY werden nicht zu Exchange Online migriert. Sie müssen sie manuell in Exchange Online anwenden. Führen Sie dazu den Befehl unten in Exchange Online PowerShell aus. Führen Sie den Befehl jeweils einmal für jeden Berechtigungseintrag aus, der lokal vorhanden ist, in Exchange Online aber fehlt:

```
Add-PublicFolderClientPermission "\\" -User <user> -AccessRights <access rights>
Add-PublicFolderClientPermission "\NON_IPM_SUBTREE\EFOMS REGISTRY" -User <user> -AccessRights <access rights>
```

- Einige Öffentliche Ordner-Migrationen schlägt fehl, wenn einige Postfächer für Öffentliche Ordner die Hierarchie Öffentlicher Ordner nicht verarbeitet werden. Dies bedeutet, dass die

**IsExcludedFromServingHierarchy** Parameter für eine oder mehrere Postfächer festgelegt ist `$true`. Um dies zu vermeiden, legen Sie alle Postfächer in Exchange Online, um die Hierarchie zu verarbeiten.

- Die Berechtigungen **Send As** und **Senden im Auftrag von** werden nicht zu Exchange Online migriert. Falls dies bei Ihrer Migration der Fall ist, können Sie die Befehle unten in Ihrer lokalen Umgebung ausführen, um herauszufinden, wer diese Berechtigungen besitzt.

So finden Sie heraus, welche öffentlichen Ordner lokal über Berechtigungen des Typs „Send As“ verfügen:

```
Get-MailPublicFolder | Get-ADPermission | ?{$_._.ExtendedRights -like "*Send-As*"}
```

So finden Sie heraus, welche öffentlichen Ordner lokal über Berechtigungen des Typs „Senden im Auftrag von“ verfügen:

```
Get-MailPublicFolder | ?{$_._.GrantSendOnBehalfTo -ne "$null"} | ft name,GrantSendOnBehalfTo
```

Geben Sie Folgendes in Exchange Online PowerShell ein, um einem E-Mail-aktivierten öffentlichen Ordner in Exchange Online die Berechtigung „Send As“ hinzuzufügen:

```
Add-RecipientPermission -Identity <mail-enabled public folder primary SMTP address> -Trustee <name of user to be assigned permission> -AccessRights SendAs
```

### Beispiel:

```
Add-RecipientPermission -Identity send1 -Trustee Exo1 -AccessRights SendAs
```

Geben Sie Folgendes in Exchange Online PowerShell ein, um einem E-Mail-aktivierten öffentlichen Ordner in Exchange Online die Berechtigung „Senden im Auftrag von“ hinzuzufügen:

```
Set-MailPublicFolder -Identity <name of public folder> -GrantSendOnBehalfTo <user or comma-separated list of users>
```

### Beispiel:

```
Set-MailPublicFolder send2 -GrantSendOnBehalfTo exo1,exo2
```

- Wenn mehr als 10.000 Ordner unter dem Ordner „\NON\_IPM\_SUBTREE\DUMPSTER\_ROOT“ vorhanden sind, kann es zu einem Migrationsfehler kommen. Überprüfen Sie deshalb den Ordner „\NON\_IPM\_SUBTREE\DUMPSTER\_ROOT“, um festzustellen, ob er mehr als 10.000 direkte Unterordner (unmittelbar untergeordneten Elemente) hat. Sie können den folgenden Befehl verwenden, um die Anzahl der öffentlichen Ordner an diesem Speicherort zu ermitteln:

```
(Get-PublicFolder -GetChildren "\NON_IPM_SUBTREE\DUMPSTER_ROOT").Count
```

Exchange Online unterstützt nicht mehr als 10.000 Unterordner, weshalb es bei Migrationen von mehr als 10.000 Ordnern zu einem Fehler kommt. Wir entwickeln zurzeit ein Skript, damit auch solche Konfigurationen unterstützt werden. In der Zwischenzeit wird empfohlen, mit der Migration Ihrer öffentlichen Ordner zu warten.

- Migrationsaufgaben keine Fortschritte oder angehalten werden. Dies kann vorkommen, wenn es zu viele Aufträge parallel ausgeführt sind, Aufträge mit Fehlern zeitweilige Fehler verursacht. Sie können die

Anzahl der gleichzeitigen Aufträge reduzieren, indem ändern `MaxConcurrentMigrations` und `MaxConcurrentIncrementalSyncs` auf eine geringere Anzahl. Verwenden Sie das folgende Beispiel, um diese Werte festzulegen:

```
Set-MigrationEndpoint <PublicFolderEndpoint> -MaxConcurrentMigrations 30 -  
MaxConcurrentIncrementalSyncs 20 -SkipVerification
```

- Fehlerhafte Ausführung von Migrationsaufträgen mit Fehler „Fehler: Dumpster des Dumpster-Ordners.“ Falls dieser Fehler angezeigt wird, sollte er behoben werden, wenn Sie den Batch beenden und dann erneut starten.
- Migrationsaufgaben fehl und zum Generieren einer "Anforderung wurde unter Quarantäne gestellte e-Mails aufgrund der folgenden Fehler: der angegebene Schlüssel war nicht im Wörterbuch vorhanden" Fehlermeldung angezeigt. Dies geschieht, wenn ein beschädigtes Element in einem Ordner vorhanden ist, die Migrationsaufgaben kopieren kann. Um dieses Problem zu umgehen:
  1. Beenden Sie den Migrationsbatch.
  2. Identifizieren Sie den Ordner, der das fehlerhafte Element enthält. Der Migrationsbericht sollte Verweise auf den Ordner enthalten, der beim Auftreten des Fehlers kopiert wurde.
  3. Verschieben Sie den betroffenen Ordner in Ihrer lokalen Umgebung an das Postfach des primären Öffentlichen Ordner. Sie können die `New-PublicFolderMoveRequest` -Cmdlet zum Verschieben von Ordnern.
  4. Warten Sie auf den Ordner verschieben für die Durchführung. Nachdem er abgeschlossen ist, entfernen Sie die Move-Anforderung. Klicken Sie dann migrationsbatch neu gestartet.

## Entfernen von Postfächern für öffentliche Ordner aus Ihrer lokalen Exchange-Umgebung

Sobald die Migration abgeschlossen ist und Sie sichergestellt haben, dass Ihre öffentlichen Ordner in Exchange Online wie erwartet funktionieren und alle erwarteten Daten enthalten, können Sie Ihre lokalen Postfächer für öffentliche Ordner entfernen.

Beachten Sie, dass dieser Schritt nicht rückgängig gemacht werden, ist, da gelöschte Postfächer für Öffentliche Ordner sind sie nicht wiederhergestellt werden können. Aus diesem Grund wird dringend empfohlen, dass zusätzlich zu den Erfolg der Migration überprüft haben, Sie auch Ihre Exchange Online Öffentliche Ordner für einige Wochen vor dem Entfernen der lokale Postfächer für Öffentliche Ordner überwachen.

# Zurücksetzen einer Migrations öffentlicher Ordner von Exchange Server zu Exchange Online

18.12.2018 • 3 minutes to read

**Zusammenfassung:** Führen Sie diese Schritte, um Öffentliche Ordner-Infrastruktur in den Zustand vor der Migration in Ihrem lokalen Exchange-Server zurückgegeben.

Wenn Sie Probleme mit der Migration der öffentlichen Ordner zu Exchange Online oder für alle anderen Grund müssen so reaktivieren Sie Ihre öffentlichen Ordner von Exchange Server ausgeführt wird, führen Sie die folgenden Schritte aus.

## Durchführen eines Rollbacks der Migration

Beachten Sie: Wenn Sie ein Rollback der Migration ausführen, gehen alle Inhalte verloren, die nach der Migration zu den öffentlichen Ordnern in Exchange Online hinzugefügt worden sind, ob über Clients oder per E-Mail (im Falle E-Mail-aktivierter öffentlicher Ordner). Zum Speichern dieser Inhalte können Sie die nach der Migration in den öffentlichen Ordnern abgelegten Inhalte in eine PST-Datei exportieren. Diese Datei lässt sich dann nach Abschluss des Rollbacks in die lokalen öffentlichen Ordner importieren.

1. Führen Sie in Ihrer lokalen Exchange-Umgebung so entsperren Sie Ihre öffentlichen Ordner von Exchange Server (Beachten Sie, die das Aufheben der Sperrung mehrere Stunden dauern kann) den folgenden Befehl aus:

```
Set-OrganizationConfig -PublicFolderMailboxesLockedForNewConnections:$false -  
PublicFolderMailboxesMigrationComplete:$false -PublicFoldersEnabled Local
```

2. In Ihrer lokalen Exchange-Umgebung Wiederherstellen der `ExternalEmailAddress` alle e-Mail-aktivierten Öffentlichen Ordners, der von SetMailPublicFolderExternalAddress.ps1 aktualisiert wurde (das Skript in verwendet *Schritt 8: Testen und Entsperren von öffentlichen Ordner in Exchange Online Verwendung Blattnamen Migration zu Migration Öffentlicher Ordner von Exchange Server zu Exchange Online*). Sie können finden Sie in der Zusammenfassung Datei erstellt, die von dem Skript auf diejenigen zu identifizieren, die geändert wurden, oder verwenden die Datei OnPrem\_MEPM.xml Datei weiter oben in der gleichen Migriert Batchvorgang generiert die ursprünglichen Eigenschaften für alle e-Mail-aktivierten Öffentlichen Ordner abgerufen.
3. Führen Sie in Exchange Online PowerShell die folgenden Befehle aus, um alle öffentlichen Ordner und Postfächer aus Exchange Online zu entfernen:

```
Get-MailPublicFolder -ResultSize Unlimited | where {$_.EntryId -ne $null} | Disable-MailPublicFolder -  
Confirm:$false  
Get-PublicFolder -GetChildren \ -ResultSize Unlimited | Remove-PublicFolder -Recurse -Confirm:$false  
$hierarchyMailboxGuid = $(Get-OrganizationConfig).RootPublicFolderMailbox.HierarchyMailboxGuid  
Get-Mailbox -PublicFolder | Where-Object {$_.ExchangeGuid -ne $hierarchyMailboxGuid} | Remove-Mailbox -  
PublicFolder -Confirm:$false -Force  
Get-Mailbox -PublicFolder | Where-Object {$_.ExchangeGuid -eq $hierarchyMailboxGuid} | Remove-Mailbox -  
PublicFolder -Confirm:$false -Force  
Get-Mailbox -PublicFolder -SoftDeletedMailbox | Remove-Mailbox -PublicFolder -PermanentlyDelete:$true
```

4. Führen Sie den folgenden Befehl in der Exchange Online-Umgebung zum Umleiten von Öffentliche Ordner-Datenverkehr an lokale (Exchange Server):

```
Set-OrganizationConfig -PublicFoldersEnabled Remote
```

5. Finden Sie unter [Konfigurieren der Exchange-Server Öffentliche Ordner für eine hybridbereitstellung](#) Anweisungen Neukonfigurieren der Zugriff auf Ihre lokale Öffentliche Ordner, damit Ihre Exchange Online-Benutzer darauf zugreifen können.

# Migrieren Ihrer öffentlichen Ordner zu Office 365-Gruppen

18.12.2018 • 17 minutes to read

**Zusammenfassung:** Gründe für und gegen eine Migration Ihrer öffentlichen Exchange-Ordner zu Office 365-Gruppen.

Dieser Artikel bietet einen Vergleich von öffentlichen Ordnern und Office 365-Gruppen und erklärt, welche Lösung sich jeweils am besten für Ihre Organisation eignet. Öffentliche Ordner gibt es bereits ebenso lange wie Exchange, während Gruppen erst kürzlich eingeführt wurden. Wenn Sie einige oder alle Ihre öffentlichen Ordner zu Gruppen migrieren möchten, erfahren Sie in diesem Artikel mehr über die Vorgehensweise. Er enthält Links zu Artikeln, die Sie Schritt für Schritt durch den Prozess führen.

## Was sind öffentliche Ordner?

[Öffentliche Ordner](#) verschiedene Arten von Daten enthalten und in einer hierarchischen Struktur organisiert sind.

Öffentliche Ordner werden nicht für die folgenden Zwecke empfohlen:

- **Datenarchivierung.** Benutzer, die Postfachbeschränkungen beachten müssen, verwenden zum Archivieren von Daten manchmal öffentliche Ordner anstelle von Postfächern. Diese Vorgehensweise wird nicht empfohlen, da dadurch Speicherplatz in öffentlichen Ordnern belegt wird und Postfachbeschränkungen ihren Sinn verlieren.
- **Gemeinsame Nutzung von Dokumenten und Zusammenarbeit.** Öffentliche Ordner stellen keine Dokumentverwaltungsfunktionen, wie z. B. Versionsverwaltung, gesteuerte Eincheck- und Auscheckfunktionen oder automatische Benachrichtigungen bei Inhaltsänderungen, zur Verfügung.

## Was sind Office 365-Gruppen?

Mit Gruppen in Office 365 können Sie eine Gruppe von Personen auswählen, mit denen Sie zusammenarbeiten möchten, und dann können Sie ganz einfach eine Sammlung von Ressourcen für diese Personen freigeben. Sie müssen die Berechtigungen für diese Ressourcen nicht manuell zuweisen, da die Personen beim Hinzufügen zu Ihrer Gruppe automatisch die notwendigen Berechtigungen für den Zugriff auf die Tools und Ressourcen Ihrer Gruppe erhalten. Gruppen bieten auch eine neue und verbesserte Erfahrung bei Aufgaben, die zuvor von Verteilerlisten und freigegebenen Postfächern ausgeführt wurden.

Die vollständigen Informationen zu Gruppen finden Sie unter [Weitere Informationen zu Office 365-Gruppen](#).

## Sollten Sie Ihre öffentlichen Ordner zu Office 365-Gruppen migrieren?

Office 365-Gruppen ist das neueste Zusammenarbeitsangebot von Microsoft, d. h., es gibt viele Gründe, diese Gruppen der viel älteren Technologie der öffentlichen Ordner vorzuziehen. In Outlook können z. B. Gruppen E-Mail-aktivierte öffentliche Ordner vollständig ersetzen. Es ist unmöglich, eine Liste aller erdenklicher Szenarien zusammenzustellen, in denen Office 365-Gruppen besser funktionieren als öffentliche Ordner, aber nachfolgend finden Sie die wichtigsten Informationen:

- **Zusammenarbeit per E-Mail.** Gruppen in Outlook verfügen über einen eigenen **Unterhaltungsbereich**, in dem alle E-Mails für die Zusammenarbeit gespeichert werden. Die Gruppe kann sogar so eingestellt werden, dass sie Nachrichten von Personen außerhalb der Gruppe oder außerhalb des Unternehmens erhält. Wenn Sie derzeit beispielsweise E-Mail-aktivierte öffentliche Ordner zum Speichern

projektbezogener Diskussionen verwenden oder Bestellungen von einem Team genehmigt werden müssen, wäre die Verwendung von Gruppen eine Verbesserung. Gruppen sind auch dann besser, wenn Sie Informationen zu einer Gruppe von Benutzern übertragen möchten.

- **Zusammenarbeit über Dokumente.** In Outlook, verfügen Gruppen über eine eigene **Dateien**-Registerkarte, auf der alle Dateien der SharePoint-Teamwebsite der Gruppe sowie aus E-Mail-Anlagen angezeigt werden. Sie erhalten eine Ansicht aller Dateien, so dass Sie nicht wie in öffentlichen Ordnern nach Dateien suchen müssen. Die gemeinsame Dokumenterstellung wird ebenfalls einfacher. Wenn Sie öffentliche Ordner zum Speichern von Dateien verwenden, die von mehreren Personen genutzt werden sollen, ziehen Sie eine Migration zu Gruppen in Betracht.
- **Freigegebener Kalender.** Bei der Erstellung erhält jede Gruppe einen freigegebenen Kalender. Jedes Mitglied der Gruppe kann Ereignisse in diesem Kalender erstellen. Wenn Sie eine Gruppe zu Ihren Favoriten hinzufügen, kann der Kalender dieser Gruppe neben Ihrem persönlichen Kalender angezeigt werden. Sie können auch die Ereignisse einer Gruppe abonnieren, sodass in dieser Gruppe erstellte Ereignisse in Ihrem persönlichen Kalender angezeigt werden. Wenn Sie öffentliche Ordner verwenden, um Kalender für Ihr Team zu hosten, wie z. B. einen Zeitplan, bieten Gruppen eine bessere Erfahrung.
- **Vereinfachte Berechtigungen.** Wenn Sie Benutzer einer Gruppe zuweisen, erhalten diese sofort die Berechtigungen, die sie benötigen, wohingegen Sie bei öffentlichen Ordnern die entsprechenden Berechtigungen manuell zuweisen müssen. Mitglieder können als „Besitzer“ oder „Mitglieder“ hinzugefügt werden. Besitzer besitzen in der Gruppe alle Rechte, einschließlich der Möglichkeit, Gruppen-Verwaltungsaufgaben durchzuführen. Mitglieder können auch Inhalte erstellen und Dateien wie Besitzer bearbeiten, aber sie können Inhalte, die sie nicht erstellt haben, nicht löschen. Wenn Ihnen das Berechtigungsmodell für die öffentlichen Ordner zu umfangreich erscheint und Sie eine einfache und schnelle Lösung suchen, sind Office 365-Gruppen die beste Wahl.
- **Mobile und Internetpräsenz.** Sie können nicht über mobile Geräte auf öffentliche Ordner zugreifen, und die Funktionen im Internet sind begrenzt. Mit mobilen Outlook-Apps können Sie jedoch auf Office 365-Gruppen zugreifen, und die Funktionen im Internet sind umfangreicher. Wenn Ihr Team unterwegs ist und mobilen Zugriff benötigt, sollten Sie Office 365-Gruppen verwenden.
- **Zugriff auf eine Vielzahl von Office 365-Apps.** Wenn Sie eine Gruppe erstellen, schalten Sie den Zugriff auf eine Bandbreite von Apps aus der Office 365-Suite frei. Sie erhalten eine SharePoint-Teamwebsite, um Dateien zu speichern, und einen Plan im Planer, um Ihre Aufgaben zu verfolgen. Office 365-Gruppen ist ein Mitgliederservice, der Elemente der gesamten Office 365-Suite kombiniert.

Während Office 365-Gruppen viele Vorteile bieten, sollten Sie einige wichtige Unterschiede beachten, die Sie bemerken werden, nachdem Sie die Nutzung der öffentlichen Ordner beendet haben. Primäre Unterschiede:

- **Ordnerhierarchie.** Während öffentliche Ordner häufig verwendet werden, um Inhalte in einer tief verwurzelten Hierarchie zu organisieren, verfügen Office 365-Gruppen über eine flache Struktur. Alle E-Mails in der Gruppe befinden sich im Bereich Unterhaltungen, und alle Dokumente werden unter der Registerkarte **Dateien** abgelegt. Zudem können Sie in Office 365-Gruppen keine Unterordner erstellen.
- **Granulare Berechtigungsrollen.** Während öffentliche Ordner über eine Vielzahl von Berechtigungsrollen verfügen, besitzen Office 365-Gruppen lediglich zwei: Besitzer und Mitglied.

Bevor Sie zu Gruppen wechseln, empfiehlt es sich zudem, sich die verschiedenen Einschränkungen bei der Erstellung und Verwaltung von Gruppen vor Augen zu führen. Unter *Wie verwalte ich meine Gruppen?* in [Weitere Informationen zu Office 365-Gruppen](#) finden Sie weitere Informationen.

## Migrieren Ihrer öffentlichen Ordner zu Office 365-Gruppen

Wenn Sie sich entscheiden, zu Office 365-Gruppen zu wechseln, können Sie ein Stapelmigration genanntes Verfahren verwenden, um Ihre E-Mail- und Kalenderinhalte aus Ihren vorhandenen öffentlichen Ordnern in

Gruppen zu verschieben. Die jeweiligen Schritte zum Ausführen einer Stapelmigration hängen davon ab, welche Version von Exchange Sie derzeit verwenden, um die Hierarchie Ihrer öffentlichen Ordner zu hosten. Am Ende dieses Artikels finden Sie Links zu Anweisungen, die Sie durch den Prozess der Stapelmigration führen.

#### **NOTE**

Nach Abschluss der Migration eines E-Mail-aktivierten öffentlichen Ordners zu einer bestimmten Gruppe in Office 365 werden alle E-Mails, die an diesen öffentlichen Ordner adressiert sind, von der Gruppe empfangen.

Hauptvorteile von Stapelmigrationen:

- **Auf dem Postfachreplikationsdienst (Mailbox Replication Service, MRS) basierende Migration.** Der Migrationsprozess verwendet Migrationsbatch-Cmdlets. Die Migration zu mehreren Gruppen kann zusammen in einem einzigen Migrationsbatch ausgelöst werden. Es stehen auch Skripts zur Verfügung, um den Migrationsprozess zu unterstützen.
- **Unterstützung von öffentlichen E-Mail- und Kalenderordnern.** Kopierte E-Mails und Beiträge werden wie in Gruppen als Gruppenunterhaltungen angezeigt, und kopierte Kalenderelemente sind in Gruppenkalendern sichtbar. Andere Arten von öffentlichen Ordner, wie z. B. Aufgaben und Kontakten, werden derzeit nicht für diese Migration unterstützt.
- **Direkt zu Office 365-Gruppen können lokale Öffentliche Ordner migriert werden.** Diese Migration müssen Sie für die erste Verschiebung öffentlicher Ordner zu Office 365 nicht und ziehen Sie dann auf Gruppen. Die MRS Daten kopieren-Cmdlets Lesen von Daten des öffentlichen Ordners direkt aus Ihrer lokalen Umgebung und kopieren Sie die Daten in Office 365-Gruppen. Beachten Sie, dass es sich bei öffentlichen Ordner von Exchange 2010 Outlook Anywhere Endpunkt erforderlich ist. Öffentliche Ordner von Exchange 2013 benötigen einen Endpunkt MRS-Proxy-basierte.
- **Bei dieser Migration müssen Sie nicht zwangsläufig alles migrieren.** Sie können bestimmte öffentliche Ordner für die Migration zu Gruppen auswählen, damit nur diese öffentlichen Ordner migriert werden.
- **Einmaliges Kopieren der Daten.** Bei der Stapelmigration werden die Daten einmal aus den Quellordnern der öffentlichen Ordner kopiert, sodass komplexe Vorgänge wie die inkrementelle Synchronisierung und Fertigstellung nicht erforderlich sind.
- **Die Daten der öffentlichen Ordner werden mit den vorhandenen Daten einer Gruppe zusammengeführt.** Die Datenkopie führt die Inhalte der öffentlichen Ordner mit ggf. vorhandenen Gruppeninhalten zusammen. Wenn eine inkrementelle Datenkopie erforderlich ist, können Sie die Datenkopie einfach so oft wie nötig ausführen. Auf diese Weise werden inkrementelle Daten in die Gruppe kopiert.

#### **Übersicht über Stapelmigrationen**

Die folgenden Schritte beschreiben den Prozess der Migration von Inhalten öffentlicher Ordner zu Office 365-Gruppen in einer Stapelmigration. Die Einzelheiten finden Sie in den unten aufgeführten Artikeln.

1. **Quelle wählen:** Wählen Sie die öffentlichen Ordner, die Sie migrieren möchten. Sie können alle Ordner mit E-Mail- oder Kalenderinhalten auswählen.
2. **Ziel erstellen:** Erstellen Sie entsprechende Gruppen für Ihre Ordner mit den gewünschten Konfigurationen, z. B. Mitglieder, Datenschutz und Klassifizierung von Daten.
3. **Daten kopieren:** Verwenden Sie die Migrationsbatch-Cmdlets, um Daten aus öffentlichen Ordner in Gruppen zu kopieren.
4. **Quelle sperren:** Sperren Sie die öffentlichen Ordner, nachdem Sie die Daten in Gruppen überprüft haben.

## 5. Übernahme:

Kopieren Sie die neuen Daten, die in den Schritten 3 und 4 erstellt wurden.

Beachten Sie, dass Ihre öffentlichen Ordner und die entsprechenden Gruppen während der Schritte 1 bis 3 online bleiben. Nach Schritt 3 können Sie basierend auf der Gruppenerfahrung und der Meinung der Benutzer abwägen, ob die Lösung zu Ihrem Unternehmen passt, und die Migration ggf. fortsetzen. Zu diesem Zeitpunkt können Sie ein Rollback zu den öffentlichen Ordnern durchführen. Wenn Sie nach Abschluss von Schritt 5 mit der Migration fortfahren, können Sie die ursprünglichen öffentlichen Ordner löschen. Selbst nach der Migration ist es möglich, ein Rollback zu den öffentlichen Ordnern durchzuführen, wenn Sie während der Migration Sicherungsdateien gespeichert und Ihre ursprünglichen öffentlichen Ordner nicht gelöscht haben.

### Voraussetzungen für die Stapelmigration und schrittweise Anleitungen

Die folgenden Voraussetzungen müssen in Ihrer Exchange-Umgebung erfüllt sein, bevor Sie eine Stapelmigration ausführen können. Die spezifischen Voraussetzungen hängen davon ab, welche Version von Exchange Sie momentan ausführen.

1. Wenn Ihre öffentlichen Ordner lokal sind, müssen Ihre Server mit einer der folgenden Versionen ausgeführt werden:
  - Exchange 2010 SP3 RU8 oder höher
  - Exchange 2013 CU15 oder höher
  - Exchange 2016 CU4 oder höher
2. Wenn Ihre öffentlichen Ordner lokal sind, muss eine Exchange-Hybrid-Umgebung einrichtet werden. Unter [Hybridbereitstellungen in Exchange Server](#) finden Sie weitere Informationen.

### Die Migrationsanleitung

Wählen Sie unten den entsprechenden Link, um eine schrittweise Anleitung zur Ausführung einer Stapelmigration zu erhalten.

- [Verwenden der Stapelmigration zum Migrieren von öffentlichen Exchange Online-Ordnern zu Office 365-Gruppen](#)
- [Verwenden der Stapelmigration zum Migrieren von öffentlichen Exchange 2010-Ordnern zu Office 365-Gruppen](#)
- [Verwenden der Batchmigration für die Migration von öffentlichen Exchange 2013-Ordnern in Office 365-Gruppen](#)
- [Verwenden der Stapelmigration für die Migration von öffentlichen Exchange-Ordner 2016 zu Office 365-Gruppen](#)

# Verwenden der Stapelmigration zum Migrieren von öffentlichen Exchange Online-Ordnern zu Office 365-Gruppen

18.12.2018 • 32 minutes to read

**Zusammenfassung:** So verschieben Sie öffentliche Exchange Online-Ordner in Office 365-Gruppen.

Mit einem Prozess, der auch Batchmigration genannt wird, können Sie einige oder alle Ihre öffentlichen Exchange Online-Ordner in Office 365-Gruppen verschieben. Gruppen sind ein neues Angebot von Microsoft für die Zusammenarbeit, das bestimmte Vorteile für öffentliche Ordner bietet. Unter [Migrate your public folders to Office 365 Groups](#) finden Sie einen Überblick über die Unterschiede zwischen öffentlichen Ordnern und Gruppen sowie Gründe, warum Ihre Organisation möglicherweise von einem Wechsel zu Gruppen profitieren kann.

Dieser Artikel enthält die schrittweisen Verfahren zur Durchführung der tatsächlichen Batchmigration Ihrer öffentlichen Exchange Online-Ordner.

## Was sollten Sie wissen, bevor Sie beginnen?

Stellen Sie sicher, dass alle der folgenden Bedingungen erfüllt sind, bevor Sie mit der Vorbereitung der Migration beginnen.

- Derzeit können nur öffentliche Ordner des Typs Kalender und E-Mail zu Office 365-Gruppen migriert werden. Die Migration anderer Arten öffentlicher Ordner wird nicht unterstützt. Darüber hinaus sollten die Zielgruppen in Office 365 vor der Migration erstellt werden.
- Office 365-Gruppen unterstützen keine Berechtigungsrollen und Zugriffsrechte, die in öffentlichen Ordnern verfügbar sind. In Office 365-Gruppen werden die Benutzer entweder als **Mitglieder** oder **Besitzer** bezeichnet.
- Bei der Batchmigration werden nur Nachrichten- und Kalenderelemente aus öffentlichen Ordnern für die Migration zu Office 365-Gruppen kopiert. Dabei werden keine anderen Arten von Inhalten für öffentliche Ordner kopiert, wie z. B. Regeln und Berechtigungen, da diese in Office 365-Gruppen nicht unterstützt werden.
- Office 365-Gruppen verfügen über ein Postfach mit 50 GB Speicherplatz. Stellen Sie sicher, dass die Summe der Daten aus öffentlichen Ordnern, die Sie migrieren möchten, maximal 50 GB beträgt. Lassen Sie zudem Speicherplatz frei, damit Benutzer nach der Migration, zusätzliche Inhalte hinzufügen können. Es wird empfohlen, keine öffentlichen Ordner zu migrieren, die eine Gesamtgröße von 25 GB überschreiten.
- Bei dieser Migration müssen Sie nicht zwangsläufig alles migrieren. Sie können bestimmte öffentliche Ordner für die Migration auswählen, damit nur diese öffentlichen Ordner migriert werden. Wenn der migrierten öffentlichen Ordner Unterordner enthält, werden diese Unterordner nicht automatisch in die Migration einbezogen. Wenn Sie sie migrieren möchten, müssen Sie sie ausdrücklich einbeziehen.
- Die öffentlichen Ordner werden durch diese Migration in keiner Weise beeinträchtigt. Wenn Sie jedoch unser Sperrskript verwenden, um die migrierten öffentlichen Ordner mit einem Schreibschutz zu versehen, müssen die Benutzer Office 365-Gruppen anstelle von öffentlichen Ordnern verwenden.
- Sie müssen einen einzelnen migrationsbatch verwenden, um alle Daten Ihrer öffentlichen Ordner zu migrieren. Exchange kann nur einen migrationsbatch zu einem Zeitpunkt erstellen. Wenn Sie versuchen, die gleichzeitig mehrere migrationsbatch zu erstellen, wird das Ergebnis ein Fehler.

- Bevor Sie beginnen, sollten Sie diesen Artikel vollständig lesen, da für einige Schritte Ausfallzeiten erforderlich sind.

## Schritt 1: Abrufen der Skripts

Die Batch-Migration zu Office 365-Gruppen erfordert eine Reihe von Skripts an verschiedenen Punkten bei der Migration auszuführen, wie unten in diesem Artikel beschrieben. Laden Sie die Skripts und ihre Dateienunterstützenden [aus diesem Speicherort](#). Nachdem die Skripts und Dateien heruntergeladen wurden, speichern Sie sie an den gleichen Speicherort wie `c:\PFToGroups\Scripts`.

Überprüfen Sie vor dem Fortfahren, ob Sie alle der folgenden Skripts und Dateien heruntergeladen und gespeichert haben:

### NOTE

Stellen Sie sicher, dass Sie alle Skripts und Dateien am gleichen Speicherort speichern.

- **AddMembersToGroups.ps1**. Mit diesem Skript fügen Sie basierend auf Berechtigungseinträgen in der Quelle von öffentlichen Ordner Mitglieder und Besitzer zu Office 365-Gruppen hinzu.
- **AddMembersToGroups.strings.psd1**: diese Unterstützungsdatei wird von dem Skript `AddMembersToGroups.ps1`.
- **LockAndSavePublicFolderProperties.ps1**. Dieses Skript versetzt öffentliche Ordner in den schreibgeschützten Modus, um jegliche Änderungen zu verhindern, und es überträgt die E-Mail-bezogenen Eigenschaften der öffentlichen Ordner (vorausgesetzt, die öffentlichen Ordner sind E-Mail-aktiviert) auf die Zielgruppen, die E-Mails von den öffentlichen Ordnern zu den Zielgruppen umleiten. Mit diesem Skript werden zudem die Berechtigungseinträge und die E-Mail-Eigenschaften vor der Änderung gesichert.
- **LockAndSavePublicFolderProperties.strings.psd1**: Diese Unterstützungsdatei wird von dem Skript `LockAndSavePublicFolderProperties.ps1`.
- **UnlockAndRestorePublicFolderProperties.ps1**: dieses Skript stellt Zugriffsrechte und E-Mail-Eigenschaften der öffentlichen Ordner mithilfe von erstellte Sicherungsdateien wieder her `LockandSavePublicFolderProperties.ps1`.
- **UnlockAndRestorePublicFolderProperties.strings.psd1**: diese Unterstützungsdatei wird von dem Skript `UnlockAndRestorePublicFolderProperties.ps1`.
- **WriteLog.ps1**: Dieses Skript ermöglicht es den vorhergehenden drei Skripts, Protokolle zu schreiben.
- **RetryScriptBlock.ps1**: dieses Skript ermöglicht die `AddMembersToGroups`, `LockAndSavePublicFolderProperties`, und `UnlockAndRestorePublicFolderProperties` Skripts bestimmter Aktionen im Falle vorübergehender Fehler zu wiederholen.

Ausführliche Informationen zu `AddMembersToGroups.ps1`, `LockAndSavePublicFolderProperties.ps1`, und `UnlockAndRestorePublicFolderProperties.ps1`, und die Aufgaben, die sie ausführen, in der Umgebung finden Sie unter [-Migrations-Skripts](#) weiter unten in diesem Artikel.

## Schritt 2: Vorbereiten der Migration

Die folgenden Schritte sind erforderlich, um Ihre Organisation für die Migration vorzubereiten:

1. Kompilieren Sie eine Liste der öffentlichen Ordner (E-Mail- und Kalendertypen), die Sie in Office 365-Gruppen migrieren möchten.
2. Erstellen Sie eine Liste der entsprechenden Zielgruppen für jeden öffentlichen Ordner, der migriert werden

soll. Sie können entweder eine neue Gruppe in Office 365 für jeden öffentlichen Ordner erstellen oder eine vorhandene Gruppe verwenden. Wenn Sie eine neue Gruppe erstellen, erfahren Sie unter [Weitere Informationen zu Office 365-Gruppen](#) mehr über die für eine Gruppe erforderlichen Einstellungen. Wenn bei einem öffentlichen Ordner, den Sie migrieren, die Standardberechtigung auf **Author** oder höher eingestellt ist, sollten Sie die entsprechende Gruppe in Office 365 mit der Datenschutzeinstellung **Öffentlich** erstellen. Benutzer, die die öffentliche Gruppe unter dem Knoten der **Gruppen** in Outlook anzeigen, müssen jedoch weiterhin der Gruppe beitreten.

3. Benennen Sie Öffentliche Ordner, die einen umgekehrten Schrägstrich enthalten (\) in ihrem Namen. Andernfalls diese öffentlichen Ordner möglicherweise nicht ordnungsgemäß migriert.
4. Die Migrationsfunktion **PAW** muss für Ihren Office 365-Mandanten aktiviert sein. Führen Sie den folgenden Befehl in Exchange Online PowerShell aus, um dies zu überprüfen:

```
Get-MigrationConfig
```

Wenn in der Ausgabe unter **Features** der Eintrag **PAW** aufgeführt ist, ist die Funktion aktiviert und Sie können mit *Schritt 3: Generieren der CSV-Datei* fortfahren.

Wenn KRALLE noch nicht für Ihre Mandanten aktiviert, es sein kann, da stehen Ihnen einige vorhandenen migrationsbatches, batches Öffentliche Ordner Batches oder Benutzer. Diese Batches konnte in jeder Zustand, einschließlich abgeschlossen sein. Wenn dies der Fall ist, schließen Sie, und entfernen Sie alle vorhandenen migrationsbatches, bis keine Datensätze zurückgegeben werden, bei der Ausführung `Get-MigrationBatch`. Nachdem alle vorhandenen Stapel entfernt werden, KRALLE sollte automatisch aktiviert worden. Notiz, die entsprechend der Änderung in möglicherweise nicht `Get-MigrationConfig` sofort, ist das kein Problem. Sobald dieser Schritt abgeschlossen ist, können Sie weiterhin neue Stapel von Benuttermigrationen zu erstellen.

## Schritt 3: Generieren der CSV-Datei

Erstellen Sie eine CSV-Datei, um die Eingabe für eines der Migrationsskripts bereitzustellen.

Die CSV-Datei muss die folgenden Spalten enthalten:

- **FolderPath**. Der Pfad des öffentlichen Ordners, der migriert werden soll.
- **TargetGroupMailbox**. Die SMTP-Adresse der Zielgruppe in Office 365. Sie können den folgenden Befehl ausführen, um die primäre SMTP-Adresse anzuzeigen.

```
Get-UnifiedGroup <alias of the group> | Format-Table PrimarySmtpAddress
```

CSV-Beispieldatei:

```
"FolderPath", "TargetGroupMailbox"  
\Sales", "sales@contoso.onmicrosoft.com"  
\Sales\EMEA", "emeasales@contoso.onmicrosoft.com"
```

Beachten Sie, dass ein E-Mail-Ordner und ein Kalenderordner in einer einzigen Gruppe in Office 365 zusammengeführt werden können. Alle anderen Szenarien, bei denen mehrere öffentliche Ordner in einer einzigen Gruppe zusammenführt werden, werden in einem einzigen Migrationsbatch nicht unterstützt. Wenn Sie mehrere öffentliche Ordner der gleichen Office 365-Gruppe zuordnen müssen, können Sie zu diesem Zweck unterschiedliche Migrationsbatches fortlaufend und nacheinander ausführen. Jedes Migrationsbatch kann bis zu 500 Einträge umfassen.

Ein öffentlicher Ordner sollte nur in eine Gruppe in einem Migrationsbatch migriert werden.

## Schritt 4: Starten der Migrationsanforderung

In diesem Schritt sammeln Sie Informationen aus Ihrer Exchange-Umgebung. Dann verwenden Sie diese Informationen, um ein Exchange Online PowerShell Migrationsbatch zu erstellen. Anschließend starten Sie die Migration.

1. Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um einen neuen öffentlichen Ordner im Office- 365-Gruppen-Migrationsbatch zu erstellen. Dabei gilt Folgendes:

- **CSVData** wird die CSV-Datei oben erstellte *Schritt 3: Erstellen Sie die CSV-Datei*. Achten Sie darauf, dass dieser Datei finden Sie den vollständigen Pfad angeben. Wenn die Datei aus irgendeinem Grund verschoben wurde, müssen Sie überprüfen, und verwenden Sie den neuen Speicherort.
- **AutoStart** ist ein optionaler Parameter, der verwendet wird, um den Migrationsbatch zu starten, sobald er erstellt wurde.
- **PublicFolderToUnifiedGroup** ist der Parameter, in dem angegeben ist, dass es sich um einen öffentlichen Ordner des Office 365-Gruppen-Migrationsbatches handelt.

```
New-MigrationBatch -Name PublicFolderToGroupMigration -CSVData (Get-Content <path to .csv file> -Encoding Byte) -PublicFolderToUnifiedGroup [-AutoStart]
```

2. Starten Sie die Migration mithilfe des folgenden Befehls in Exchange Online PowerShell. Beachten Sie, dass dieser Schritt erforderlich ist nur, wenn die `-AutoStart` Parameter wurde nicht bei der Erstellung des Batches oben in Schritt 1 verwendet.

```
Start-MigrationBatch PublicFolderToGroupMigration
```

Während Migrationen Batch mit erstellt werden, müssen die `New-MigrationBatch` -Cmdlet in Exchange Online PowerShell den Fortschritt der Migration kann angezeigt und in der Exchange-Verwaltungskonsole verwaltet werden. Sie können auch den Fortschritt der Migration anzeigen, indem Sie die Cmdlets `Get-MigrationBatch` und `Get-MigrationUser` ausführen. Die `New-MigrationBatch` Cmdlet initiiert einen Migrationsbenutzer für jedes Postfach der Office 365-Gruppe, und Sie können den Status der diese Anforderungen mithilfe der Seite Postfach Migration anzeigen.

So zeigen Sie die Seite der Postfachmigration an:

1. Öffnen Sie in Exchange Online Exchange-Verwaltungskonsole.
2. Navigieren Sie zu **Empfänger**, und wählen Sie **Migration** aus.
3. Wählen Sie die soeben erstellte Migrationsanforderung aus, und klicken Sie im Bereich **Details** auf **Details anzeigen**.

Wenn der Batchstatus **Abgeschlossen** lautet, können Sie mit *Schritt 5 fortfahren: Fügen Sie Mitglieder aus öffentlichen Ordnern zu Office 365-Gruppen hinzu*.

## Schritt 5: Hinzufügen von Mitglieder aus öffentlichen Ordnern zu Office 365-Gruppen

Sie können die Mitglieder der Zielgruppe in Office 365 nach Bedarf manuell hinzufügen. Jedoch, wenn Sie Mitglieder der Gruppe basierend auf der Berechtigungseinträge in öffentlichen Ordnern hinzufügen möchten, müssen Sie dafür durch Ausführen des Skripts `AddMembersToGroups.ps1` wie in den folgenden Befehl gezeigt. Wenn

Sie wissen, welche Berechtigungen für Öffentliche Ordner, die als Mitglieder einer Gruppe in Office 365 hinzugefügt werden können, finden Sie weiter unten in diesem Artikel [Migrations-Skripts](#).

Hinweise zum folgenden Befehl:

- **MappingCsv** ist die CSV-Datei, die Sie in *Schritt 3: Generieren der CSV-Datei* erstellt haben. Achten Sie darauf, den vollständigen Pfad zu dieser Datei anzugeben. Falls die Datei aus irgendeinem Grund verschoben wurde, müssen Sie unbedingt den neuen Speicherort überprüfen und angeben.
- **BackupDir** ist das Verzeichnis, in dem die Migrationsprotokolldateien gespeichert werden.
- **ArePublicFoldersOnPremises** ist ein Parameter, mit dem angegeben werden kann, ob sich öffentliche Ordner auf einem lokalen Server oder in Exchange Online befinden.

```
.\\AddMembersToGroups.ps1 -MappingCsv <path to .csv file> -BackupDir <path to backup directory> -ArePublicFoldersOnPremises $false
```

Sobald Benutzer zu einer Gruppe in Office 365 hinzugefügt wurden, können sie diese verwenden.

## Schritt 6: Sperren der öffentlichen Ordner (Downtime der öffentlichen Ordner erforderlich)

Wenn die Mehrzahl der Daten in Ihren öffentlichen Ordnern zu Office 365 Gruppen migriert wurde, können Sie das Skript ausführen `LockAndSavePublicFolderProperties.ps1` zu öffentlichen Ordnern schreibgeschützt festlegen. Dieser Schritt wird sichergestellt, dass keine neuen Daten vor dem Abschluss der Migration öffentlicher Ordner hinzugefügt werden.

### NOTE

Wenn in den migrierten öffentlichen Ordnern E-Mail-aktivierte öffentliche Ordner (MEPFs) vorhanden sind, werden in diesem Schritt einige Eigenschaften der MEPFs, wie z. B. SMTP-Adressen, in die entsprechende Gruppe in Office 365 kopiert und die E-Mail-Funktionen für die öffentlichen Ordner deaktiviert. Da die E-Mail-Funktionen der migrierten MEPFs nach der Ausführung dieses Skripts deaktiviert werden, werden an die MEPFs gesandte E-Mails in den entsprechenden Gruppen empfangen. Weitere Informationen hierzu finden Sie unter [Migrationsskripts](#) weiter unten in diesem Artikel.

Hinweise zum folgenden Befehl:

- **MappingCsv** ist die CSV-Datei, die Sie in *Schritt 3: Generieren der CSV-Datei* erstellt haben. Achten Sie darauf, den vollständigen Pfad zu dieser Datei anzugeben. Falls die Datei aus irgendeinem Grund verschoben wurde, müssen Sie unbedingt den neuen Speicherort überprüfen und angeben.
- **BackupDir** ist das Verzeichnis, in dem die Sicherungsdateien für Berechtigungseinträge, MEPF-Eigenschaften und Migrationsprotokolldateien gespeichert werden. Diese Sicherung wird nützlich sein, falls Sie einmal ein Rollback auf öffentliche Ordner durchführen müssen.
- **ArePublicFoldersOnPremises** ist ein Parameter, mit dem angegeben werden kann, ob sich öffentliche Ordner auf einem lokalen Server oder in Exchange Online befinden.

```
.\\LockAndSavePublicFolderProperties.ps1 -MappingCsv <path to .csv file> -BackupDir <path to backup directory> -ArePublicFoldersOnPremises $false
```

## Schritt 7: Fertigstellen des öffentlichen Ordners für die Migration in Office 365-Gruppen

Nachdem Sie Ihre öffentliche Ordner mit einem Schreibschutz versehen haben, müssen Sie die Migration erneut ausführen. Dies ist für eine endgültige inkrementelle Kopie der Daten erforderlich. Bevor Sie die Migration erneut ausführen können, müssen Sie den vorhandenen Batch entfernen, indem Sie den folgenden Befehl ausführen:

```
Remove-MigrationBatch <name of migration batch>
```

Erstellen Sie anschließen einen neuen Batch mit der gleichen CSV-Datei, indem Sie den folgenden Befehl ausführen. Dabei gilt Folgendes:

- **CSVData** wird die CSV-Datei oben erstellte *Schritt 3: Erstellen Sie die CSV-Datei*. Achten Sie darauf, dass dieser Datei finden Sie den vollständigen Pfad angeben. Wenn die Datei aus irgendeinem Grund verschoben wurde, müssen Sie überprüfen, und verwenden Sie den neuen Speicherort.
- **NotificationEmails** ist ein optionaler Parameter, der verwendet werden kann, um E-Mail-Adressen festzulegen, an die Benachrichtigungen über den Status und Fortschritt der Migration übermittelt werden.
- **AutoStart** ist ein optionaler Parameter, der verwendet wird, um den Migrationsbatch zu starten, sobald er erstellt wurde.

```
New-MigrationBatch -Name PublicFolderToGroupMigration -CSVData (Get-Content <path to .csv file> -Encoding Byte) -PublicFolderToUnifiedGroup [-NotificationEmails <email addresses for migration notifications>] [-AutoStart]
```

Nachdem das neue Blatt erstellt wurde, starten Sie die Migration mithilfe des folgenden Befehls in Exchange Online PowerShell. Beachten Sie, dass dieser Schritt nur erforderlich ist, wenn die `-AutoStart` Parameter wurde nicht im vorstehenden Befehl verwendet.

```
Start-MigrationBatch PublicFolderToGroupMigration
```

Nachdem Sie diesen Schritt abgeschlossen haben (der Batchstatus lautet **Abgeschlossen**), stellen Sie sicher, dass alle Daten in die Office 365-Gruppen kopiert wurden. Wenn Sie mit der Gruppen-Erfahrung zufrieden sind, können Sie nun beginnen, die migrierten öffentlichen Ordner aus Ihrer Exchange Online-Umgebung zu löschen.

#### IMPORTANT

Es gibt zwar unterstützte Verfahren zum Zurücksetzen der Migration und zur Rückkehr zu öffentlichen Ordnern, dies ist jedoch nicht mehr möglich, nachdem die ursprünglichen öffentlichen Ordner gelöscht wurden. Weitere Informationen finden Sie unter [Wie führe ich ein Rollback von Office 365-Gruppen zu öffentlichen Ordnern durch?](#).

## Bekannte Probleme

Die folgenden bekannten Probleme können während einer normalen Migration von öffentlichen Ordnern zu Office 365-Gruppen auftreten.

- Das Skript, das die SMTP-Adresse aus den E-Mail-aktivierten öffentlichen Ordnern in die Office 365-Gruppe überträgt, fügt die Adressen lediglich als sekundäre E-Mail-Adressen in Exchange Online hinzu. Wenn Sie Exchange Online Protection (EOP) oder die zentralisierte Nachrichtenübermittlung in Ihrer Umgebung eingerichtet haben, gibt es nach der Migration Probleme beim Senden von E-Mails an Gruppen (an die sekundären E-Mail-Adressen).
- Weist die CSV-Zuordnungsdatei einen Eintrag mit ungültigem Pfad zum öffentlichen Ordner auf, wird das Migrationsbatch ohne Fehler als **abgeschlossen** angezeigt, und keine weiteren Daten werden kopiert.

# Migrationsskripts

Als Referenz enthält dieser Abschnitt detaillierte Beschreibungen für drei der Migrationsskripts und Aufgaben, die sie in Ihrer Exchange-Umgebung ausführen. Laden Sie die Skripts und die dazugehörigen unterstützenden Dateien von diesem Speicherort herunter herunter.

## AddMembersToGroups.ps1

Mit diesem Skript werden die Berechtigungen der öffentlichen Ordner migriert, anschließend werden die Mitglieder und Besitzer folgendermaßen zu Office 365-Gruppen hinzugefügt:

- Benutzer mit folgenden Berechtigungsrollen werden als Mitglieder zu einer Gruppe in Office 365 hinzugefügt. **Berechtigungsrollen** Besitzer, PublishingEditor, Editor, PublishingAuthor, Autor
- Darüber hinaus werden Benutzer mit den Mindestzugriffsrechten ebenfalls als Mitglieder zu einer Gruppe in Office 365 hinzugefügt. **Zugriffsrechte**: ReadItems, CreateItems, FolderVisible, EditOwnedItems, DeleteOwnedItems
- Benutzer mit der Zugriffsberechtigung „Besitzer“ werden als Besitzer einer Gruppe hinzugefügt, und Benutzer mit anderen berechtigten Zugriffsrechten werden als Mitglieder hinzugefügt.
- Sicherheitsgruppen können nicht als Mitglieder zu Gruppen in Office 365 hinzugefügt werden. Daher werden diese erweitert, und anschließend werden die einzelnen Benutzer als Mitglieder oder Besitzerauf Grundlage der Zugriffsrechte auf die Sicherheitsgruppe zu den Gruppen hinzugefügt.
- Wenn Benutzer mit Zugriffsrechten über einen öffentlichen Ordner in Sicherheitsgruppen selbst über ausdrückliche Berechtigungen über denselben öffentlichen Ordner verfügen, werden die ausdrücklichen Berechtigungen priorisiert behandelt. Sehen wir uns beispielsweise einen Fall an, in dem eine Sicherheitsgruppe mit der Bezeichnung „SG1“ als Mitglieder Benutzer1 und Benutzer2 enthält. Berechtigungseinträge für den öffentlichen Ordner „PF1“ lauten wie folgt:

SG1: Autor in PF1

Benutzer1: Besitzer in PF1

In diesem Fall wird Benutzer1 als Besitzer zur Gruppe in Office 365 hinzugefügt werden.

- Wenn die Standardberechtigung eines öffentlichen zu migrierenden Ordners „Autor“ oder höher lautet, schlägt das Skript vor, Datenschutzeinstellungen der entsprechenden Gruppe als „Öffentlich“ festzulegen.

Dieses Skript ausgeführt werden kann, auch nach der gesperrt öffentlicher Ordner, mit dem Parameter `ArePublicFoldersLocked` legen Sie auf `$true`. In diesem Szenario wird das Skript Berechtigungen Sichern während gesperrt erstellte Datei gelesen werden.

## LockAndSavePublicFolderProperties.ps1

Dieses Skript versieht die zu migrierenden öffentlichen Ordner mit einem Schreibschutz. Beim Migrieren von E-Mail-aktivierten öffentlichen Ordnern sind sie zunächst E-Mail-deaktiviert und ihre SMTP-Adressen werden zu den entsprechenden Gruppen in Office 365 hinzugefügt. Anschließend werden die Berechtigungseinträge geändert, damit sie schreibgeschützt sind. Eine Sicherung der E-Mail-Eigenschaften der E-Mail-aktivierten öffentlichen Ordner sowie die Berechtigungseinträge aller öffentlichen Ordner werden vor dem Ausführen von Änderungen kopiert.

Wenn es mehrere Migrationsbatches gibt, sollte für jede CSV-Zuordnungsdatei ein separates Sicherungsverzeichnis verwendet werden.

Folgenden E-Mail-Eigenschaften werden zusammen mit den E-Mail-aktivierten öffentlichen Ordnern und Office 365-Gruppen gespeichert:

- PrimarySMTPAddress

- EmailAddresses
- ExternalEmailAddress
- EmailAddressPolicyEnabled
- GrantSendOnBehalfTo
- SendAs-Vertrauensnehmerliste

Die oben angegebenen E-Mail-Eigenschaften werden in einer CSV-Datei gespeichert, die im Rollback verwendet wird (wenn Sie zur Verwendung von öffentlichen Ordner zurückkehren möchten, finden Sie weitere Informationen unter [Wie führe ich ein Rollback von Office 365-Gruppen zu öffentlichen Ordner durch?](#)). Eine Momentaufnahme der Eigenschaften E-Mail-aktivierter Ordner wird außerdem in einer Datei mit der Bezeichnung PfMailProperties.csv gespeichert. Diese Datei ist für das Rollback nicht erforderlich, Sie können Sie jedoch als Referenz verwenden.

Die folgenden E-Mail-Eigenschaften werden als Teil der Sperre in die Zielgruppe migriert:

- PrimarySMTPAddress
- EmailAddresses
- SendAs-Vertrauensnehmerliste
- GrantSendOnBehalfTo

Das Skript stellt sicher, dass die PrimarySMTPAddress und EmailAddresses der zu migrierenden E-Mail-aktivierten öffentlichen Ordner als sekundäre SMTP-Adressen der entsprechenden Gruppen in Office 365 hinzugefügt werden. Darüber hinaus erhalten SendAs- und SendOnBehalfTo-Berechtigungen von Benutzern für E-Mail-aktivierte öffentliche Ordner die entsprechende Berechtigung in den entsprechenden Zielgruppen.

#### **Zulässige Zugriffsrechte:**

Nur folgende Zugriffsrechte sind für Benutzer zulässig, damit sichergestellt ist, dass die öffentlichen Ordner für alle Benutzer mit einem Schreibschutz versehen werden. Diese werden in den **ListOfAccessRightsAllowed** gespeichert.

- ReadItems
- CreateSubfolders
- FolderContact
- FolderVisible

Die Berechtigungseinträge werden wie folgt geändert:

1.

VOR DEM SPERREN	NACH DEM SPERREN
Keine	Keine
AvailabilityOnly	AvailabilityOnly
LimitedDetails	LimitedDetails
Mitwirkender	FolderVisible

VOR DEM SPERREN	NACH DEM SPERREN
Reviewer	ReadItems FolderVisible
NonEditingAuthor	ReadItems FolderVisible
Aughor	ReadItems FolderVisible
Editor	ReadItems FolderVisible
PublishingAuthor	ReadItems, CreateSubfolders, FolderVisible
Vom Typ PublishingEditor	ReadItems, CreateSubfolders, FolderVisible
Besitzer	ReadItems, CreateSubfolders, FolderContact, FolderVisible

2. Zugriffsrechte für Benutzer ohne Leseberechtigungen bleiben unverändert und erhalten weiterhin keine Leserechte.

3. Für Benutzer mit benutzerdefinierten Rollen werden alle Zugriffsrechte, die nicht in **ListOfAccessRightsAllowed** enthalten sind, entfernt. Für den Fall, dass die Benutzer nach dem Filtern keine Zugriffsrechte aus der zulässigen Liste erhalten haben, wird das Zugriffsrecht dieser Benutzer auf „Keine“ festgelegt.

Möglicherweise gibt es eine Unterbrechung beim Senden von E-Mails an E-Mail-aktivierte öffentliche Ordner für den Zeitraum, wenn die Ordner E-Mail-deaktiviert sind und ihre SMTP-Adressen zu den Office 365-Gruppen hinzugefügt werden.

#### **UnlockAndRestorePublicFolderProperties.ps1**

Dieses Skript weist die Berechtigungen auf Grundlage der Sicherungsdatei wieder den öffentlichen Ordnern zu, die während des Sperrens des öffentlichen Ordners erstellt wurde. Dieses Skript E-Mail-aktiviert zuvor E-Mail-deaktivierte öffentliche Ordner, nachdem es die SMTP-Adressen der Ordner aus den entsprechenden Gruppen in Office 365 entfernt hat. Es gibt möglicherweise eine geringe Ausfallzeit während dieses Vorgangs.

## Wie führe ich ein Rollback von Office 365-Gruppen zu öffentlichen Ordnern durch?

Für den Fall, dass Sie Ihre Meinung ändern und zu öffentliche Ordnern zurückkehren möchten, nachdem Sie Office 365-Gruppen verwendet haben, wird Ihre Umgebung durch den nachstehenden Befehl auf den Zustand vor der Migration zurückgesetzt. Ein Rollback kann ausgeführt werden, solange die Sicherungsdateien vorhanden sind und solange Sie die öffentlichen Ordner nach der Migration nicht gelöscht haben.

Führen Sie den folgenden Befehl aus. Dabei gilt Folgendes:

- **BackupDir** ist das Verzeichnis, in dem die Sicherungsdateien für Berechtigungseinträge, MEPF-Eigenschaften und Migrationsprotokolldateien gespeichert werden. Vergewissern Sie sich, dass Sie denselben Speicherort verwenden, den Sie in *Schritt 6 angegeben haben: Sperren der öffentlichen Ordner (Downtime der öffentlichen Ordner erforderlich)*.
- **ArePublicFoldersOnPremises** ist ein Parameter, mit dem angegeben werden kann, ob sich öffentliche Ordner auf einem lokalen Server oder in Exchange Online befinden.

```
.\\UnlockAndRestorePublicFolderProperties.ps1 -BackupDir <path to backup directory> -ArePublicFoldersOnPremises  
$false
```

Beachten Sie, dass alle zu Gruppen in Office 365 hinzugefügte Elemente oder in den Gruppen durchgeführte Bearbeitungsvorgänge nicht zurück in die öffentlichen Ordner kopiert werden. Deshalb gehen Daten verloren, unter der Voraussetzung, dass neue Daten hinzugefügt wurden, als der öffentliche Ordner eine Gruppe war.

Beachten Sie außerdem, dass es nicht möglich ist, einen Teil der öffentlichen Ordner wiederherzustellen, d. h. alle öffentlichen Ordner, die migriert wurden, sollten wiederhergestellt werden.

Die entsprechenden Gruppen in Office 365 werden nicht als Teil des Rollbacks gelöscht. Sie müssen diese Gruppen manuell bereinigen oder löschen.

# Konfigurieren lokaler öffentlicher Ordner aus Vorversionen für eine Hybridbereitstellung

18.12.2018 • 15 minutes to read

**Zusammenfassung:** Verwenden Sie die Schritte in diesem Artikel zum Synchronisieren von öffentlicher Ordnern zwischen Office 365 und Ihrer lokalen Exchange Server 2010-Bereitstellung.

In einer hybridbereitstellung können Ihre Benutzer in Exchange Online, lokalen oder beides, und Ihre öffentlichen Ordner sind entweder im Exchange Online oder lokalen. Öffentliche Ordner können nur einmal werden, und Sie müssen entscheiden, ob Ihre öffentlichen Ordner in Exchange Online oder lokalen sein werden. In beiden Quellen ist nicht möglich. Postfächer für Öffentliche Ordner werden vom Dienst Directory-Synchronisierung mit Exchange Online synchronisiert. Allerdings werden nicht über lokale e-Mail-aktivierten Öffentlichen Ordner synchronisiert.

In diesem Thema wird beschrieben, wie e-Mail-aktivierte Öffentliche Ordner synchronisieren, wenn Ihre Benutzer befinden sich in Office 365 und Ihre öffentlichen Ordner von Exchange Server 2010 SP3 lokale sind. Allerdings werden nicht Office 365-Benutzer, die nicht durch ein MailUser-Objekt: lokal (lokal in der Ziel-Hierarchie Öffentlicher Ordner) dargestellt wird veraltete oder modernen lokale Öffentliche Ordner zugreifen kann.

## NOTE

Dieses Thema bezieht sich auf die Exchange Server 2010 SP3-Server als Exchange-Legacyserver.

Sie werden Ihre e-Mail-aktivierten Öffentlichen Ordner synchronisiert, mithilfe der folgenden Skripts, der von einer Windows-Aufgabe initiiert werden, die in der lokalen Umgebung ausgeführt wird:

- `Sync-MailPublicFolders.ps1` : Mit diesem Skript werden e-Mail-aktivierte Öffentliche Ordner-Objekte aus der lokalen Exchange-lokale Bereitstellung mit Office 365 synchronisiert. Die lokale Bereitstellung in lokalen Exchange verwendet um zu bestimmen, welche Änderungen auf O365 angewendet werden müssen als Master. Das Skript erstellen, aktualisieren oder Löschen von e-Mail-aktivierten Öffentlichen Ordner-Objekten auf O365 Active Directory basierend auf was in der lokalen lokalen Exchange-Bereitstellung vorhanden ist.
- `SyncMailPublicFolders.strings.ps1` : Dies ist eine Unterstützungsdatei, die von der dieses Synchronisierungsskript verwendet und sollte an den gleichen Speicherort wie die vorhergehenden Skripts kopiert werden.

Wenn Sie dieses Verfahren abschließen, können Ihre lokalen und Office 365-Benutzer auf die gleiche lokale öffentliche Ordner-Infrastruktur zugreifen.

## Welche Hybridversionen von Exchange sind mit Öffentlichen Ordnern kompatibel?

Die folgende Tabelle enthält die unterstützten Versions- und Speicherortkombinationen von Benutzerpostfächern und Öffentlichen Ordnern. "Hybrid nicht möglich" ist ein unterstütztes Szenario, gilt aber nicht als Hybridszenario, da Öffentliche Ordner und Benutzer den gleichen Speicherort aufweisen.

	LOKALE EXCHANGE 2010-BENUTZERPOSTFACH	LOKALES BENUTZERPOSTFACH IN EXCHANGE 2013	EXCHANGE ONLINE-BENUTZERPOSTFACH
Lokale Exchange 2010 Öffentliche Ordner	Hybrid nicht zutreffend	Hybrid nicht zutreffend	Unterstützt
Lokale Öffentliche Ordner in Exchange 2013	Hybrid nicht zutreffend	Hybrid nicht zutreffend	Unterstützt
Öffentliche Ordner in Exchange Online	Nicht unterstützt	Unterstützt	Hybrid nicht zutreffend

#### NOTE

Zugreifen auf Exchange 2007 ältere öffentliche Ordner unterstützt 2016 Outlook nicht. Wenn Sie Benutzer Outlook 2016 verwenden, müssen Sie Ihre öffentlichen Ordner zu einer neueren Version von Exchange Server verschieben. Weitere Informationen zu Outlook 2016 und 2016 Office-Kompatibilität mit Exchange 2007 und früheren Versionen finden Sie in [diesem Artikel](#).

## Schritt 1: Was haben Sie wissen, bevor Sie beginnen?

- Diese Anweisungen wird davon ausgegangen, dass Sie den Konfigurations-Assistenten für Hybrid verwendet haben, konfigurieren und Synchronisieren der lokalen und Exchange Online-Umgebung und die DNS-Einträge, die für die AutoErmittlung verwendet werden für die meisten Benutzer Verweis-service ein lokaler Endpunkt. Weitere Informationen finden Sie unter [Hybrid Configuration Wizard](#).
- Diese Anweisungen wird davon ausgegangen, dass Outlook Anywhere aktiviert und auf alle lokalen älteren Exchange Server für Öffentliche Ordner funktionsfähig ist. Informationen dazu, wie Sie Outlook Anywhere zu aktivieren finden Sie unter [Outlook Anywhere](#).
- Implementieren der Koexistenz der Vorversion für Öffentliche Ordner für eine hybridbereitstellung von Exchange mit Office 365 erfordern möglicherweise beheben von Konflikten beim Import. Konflikte können auftreten, da von Konflikten mit anderen Benutzern und Gruppen in Office 365 und aus anderen Gründen eine nicht-routingfähigen e-Mail-Adresse, die e-Mail-aktivierte Öffentliche Ordner zugeordnet ist.
- Diese Anweisungen wird davon ausgegangen, dass die Exchange Online-Organisation auf eine Version aktualisiert wurde, die Öffentliche Ordner unterstützt.
- In Exchange Online müssen Sie Mitglied der Rollengruppe "Organisationsverwaltung" sein. Dieser Rollengruppe unterscheidet sich von den Berechtigungen, die Ihnen zugewiesen werden, wenn Sie Exchange Online abonnieren. Informationen zum Aktivieren der Rollengruppe "Organisationsverwaltung" finden Sie unter [Manage Role Groups](#).
- In Exchange 2010 müssen Sie ein Mitglied der Rollengruppen "Organisationsverwaltung" oder "Server Management RBAC" sein. Nähere Informationen finden Sie unter [Hinzufügen von Mitgliedern zu einer Rollengruppe](#)
- Zugriff auf Öffentliche Ordner standortübergreifenden müssen Benutzer ihre Outlook-Clients auf vom November 2012 aktualisieren öffentlichen Outlook-Update oder eine höhere Version.
  1. Unter [Update für Microsoft Outlook 2010 \(KB2687623\) 32-Bit-Edition](#) können Sie das Outlook-Update vom November 2012 für Outlook 2010 herunterladen.
  2. Unter [Update für Microsoft Office Outlook 2007 \(KB2687404\)](#) können Sie das Outlook-Update vom November 2012 für Outlook 2007 herunterladen.

- Outlook 2016 für Mac (und früheren Versionen) und Outlook für Mac für Office 365 werden für standortübergreifende ältere öffentliche Ordner nicht unterstützt. Benutzer müssen in den gleichen Speicherort wie der öffentlichen Ordner, die mit Outlook für Mac oder Outlook für Mac für Office 365, darauf zugreifen können. Darüber hinaus wird nicht Benutzer, deren Postfächer in Exchange Online sind, lokale Öffentliche Ordner mit Outlook Web App zugreifen können.
- Nachdem Sie die Anweisungen in diesem Artikel zum Konfigurieren Ihrer lokalen öffentlichen Ordner für eine hybridbereitstellung zu befolgen, werden nicht Benutzer, die sich außerhalb Ihrer Organisation befinden Nachrichten an Ihre lokale Öffentliche Ordner senden, wenn Sie zusätzliche Schritte erforderlich. Sie können entweder die akzeptierte Domäne für die Öffentliche Ordner auf Internes Relay festlegen (siehe [Verwalten akzeptierte Domänen im Exchange, Online](#)) oder deaktivieren Sie Directory basierend Edge-Blockierung (DBEB) (siehe [Verwendung verzeichnisbasierte Edge-Blockierung zum Ablehnen von Nachrichten an Ungültige Empfänger](#)).

## Schritt 2: Sichtbarmachen von remote gespeicherten Öffentlichen Ordnern

- Wenn Ihre öffentlichen Ordner auf Exchange 2010 oder höher Servern befinden, müssen Sie die Clientzugriffs-Serverrolle (CAS) auf allen Postfachservern installieren, die Öffentliche Ordner-Datenbank verfügen. Dadurch wird den Dienst Microsoft Exchange-RpcClientAccess ausgeführt werden, sodass alle Clients auf Öffentliche Ordner zugreifen können. Weitere Informationen finden Sie unter [Installieren von Exchange Server 2010](#).

**NOTE**

Dieser Server muss nicht Teil des Lastenausgleichs von Clientzugriffsservern sein. Weitere Informationen finden Sie unter [Grundlegendes zum Lastenausgleich in Exchange 2010](#).

- Erstellen Sie eine leere Postfachdatenbank auf jedem Server für öffentliche Ordner.

Führen Sie für Exchange 2010 den folgenden Befehl ein. Dieser Befehl schließt die Postfachdatenbank aus der Lastenausgleichskonfiguration der Postfach-Bereitstellung. Dadurch wird verhindert, dass neue Postfächer automatisch in diese Datenbank hinzugefügt wird.

```
New-MailboxDatabase -Server <PFServerName_with_CASRole> -Name <NewMDBforPFs> -IsExcludedFromProvisioning $true
```

**NOTE**

Es wird empfohlen, dass Sie nur das Proxypostfach, das Sie in Schritt 3 erstellen, zu dieser Datenbank hinzufügen. In dieser Postfachdatenbank sollten keine anderen Postfächer erstellt werden.

- Erstellen eines Postfachs Proxy innerhalb der neuen Postfachdatenbank, und blenden Sie das Postfach aus dem Adressbuch. Der SMTP-Server für dieses Postfach wird von AutoErmittlung als *DefaultPublicFolderMailbox* SMTP, zurückgegeben werden, so dass durch das Auflösen dieser SMTP der Client den legacy-Exchange-Server für den Zugriff auf Öffentliche Ordner zugreifen kann.

```
New-Mailbox -Name <PFMailbox1> -Database <NewMDBforPFs>
```

```
Set-Mailbox -Identity <PFMailbox1> -HiddenFromAddressListsEnabled $true
```

4. Aktivieren Sie bei Exchange 2010 die AutoErmittlung, um die Proxypostfächer für öffentliche Ordner zurückzugeben.

```
Set-MailboxDatabase <NewMDBforPFs> -RPCClientAccessServer <PFServerName_with_CASRole>
```

5. Wiederholen Sie die vorhergehenden Schritte für jeden Öffentlichen Ordner-Server in Ihrer Organisation.

## Schritt 3: Herunterladen der Skripts

1. Laden Sie unter [Mail-enabled Public Folders - directory sync script](#) die folgenden Dateien herunter:

- [Sync-MailPublicFolders.ps1](#)
- [SyncMailPublicFolders.strings.psd1](#)

2. Speichern Sie die Dateien auf dem lokalen Computer, auf dem Sie PowerShell ausführen. Verwenden Sie als Speicherort beispielsweise C:\PFSscripts.

## Schritt 4: Konfigurieren der Verzeichnissynchronisierung

Der Verzeichnissynchronisierungsdienst synchronisieren nicht e-Mail-aktivierte Öffentliche Ordner. Das folgende Skript ausführen, werden die e-Mail-aktivierten Öffentlichen Ordner über lokale synchronisiert. Spezielle Berechtigungen für e-Mail-aktivierten Öffentlichen Ordner müssen in der Cloud wiederhergestellt werden, da Cross standortbasierte Berechtigung werden in Szenarien für die Hybridbereitstellung nicht unterstützt. Weitere Informationen finden Sie unter [Exchange Server-Hybridbereitstellung](#).

### NOTE

Synchronisierte E-Mail-aktivierte öffentliche Ordner werden für Nachrichtenflusszwecke als E-Mail-Kontaktobjekte angezeigt und werden im Exchange-Verwaltungskonsole nicht angezeigt. Siehe „Get-MailPublicFolder“-Befehl. Verwenden Sie zum erneuten Erstellen der SendAs-Berechtigungen in der Cloud den „RecipientPermission“-Befehl.

Führen Sie auf dem älteren Exchange-Server den folgenden Befehl zum Synchronisieren von E-Mail-aktivierten öffentlichen Ordner vom lokalen Active Directory mit O365 aus.

```
...
Sync-MailPublicFolders.ps1 -Credential (Get-Credential) -CsvSummaryFile "<sync_summary.csv>"
```

In denen Sie für Office 365-Benutzernamen und Ihr Kennwort aufgefordert werden, und \_ <Sync\_summary.csv> \_ ist der Pfad, in dem Sie Synchronisierungsvorgänge und Fehler, in der CSV-Format erfassen möchten.

### NOTE

Vor dem Ausführen des Skripts, wird empfohlen, dass Sie zunächst die Aktionen, die das Skript ausführen würden in Ihrer Umgebung simulieren ausgeführt wird, wie oben beschrieben, mit dem Parameter *WhatIf*. > Es wird auch empfohlen, dass Sie dieses Skript täglich ausführen, um Ihre e-Mail-aktivierten Öffentlichen Ordner zu synchronisieren.

## Schritt 5: Konfigurieren des Zugriffs auf lokale öffentliche Ordner für Exchange Online-Benutzer

Der letzte Schritt in diesem Verfahren ist, die Exchange Online-Organisation zu konfigurieren und Zugriff auf die

älteren lokalen öffentlichen Ordner zu gewähren.

Aktivieren Sie die Exchange-Onlineorganisation für den Zugriff auf lokale Öffentliche Ordner. Sie zeigen auf alle Öffentliche Ordner-Proxypostfächer, die Sie in [Schritt 2: Sichtbarmachen von remote gespeicherten Öffentlichen Ordnern](#) erstellt haben.

Führen Sie in **Exchange Online PowerShell** den folgenden Befehl aus:

```
Set-OrganizationConfig -PublicFoldersEnabled Remote -RemotePublicFolderMailboxes  
PFMailbox1,PFMailbox2,PFMailbox3
```

Die Änderungen werden erst angezeigt, wenn die Active Directory-Synchronisierung abgeschlossen ist. Es kann bis zu 3 Stunden dauern, bis dieser Vorgang abgeschlossen ist. Wenn Sie nicht auf die sich wiederholenden Synchronisierungen warten möchten, die alle drei Stunden stattfinden, können Sie die Verzeichnissynchronisierung jederzeit erzwingen. Ausführliche Schritte für das Erzwingen der Verzeichnissynchronisierung finden Sie unter [Erzwingen der Verzeichnissynchronisierung](#). Office 365 wählt nach dem Zufallsprinzip ein Postfach für öffentliche Ordner, das in diesem Befehl angegeben wird.

#### **IMPORTANT**

Office 365-Benutzer, die nicht von einem lokalen MailUser-Objekt repräsentiert werden (lokal in der Zielhierarchie von öffentlichen Ordner), können nicht auf öffentliche Ordner in Exchange 2013 oder älteren Versionen zugreifen. Eine Lösung dazu finden Sie im Knowledge Base-Artikel [Exchange Online-Benutzer können nicht auf öffentliche Ordner in Legacy-Versionen zugreifen](#).

## Woher weiß ich, dass der Vorgang erfolgreich war?

Melden Sie sich bei Outlook für einen Benutzer, der in Exchange Online ist, und führen Sie dann die folgenden Tests für Öffentliche Ordner aus:

- Zeigen Sie die Hierarchie an.
- Prüfen Sie die Berechtigungen.
- Erstellen und löschen Sie Öffentliche Ordner.
- Veröffentlichen Sie Inhalte in einem Öffentlichen Ordner, und löschen Sie diese.

# Konfigurieren von öffentlichen Ordnern von Exchange Server für eine hybridbereitstellung

18.12.2018 • 9 minutes to read

**Zusammenfassung:** Anleitung zum Aktivieren von Exchange Online-Benutzern Zugriff auf lokale Öffentliche Ordner in der Exchange Server-Umgebung.

In einer hybridbereitstellung können Ihre Benutzer in Exchange Online, lokalen oder beides, und Ihre öffentlichen Ordner sind entweder im Exchange Online oder lokalen. Manchmal müssen Ihre online-Benutzer Zugriff auf Öffentliche Ordner in Ihrer lokalen Exchange Server-Umgebung. In ähnlicher Weise müssen Exchange Server-Benutzer Zugriff auf Öffentliche Ordner in Office 365 oder Exchange Online.

## NOTE

Wenn Sie Öffentliche Ordner von Exchange 2010 haben, finden Sie unter [Configure legacy lokaler öffentlicher Ordner für eine hybridbereitstellung](#).

In diesem Artikel wird beschrieben, wie Exchange Online/Office 365-Benutzer Zugriff auf Öffentliche Ordner in Exchange Server zu aktivieren. Um lokale Exchange Server-Benutzer für den Zugriff auf Öffentliche Ordner in Exchange Online finden Sie unter [Konfigurieren von Exchange Online Öffentliche Ordner für eine hybridbereitstellung](#) zu aktivieren.

Exchange Online/Office 365-Benutzer muss ein MailUser-Objekt in der lokalen Exchange-Umgebung, um Zugriff auf Öffentliche Ordner von Exchange Server dargestellt werden. Dieses Objekt MailUser muss auch an das Ziel des Exchange-Server Öffentliche Ordner-Hierarchie lokal sein. Wenn Sie haben dargestellt Office 365-Benutzer, die nicht aktuell sind lokale-MailUser-Objekte, finden Sie in der Microsoft Knowledge Base-Artikel 3106618 "Exchange Online-Benutzer können nicht die älteren lokalen öffentlichen Ordner zugreifen", um die entsprechende lokalen erstellen Entitäten.

## Was sollten Sie wissen, bevor Sie beginnen?

- Bei diesen Anleitungen wird davon ausgegangen, dass Sie zur Konfiguration und Synchronisierung Ihrer lokalen und Exchange Online-Umgebungen den Assistenten für die Hybridkonfiguration verwendet haben, und dass die DNS-Einträge für die AutoErmittlung bei den meisten Benutzern auf einen lokalen Endpunkt verweisen. Weitere Informationen finden Sie unter [Hybrid Configuration Wizard](#).
- Bei diesen Anweisungen wird vorausgesetzt, dass Outlook Anywhere aktiviert und auf den lokalen Exchange-Servern funktionsbereit ist. Weitere Informationen über das Aktivieren von Outlook Anywhere finden Sie unter [Outlook Anywhere](#).
- Bei der Implementierung der Koexistenz öffentlicher Ordner für eine Hybridbereitstellung von Exchange mit Office 365 müssen Sie während des Imports möglicherweise Konflikte beheben. Konflikte können aufgrund von E-Mail-aktivierten öffentlichen Ordner zugewiesenen, nicht-routingfähigen E-Mail-Adressen auftreten, oder es können sich Konflikte mit anderen Benutzern und Gruppen in Office 365 oder aufgrund von anderen Attributen ergeben.
- Um standortübergreifend auf Öffentliche Ordner zuzugreifen, müssen Benutzer ihre Outlook-Clients auf das Outlook-Update vom November 2012 oder höher aktualisieren.
  - Unter [Update für Microsoft Outlook 2010 \(KB2687623\) 32-Bit-Edition](#) können Sie das Outlook-

Update vom November 2012 für Outlook 2010 herunterladen.

- b. Unter [Update für Microsoft Office Outlook 2007 \(KB2687404\)](#) können Sie das Outlook-Update vom November 2012 für Outlook 2007 herunterladen.
5. Outlook 2011 für Mac und Outlook für Mac für Office 365 werden für standortübergreifende öffentliche Ordner nicht unterstützt. Benutzer müssen sich am selben Standort wie die öffentlichen Ordner befinden, damit sie mit Outlook 2011 für Mac oder Outlook für Mac für Office 365 auf diese Ordner zugreifen können. Darüber hinaus können Benutzer, deren Postfächer sich in Exchange Online befinden, nicht über Outlook Web App auf lokale öffentliche Ordner zugreifen.

#### NOTE

Outlook 2016 für Mac wird für standortübergreifende öffentliche Ordner unterstützt. Wenn Clients in Ihrer Organisation Outlook 2016 für Mac verwenden, müssen Sie sicherstellen, dass auf diesen Clients das Update vom April 2016 installiert ist. Andernfalls können die Benutzer dieser Clients nicht auf öffentliche Ordner in einer Hybridtopologie zugreifen. Weitere Informationen finden Sie unter [Zugreifen auf öffentliche Ordner mit Outlook 2016 für Mac](#).

## Schritt 1: Herunterladen der Skripts

1. Laden Sie unter [Mail-enabled Public Folders - directory sync script](#) die folgenden Dateien herunter:
  - `Sync-MailPublicFolders.ps1`
  - `SyncMailPublicFolders.strings.ps1`
2. Speichern Sie die Dateien auf dem lokalen Computer, auf dem Sie PowerShell ausführen. Verwenden Sie als Speicherort beispielsweise C:\PFScripts.

## Schritt 2: Konfigurieren der Verzeichnissynchronisierung

Der Verzeichnissynchronisierungsdienst synchronisiert nicht e-Mail-aktivierte Öffentliche Ordner. Das folgende Skript ausführen, werden die e-Mail-aktivierten Öffentlichen Ordner über lokale und Office 365 synchronisiert. Spezielle Berechtigungen für e-Mail-aktivierten Öffentlichen Ordner müssen in der Cloud wiederhergestellt werden, da Cross standortbasierte Berechtigung werden in Szenarien für die Hybridbereitstellung nicht unterstützt. Weitere Informationen finden Sie unter [Exchange Server-Hybridbereitstellung](#).

#### NOTE

Synchronisierte E-Mail-aktivierte öffentliche Ordner werden für Nachrichtenflusszwecke als E-Mail-Kontaktobjekte angezeigt und werden im Exchange-Verwaltungskonsole nicht angezeigt. Siehe „Get-MailPublicFolder“-Befehl. Verwenden Sie zum erneuten Erstellen der SendAs-Berechtigungen in der Cloud den „RecipientPermission“-Befehl.

1. Führen Sie auf Exchange-Server den folgenden Befehl zum Synchronisieren von e-Mail-aktivierter Öffentlicher Ordner aus der lokalen lokale Active Directory zu Office 365.

```
Sync-MailPublicFolders.ps1 -Credential (Get-Credential) -CsvSummaryFile:sync_summary.csv
```

Wobei `Credential` ist Office 365-Benutzernamen und Ihr Kennwort ein, und `CsvSummaryFile` ist der Pfad, in dem Sie Synchronisierungsvorgänge und Fehler, in der CSV-Format erfassen möchten.

#### **NOTE**

Vor dem Ausführen des Skripts, wird empfohlen, dass Sie zunächst die Aktionen, die das Skript ausführen würden in Ihrer Umgebung simulieren ausgeführt wird, wie oben beschrieben, mit der `-WhatIf` Parameter. > Es wird auch empfohlen, dass Sie dieses Skript täglich ausführen, um Ihre e-Mail-aktivierten Öffentlichen Ordner zu synchronisieren.

## Schritt 3: Konfigurieren von Exchange Online-Benutzern Zugriff auf Öffentliche Ordner von Exchange Server: lokal

Der letzte Schritt in diesem Verfahren wird zum Konfigurieren der Exchange online-Organisation und Gewährung des Zugriffs auf die öffentlichen Ordner von Exchange Server.

Ermöglichen Sie der Exchange Online-Organisation den Zugriff auf lokale Öffentliche Ordner. Sie zeigen auf alle lokalen Öffentliche Ordner-Postfächer.

```
Set-OrganizationConfig -PublicFoldersEnabled Remote -RemotePublicFolderMailboxes  
PFMailbox1,PFMailbox2,PFMailbox3
```

#### **NOTE**

Die Änderungen werden erst angezeigt, wenn die Active Directory-Synchronisierung abgeschlossen ist. Es kann bis zu 3 Stunden dauern, bis dieser Vorgang abgeschlossen ist. Wenn Sie nicht auf die sich wiederholenden Synchronisierungen warten möchten, die alle drei Stunden stattfinden, können Sie die Verzeichnissynchronisierung jederzeit erzwingen. Ausführliche Schritte für das Erzwingen der Verzeichnissynchronisierung finden Sie unter [Erzwingen der Verzeichnissynchronisierung](#).

## Woher weiß ich, dass der Vorgang erfolgreich war?

Melden Sie sich mit einem Benutzer bei Outlook an, der in Exchange Online gespeichert ist, und führen Sie die folgenden Tests für Öffentliche Ordner durch:

- Zeigen Sie die Hierarchie an.
- Prüfen Sie Berechtigungen.
- Erstellen und löschen Sie Öffentliche Ordner.
- Veröffentlichen Sie Inhalte in einem Öffentlichen Ordner, und löschen Sie diese.

# Konfigurieren öffentlicher Exchange Online-Ordner für eine Hybridbereitstellung

18.12.2018 • 9 minutes to read

**Zusammenfassung:** Anleitung zum Aktivieren von lokalen Exchange-Server-Benutzern Zugriff auf Öffentliche Ordner in Exchange Online.

In einer hybridbereitstellung können Ihre Benutzer in Exchange Online, lokalen oder beides, und Ihre öffentlichen Ordner sind entweder im Exchange Online oder lokalen. Manchmal müssen Ihre online-Benutzer Zugriff auf Öffentliche Ordner in Ihrer lokalen Exchange Server-Umgebung. In ähnlicher Weise müssen Exchange Server-Benutzer Zugriff auf Öffentliche Ordner in Office 365 oder Exchange Online.

In diesem Artikel wird beschrieben, wie zum Zugreifen auf Öffentliche Ordner von Exchange Online/Office 365-Benutzern in Ihrer lokalen Exchange Server-Umgebung ermöglichen. Damit Exchange Online/Office 365-Benutzer auf lokalen Exchange-Server Öffentliche Ordner zugreifen können, finden Sie unter [Konfigurieren der Exchange-Server Öffentliche Ordner für eine hybridbereitstellung](#).

## NOTE

Wenn Sie Öffentliche Ordner von Exchange 2010 haben, finden Sie unter [Configure legacy lokaler öffentlicher Ordner für eine hybridbereitstellung](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Bei diesen Anleitungen wird davon ausgegangen, dass Sie zur Konfiguration und Synchronisierung Ihrer lokalen und Exchange Online-Umgebungen den Assistanten für die Hybridkonfiguration verwendet haben, und dass die DNS-Einträge für die AutoErmittlung bei den meisten Benutzern auf einen lokalen Endpunkt verweisen. Weitere Informationen finden Sie unter [Hybrid Configuration Wizard](#).
- Bei diesen Anweisungen wird vorausgesetzt, dass Outlook Anywhere aktiviert und auf den lokalen Exchange-Servern funktionsbereit ist. Weitere Informationen über das Aktivieren von Outlook Anywhere finden Sie unter [Outlook Anywhere](#).
- Bei der Implementierung der Koexistenz öffentlicher Ordner für eine Hybridbereitstellung von Exchange mit Office 365 müssen Sie während des Imports möglicherweise Konflikte beheben. Konflikte können aufgrund von E-Mail-aktivierten öffentlichen Ordnern zugewiesenen, nicht-routingfähigen E-Mail-Adressen auftreten, oder es können sich Konflikte mit anderen Benutzern und Gruppen in Office 365 oder aufgrund von anderen Attributen ergeben.
- Um standortübergreifend auf Öffentliche Ordner zuzugreifen, müssen Benutzer ihre Outlook-Clients auf das Outlook-Update vom November 2012 oder höher aktualisieren.
  - Unter [Update für Microsoft Outlook 2010 \(KB2687623\) 32-Bit-Edition](#) können Sie das Outlook-Update vom November 2012 für Outlook 2010 herunterladen.
  - Unter [Update für Microsoft Office Outlook 2007 \(KB2687404\)](#) können Sie das Outlook-Update vom November 2012 für Outlook 2007 herunterladen.
- Outlook 2011 für Mac und Outlook für Mac für Office 365 werden für standortübergreifende öffentliche Ordner nicht unterstützt. Benutzer müssen sich am selben Standort wie die öffentlichen Ordner befinden, damit sie mit Outlook 2011 für Mac oder Outlook für Mac für Office 365 auf diese Ordner zugreifen

können. Darüber hinaus können Benutzer, deren Postfächer sich in Exchange Online befinden, nicht über Outlook Web App auf lokale öffentliche Ordner zugreifen.

#### NOTE

Outlook 2016 für Mac wird für standortübergreifende öffentliche Ordner unterstützt. Wenn Clients in Ihrer Organisation Outlook 2016 für Mac verwenden, müssen Sie sicherstellen, dass auf diesen Clients das Update vom April 2016 installiert ist. Andernfalls können die Benutzer dieser Clients nicht auf öffentliche Ordner in einer Koexistenz oder einer Hybrid-Topologie zugreifen. Weitere Informationen finden Sie unter [Zugreifen auf öffentliche Ordner mit Outlook 2016 für Mac](#).

## Schritt 1: Herunterladen der Skripts

1. Laden Sie die folgenden Dateien unter dem Link [Mail-enabled Public Folders - directory sync from EXO to On-prem script](#) herunter:

- Import-PublicFolderMailboxes.ps1
- ImportPublicFolderMailboxes.strings.psd1
- Sync-MailPublicFoldersCloudToOnprem.ps1
- Sync-MailPublicFoldersCloudToOnprem.strings.psd1

2. Speichern Sie die Dateien auf dem lokalen Computer, auf dem Sie PowerShell ausführen. Verwenden Sie als Speicherort beispielsweise C:\PFScripts.

## Schritt 2: Konfigurieren der Verzeichnissynchronisierung

Ausführen des Skripts `Sync-MailPublicFoldersCloudToOnprem.ps1` wird die e-Mail-aktivierten Öffentlichen Ordner zwischen Exchange Online und Ihrer lokalen Exchange Server-Umgebung zu synchronisieren. Spezielle Berechtigungen für e-Mail-aktivierte Öffentliche Ordner in der Cloud neu erstellt werden, da Cross standortbasierte Berechtigungen in Szenarien für die Hybridbereitstellung nicht unterstützt werden müssen. Weitere Informationen finden Sie unter [Exchange Server-Hybridbereitstellung](#).

#### NOTE

Synchronisierte E-Mail-aktivierte öffentliche Ordner werden für Nachrichtenflusszwecke als E-Mail-Kontaktobjekte angezeigt und werden im Exchange-Verwaltungskonsole nicht angezeigt. Siehe „Get-MailPublicFolder“-Befehl. Verwenden Sie zum erneuten Erstellen der SendAs-Berechtigungen in der Cloud den „RecipientPermission“-Befehl.

Führen Sie auf Exchange-Server den folgenden Befehl zum e-Mail-aktivierten Öffentlichen Ordner von Exchange Online/Office 365 in Ihrer lokalen lokale Active Directory zu synchronisieren.

```
...
Sync-MailPublicFoldersCloudToOnprem.ps1 -Credential (Get-Credential)
...
```

Wobei `Credential` ist Office 365-Benutzernamen und Ihr Kennwort ein.

#### NOTE

Wir empfehlen Ihnen, dieses Skript täglich auszuführen, um Ihre E-Mail-aktivierten öffentlichen Ordner zu synchronisieren.

## Schritt 3: Konfigurieren des Zugriffs auf öffentliche Exchange Online-Ordner für lokale Benutzer

Der letzte Schritt in diesem Verfahren wird so konfigurieren Sie die Exchange-Server der lokalen Organisation, um Zugriff auf Exchange Online Öffentliche Ordner ermöglichen.

Ausführen des Skripts `Import-PublicFolderMailboxes.ps1` importiert Öffentliche Ordner-Postfach-Objekte aus der Cloud als e-Mail-aktivierte Benutzer für Ihre lokale Umgebung. Das Skript wird auch die importierten Objekte als remote Öffentliche Ordner-Postfächer konfigurieren.

1. Führen Sie auf Exchange-Server den folgenden Befehl auf Öffentliche Ordner-Postfach-Objekte aus der Cloud in Ihre lokale Active Directory zu importieren.

```
Import-PublicFolderMailboxes.ps1 -Credential (Get-Credential)
```

Wobei `Credential` ist Office 365-Benutzernamen und Ihr Kennwort ein.

### NOTE

Wir empfehlen, dieses Skript täglich auszuführen, um Ihre Postfachobjekte des Typs „Öffentlicher Ordner“ zu importieren. Der Grund: Wann immer Postfächer des Typs „Öffentlicher Ordner“ ihren Kapazitätsschwellenwert erreichen, werden sie automatisch in mehrere neue Postfächer aufgeteilt. Daher sollten Sie immer sicherstellen, dass Sie die neuesten Postfächer des Typs „Öffentlicher Ordner“ aus der Cloud importiert haben.

2. Aktivieren Sie für die lokale Exchange 2013-Organisation den Zugriff auf die öffentlichen Ordner in Exchange Online.

```
Set-OrganizationConfig -PublicFoldersEnabled Remote
```

### NOTE

Die Änderungen werden erst angezeigt, wenn die Active Directory-Synchronisierung abgeschlossen ist. Es kann bis zu 3 Stunden dauern, bis dieser Vorgang abgeschlossen ist. Wenn Sie nicht auf die sich wiederholenden Synchronisierungen warten möchten, die alle drei Stunden stattfinden, können Sie die Verzeichnissynchronisierung jederzeit erzwingen. Ausführliche Schritte für das Erzwingen der Verzeichnissynchronisierung finden Sie unter [Erzwingen der Verzeichnissynchronisierung](#).

## Woher weiß ich, dass der Vorgang erfolgreich war?

Melden Sie sich mit einem Benutzer bei Outlook an, der in Exchange Online gespeichert ist, und führen Sie die folgenden Tests für Öffentliche Ordner durch:

- Zeigen Sie die Hierarchie an.
- Prüfen Sie Berechtigungen.
- Erstellen und löschen Sie Öffentliche Ordner.
- Veröffentlichen Sie Inhalte in einem Öffentlichen Ordner, und löschen Sie diese.

# Einrichten öffentlicher Ordner in einer neuen Organisation

18.12.2018 • 6 minutes to read

**Zusammenfassung:** Informationen zum Einrichten öffentlicher Ordner, einschließlich Zuweisen von Berechtigungen für diese im Exchange Admin Center.

In diesem Thema wird erklärt, wie öffentliche Ordner in einer neuen Organisation oder einer Organisation ohne vorherige öffentliche Ordner konfiguriert und in Betrieb genommen werden.

## NOTE

Weitere Informationen zu den Speichercontingenten und Grenzwerte für Öffentliche Ordner finden Sie unter den folgenden Themen: > Öffentliche Ordner in Office 365, finden Sie unter [Exchange Online-Begrenzungen](#). > Öffentliche Ordner in der lokalen Exchange-Server finden Sie unter [Grenzwerte für Öffentliche Ordner](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen dieser Aufgabe: 30 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Öffentliche Ordner" im Thema [Freigabe- und Zusammenarbeitsberechtigungen](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Bitten Sie in den Exchange-Foren um Hilfe. Besuchen Sie die Foren unter [Exchange Server](#), [Exchange Online](#) oder [Exchange Online Protection](#).

## Wie gehen Sie dazu vor?

### Schritt 1: Erstellen des primären Postfachs für öffentliche Ordner

Das primäre Postfach für öffentliche Ordner enthält eine beschreibbare Kopie der Hierarchie öffentlicher Ordner samt Inhalt und ist das erste Postfach für öffentliche Ordner, das Sie für Ihre Organisation anlegen. Alle weiteren Postfächer für öffentliche Ordner werden sekundäre Postfächer für öffentliche Ordner, die eine schreibgeschützte Kopie der Hierarchie samt Inhalt enthalten.

Ausführliche Anleitungen finden Sie unter [Erstellen eines Postfachs für öffentliche Ordner](#).

### Schritt 2: Erstellen des ersten öffentlichen Ordners

Ausführliche Schritte finden Sie unter [Erstellen eines öffentlichen Ordners](#).

### Schritt 3: Zuweisen von Berechtigungen zum öffentlichen Ordner

Nach dem Erstellen des öffentlichen Ordners müssen Sie die Berechtigungsstufe **Besitzer** festlegen, sodass mindestens ein Benutzer auf dem Client auf den öffentlichen Ordner zugreifen und Unterordner erstellen kann. Alle nachfolgend erstellten öffentlichen Ordner erben die Berechtigungen des übergeordneten öffentlichen

Ordners.

1. Wechseln Sie in der Exchange-Verwaltungskonsole (EAC) zu **Öffentliche Ordner** > **Öffentliche Ordner**.
2. Wählen Sie in der Listenansicht den öffentlichen Ordner aus.
3. Klicken Sie im Detailbereich unter **Ordnerberechtigungen** auf **Verwalten**.
4. Klicken Sie in **Berechtigungen für öffentliche Ordner** auf **Hinzufügen**
5. Klicken Sie auf **Durchsuchen**, um einen Benutzer auszuwählen.
6. Wählen Sie in der Liste **Berechtigungsstufe** eine Stufe aus. Mindestens ein Benutzer sollte die Stufe **Besitzer** innehaben.
7. Klicken Sie auf **Speichern**.
8. Sie können mehrere Benutzer hinzufügen, indem Sie auf **Hinzufügen**  klicken und die oben genannten Schritte ausführen, um die geeigneten Berechtigungen zuzuweisen. Sie können die Berechtigungsstufe auch anpassen, indem Sie die entsprechenden Kontrollkästchen aktivieren oder deaktivieren. Wenn Sie eine vordefinierte Berechtigungsstufe wie z. B. **Besitzer** bearbeiten, ändert sich die Berechtigungsstufe zu **Benutzerdefiniert**.

Weitere Informationen zum Verwenden der Shell für das Zuweisen von Berechtigungen zu einem öffentlichen Ordner finden Sie unter [Add-PublicFolderClientPermission](#).

#### **Schritt 4 (optional): Aktivieren des öffentlichen Ordners für E-Mail**

Wenn Sie möchten, dass Benutzer E-Mails an den öffentlichen Ordner senden können, müssen Sie den Ordner für E-Mail aktivieren. Dieser Schritt ist optional. Wenn Sie den öffentlichen Ordner nicht für E-Mail aktivieren, können Benutzer Nachrichten in diesem Ordner bereitstellen, indem sie Elemente aus Outlook in den Ordner ziehen.

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Öffentliche Ordner** > **Öffentliche Ordner**.
2. Wählen Sie in der Listenansicht den öffentlichen Ordner aus, den Sie für E-Mail aktivieren möchten.
3. Klicken Sie im Detailbereich unter **E-Mail-Einstellungen - Deaktiviert** auf **Aktivieren**.

Sie werden in einer Warnmeldung gefragt, ob Sie den öffentlichen Ordner tatsächlich für E-Mail aktivieren möchten. Klicken Sie auf **Ja**.

Der öffentliche Ordner ist nun für E-Mail aktiviert, und der Name des öffentlichen Ordners ist der Alias des öffentlichen Ordners. Wenn mehrere Empfänger den gleichen Namen aufweisen, wird eine Zahl an den Alias des öffentlichen Ordners angehängt. Wenn Sie beispielsweise über eine Verteilergruppe "Vertriebsteam" verfügen, einen öffentlichen Ordner namens "Vertriebsteam" erstellen und diesen für E-Mail aktivieren, erhält der öffentliche Ordner den Alias "Vertriebsteam1".

Weitere Informationen zum Verwenden der Shell für das Aktivieren eines öffentlichen Ordners für E-Mail finden Sie unter [Enable-MailPublicFolder](#).

# Zugreifen auf öffentliche Ordner mit Outlook 2016 für Mac

18.12.2018 • 3 minutes to read

**Zusammenfassung:** Dieser Artikel führt die neuesten unterstützten Exchange-Topologien auf, in denen Benutzer mit Outlook 2016 für Mac auf öffentliche Ordner zugreifen können.

Benutzer von Outlook 2016 für Mac können jetzt Öffentliche Ordner in Exchange Online in einer Reihe von unterschiedlichen Topologien zugreifen.

## Einschränkungen bei Outlook für Mac

Alle Versionen von Outlook für Mac öffentliche Exchange-Ordner zugreifen können, jedoch erst kürzlich diese Clients konnte nicht zugegriffen werden Öffentliche Ordner in der folgenden Bereitstellungsszenario:

- **Hybridtopologien:** lokale Benutzer mit einem Postfach in Exchange Online basierend konnte nicht Outlook für Mac verwenden, um lokale modernen Öffentliche Ordner zugreifen. Benutzer mit einem Exchange 2013 oder Exchange 2016 Postfach lokale ebenso konnte Outlook nicht verwenden, für Mac zum Zugreifen auf Öffentliche Ordner in Exchange Online bereitgestellt.

## Outlook 2016 für Mac

Mit dem Update von April 2016 für Outlook 2016 für Mac als auch CU14 für Exchange 2013 und CU2 für Exchange 2016 wird das oben beschriebenen Szenario jetzt für 2016 Outlook für Mac-Clients verwendet werden.

In der folgenden Tabelle sind die unterstützten Topologien für Benutzer mit 2016 Outlook für Mac-Clients, die sich auf Öffentliche Ordner in Exchange Online zusammengefasst.

### NOTE

Für die in der nachfolgenden Tabelle dargestellten Szenarien setzen wir voraus, dass das Update vom April 2016 für Outlook 2016 für Mac auf allen Clients installiert wurde.

ÖFFENTLICHE ORDNER BEREITGESTELLT IN:	BENUTZERPOSTFACH IN EXCHANGE 2010 SP3 ODER HÖHER	BENUTZERPOSTFACH IN EXCHANGE 2013 CU13 ODER HÖHER	BENUTZERPOSTFACH IN EXCHANGE 2016 CU2 ODER HÖHER	BENUTZERPOSTFACH IN OFFICE 365/EXCHANGE ONLINE
Exchange Server 2010 SP3 oder höher	Unterstützt	Unterstützt	Unterstützt	Nicht unterstützt
Exchange Server 2013 CU13 oder höher	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
Exchange Server 2016 CU2 oder höher	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
Office 365/Exchange Online	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt

In den folgenden Artikeln wird beschrieben, wie Sie in Ihrer Exchange-Organisation öffentliche Ordner in einer Koexistenztopologie oder einer Hybridtopologie bereitstellen können. Sofern auf Ihren Outlook 2016 für Mac-Clients das Update vom April 2016 installiert ist, können die Clients auf öffentliche Ordner in den in diesen Artikeln beschriebenen Konfigurationen zugreifen:

- [Konfigurieren älterer öffentlicher Ordner, wenn sich die Postfächer der Benutzer auf Exchange 2013-Servern befinden](#)
- [Konfigurieren öffentlicher Exchange 2013-Ordner für eine Hybridbereitstellung](#)
- [Konfigurieren öffentlicher Exchange Online-Ordner für eine Hybridbereitstellung](#)

# Erstellen eines Postfachs für öffentliche Ordner

18.12.2018 • 5 minutes to read

Bevor Sie einen öffentlichen Ordner erstellen können, müssen Sie zunächst ein Postfach für öffentliche Ordner erstellen. Postfächer für öffentliche Ordner enthalten die Hierarchieinformationen sowie den Inhalt öffentlicher Ordner. Das erste Postfach für öffentliche Ordner, das Sie erstellen, wird zum primären Hierarchiepostfach, das die einzige beschreibbare Kopie der Hierarchie enthält. Alle weiteren Postfächer für öffentliche Ordner, die Sie erstellen, werden sekundäre Postfächer, die eine schreibgeschützte Kopie der Hierarchie enthalten.

## NOTE

Weitere Informationen zu den Speicherkontingenzen und -grenzwerten bei öffentlichen Ordnern finden Sie unter den folgenden Themen:

- Öffentliche Ordner in Office 365 finden Sie unter [Exchange Online-Begrenzungen](#).
- Öffentliche Ordner in der lokalen Exchange-Server finden Sie unter [Grenzwerte für Öffentliche Ordner](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Öffentliche Ordner in Exchange Server, finden Sie unter [Public Folder Procedures](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Öffentliche Ordner in Exchange Online, finden Sie unter [Public Folder Procedures in Office 365](#) und [Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 5 Minuten.
- Öffentliche Exchange-Ordner und Öffentliche Ordner auf Exchange-Legacyservern können nicht in derselben Organisation vorhanden sein. Wenn Sie versuchen, ein Postfach für Öffentliche Ordner zu erstellen, wenn Sie weiterhin ältere öffentliche Ordner vorhanden sind, erhalten Sie den Fehler **einen vorhandenen öffentlichen Ordner, für die Bereitstellung erkannt wurde. Erstellen Sie zum Migrieren von vorhandener öffentlichen Ordner Daten neues Postfach für Öffentliche Ordner mithilfe der Switch - HoldForMigration.**

Vor der Erstellung von öffentlichen Ordnern in Exchange Server müssen Sie Ihre ältere öffentliche Ordner auf Exchange-Server zu migrieren. Zu diesem Zweck führen Sie die Schritte unter [Migrate Public Folders to Exchange 2013 From Previous Versions](#). Diese Schritte werden gezeigt, wie ein Postfach für Öffentliche Ordner zu erstellen, die zum Speichern von migrierten öffentlichen Ordner verwendet werden können.

- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Öffentliche Ordner" im Thema [Freigabe- und Zusammenarbeitsberechtigungen](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## Erstellen eines Postfachs für öffentliche Ordner mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie zu **Öffentliche Ordner > Postfächer für Öffentliche Ordner**, und klicken Sie dann auf

New

2. Geben Sie in **Postfach für öffentliche Ordner** einen Namen für das Postfach für den öffentlichen Ordner an.
3. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell zum Erstellen eines Postfachs für Öffentliche Ordner

In diesem Beispiel wird das primäre Postfach für öffentliche Ordner erstellt.

```
New-Mailbox -PublicFolder -Name MasterHierarchy
```

In diesem Beispiel wird ein sekundäres Postfach für öffentliche Ordner erstellt. Der einzige Unterschied zwischen der Erstellung des primären Hierarchiepostfachs und einem sekundären Hierarchiepostfach besteht darin, dass das primäre Postfach das erste Postfach ist, das in der Organisation erstellt wurde. Sie können zusätzliche Postfächer für öffentliche Ordner zum Zweck des Lastenausgleichs erstellen.

```
New-Mailbox -PublicFolder -Name Istanbul
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [new-Mailbox](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie das Postfach des primären Öffentliche Ordner erfolgreich erstellt haben, führen Sie den folgenden Befehl in Exchange Online PowerShell:

```
Get-OrganizationConfig | Format-List RootPublicFolderMailbox
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [get-OrganizationConfig](#).

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Erstellen eines öffentlichen Ordners

18.12.2018 • 4 minutes to read

Öffentliche Ordner ermöglichen den gemeinsamen Zugriff und stellen ein einfaches und effektives Mittel zum Erfassen, Organisieren und Freigeben von Informationen für andere Personen in der Arbeitsgruppe oder Organisation dar.

Ein öffentlicher Ordner erbt standardmäßig die Einstellungen seines übergeordneten Ordners, einschließlich der Einstellungen für Berechtigungen.

## NOTE

Weitere Informationen zu den Speichercontingenten und -grenzwerten bei öffentlichen Ordnern finden Sie unter den folgenden Themen:

- Öffentliche Ordner in Office 365 finden Sie unter [Exchange Online-Begrenzungen](#).
- Öffentliche Ordner in der lokalen Exchange-Server finden Sie unter [Grenzwerte für Öffentliche Ordner](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Öffentliche Ordner" im Thema [Freigabe- und Zusammenarbeitsberechtigungen](#).
- Sie können erst dann einen öffentlichen Ordner erstellen, nachdem Sie ein Postfach für öffentliche Ordner erstellt haben. Weitere Informationen zum Erstellen eines Postfachs für öffentliche Ordner finden Sie unter [Erstellen eines Postfachs für öffentliche Ordner](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## Erstellen eines öffentlichen Ordners mithilfe der Exchange-Verwaltungskonsole

Wenn Sie einen öffentlichen Ordner mithilfe der Exchange-Verwaltungskonsole erstellen, können Sie nur den Namen und den Pfad für den Ordner festlegen. Nachdem der öffentliche Ordner erstellt wurde, müssen Sie ihn bearbeiten, um weitere Einstellungen zu konfigurieren.

1. Navigieren Sie zu **Öffentliche Ordner > Öffentliche Ordner**.
2. Wenn Sie diesen öffentlichen Ordner als untergeordneten Ordner eines vorhandenen öffentlichen Ordners erstellen möchten, klicken Sie in der Listenansicht auf den gewünschten öffentlichen Ordner. Wenn Sie einen öffentlichen Ordner der obersten Ebene erstellen möchten, überspringen Sie diesen Schritt.
3. Klicken Sie auf **neue**
4. Geben Sie im Feld **Öffentlicher Ordner** den Namen des öffentlichen Ordners ein.

**IMPORTANT**

Verwenden Sie keinen umgekehrten Schrägstrich (\) in den Namen, die beim Erstellen eines öffentlichen Ordners.

5. Überprüfen Sie im Feld **Pfad** den Pfad zum öffentlichen Ordner. Wenn dies nicht der gewünschte Pfad ist, klicken Sie auf **Abbrechen**, und führen Sie Schritt 2 dieses Verfahrens durch.
6. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell, Erstellen eines öffentlichen Ordners

In diesem Beispiel wird ein öffentlicher Ordner "Reports" im Pfad "Marketing\2013" erstellt.

```
New-PublicFolder -Name Reports -Path \Marketing\2013
```

**IMPORTANT**

Verwenden Sie keinen umgekehrten Schrägstrich (\) in den Namen, die beim Erstellen eines öffentlichen Ordners.

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-PublicFolder](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Gehen Sie folgendermaßen vor, um zu überprüfen, ob der öffentliche Ordner erfolgreich erstellt wurde:

- Klicken Sie in der Exchange-Verwaltungskonsole auf **Aktualisieren**, um die Liste der öffentlichen Ordner zu aktualisieren. Ihr neuer öffentlicher Ordner sollte in der Liste angezeigt werden.
- Führen Sie in Exchange Online PowerShell einen der folgenden Befehle aus:

```
Get-PublicFolder -Identity \Marketing\2013\Reports | Format-List
```

```
Get-PublicFolder -Identity \Marketing\2013 -GetChildren
```

```
Get-PublicFolder -Recurse
```

**TIP**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Wiederherstellen eines gelöschten Postfachs für öffentliche Ordner

18.12.2018 • 5 minutes to read

**Zusammenfassung:** In diesem Artikel erfahren Sie, wie Sie in Office 365 ein Postfach für öffentliche Ordner wiederherstellen können, das zuvor vorläufig gelöscht wurde. Vorläufig gelöscht bedeutet, dass der Aufbewahrungszeitraum des Postfachs noch nicht abgelaufen ist und der Papierkorb noch nicht endgültig gelöscht wurde.

Sie können die Postfächer für Öffentliche Ordner in der Exchange-Verwaltungskonsole oder über Löschen der `Remove-Mailbox -PublicFolder` Cmdlet. Zum Löschen eines primären Postfachs müssen alle Postfächer anderer zuerst gelöscht werden. Nachdem ein Postfach gelöscht wird werden nicht mehr in der Exchange-Verwaltungskonsole angezeigt.

Gelöschte Postfächer für öffentliche Ordner können über einen Zeitraum von bis zu 90 Tagen wiederhergestellt werden.

## Was sollten Sie wissen, bevor Sie beginnen?

- Zeitaufwand für den Vorgang: 5 bis 10 Minuten
- Ein Postfach für Öffentliche Ordner kann nur gelöscht werden, nachdem alle Ordner in dem Postfach gelöscht wurden. Sie können jedoch diese Einschränkung umgehen, indem die `-Force` wechseln, wie in `Remove-Mailbox -PublicFolder -Force`.
- Gelöschte Postfächer für öffentliche Ordner können nur über einen Zeitraum von 90 Tagen wiederhergestellt werden, nachdem das Postfach vorläufig gelöscht wurde. Die Aufbewahrungsdauer für ein vorläufig gelöschtes Postfach beträgt 90 Tage; danach wird das Postfach dauerhaft gelöscht, und Sie können es nicht wiederherstellen.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Öffentliche Ordner" im Thema [Freigabe- und Zusammenarbeitsberechtigungen](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### NOTE

Wenn Sie ein gelöschtes Postfach für öffentliche Ordner mithilfe einer der folgenden Anleitungen wiederherstellen und das Postfach Ordner enthält, werden diese Ordner automatisch zusammen mit dem Postfach wiederhergestellt.

## Wiederherstellen eines primären Postfachs

Gehen Sie wie folgt vor, um ein primäres Postfach für öffentliche Ordner wiederherzustellen:

1. Geben Sie den folgenden Befehl ein, um das vorläufig gelöschte Postfach zu finden:

```
Get-Mailbox -PublicFolder -SoftDeletedMailbox
```

2. Geben Sie den folgenden Befehl ein, um das gewünschte Postfach wiederherzustellen:

```
Undo-SoftDeletedMailbox -PublicFolder
```

## Wiederherstellen eines primären Postfachs sowie sekundärer Postfächer

Die **Art**, die Informationen, die Teil der `Get-Mailbox` -Cmdlet Postfächer für Öffentliche Ordner als **primären** oder **sekundären** identifiziert. Primäre Öffentliche Ordner-Postfächer müssen zuerst wiederhergestellt werden.

Gehen Sie wie folgt vor, um ein primäres Postfach für öffentliche Ordner sowie alle relevanten sekundären Postfächer wiederherzustellen:

1. Geben Sie den folgenden Befehl ein, um die vorläufig gelöschten Postfächer zu finden:

```
Get-Mailbox -PublicFolder -SoftDeletedMailbox
```

2. Geben Sie den folgenden Befehl ein, um das primäre Postfach wiederherzustellen:

```
Undo-SoftDeletedMailbox -PublicFolder
```

3. Geben Sie den folgenden Befehl für jedes sekundäre Postfach für öffentliche Ordner ein, das Sie wiederherstellen möchten (einmal pro Postfach):

```
Undo-SoftDeletedMailbox -PublicFolder
```

## Wiederherstellen von sekundären Postfächern

Gehen Sie wie folgt vor, wenn Sie ein oder mehrere vorläufig gelöschte sekundäre Postfächer für öffentliche Ordner wiederherstellen möchten und das primäre Postfach noch in Ihrer Organisation existiert:

1. Geben Sie den folgenden Befehl ein, um die vorläufig gelöschten Postfächer zu finden:

```
Get-Mailbox -PublicFolder -SoftDeletedMailbox
```

Sie können anhand der Informationen im Feld **Type** zwischen primären und sekundären Postfächern für öffentliche Ordner unterscheiden.

2. Geben Sie den folgenden Befehl für jedes sekundäre Postfach für öffentliche Ordner ein, das Sie wiederherstellen möchten (einmal pro Postfach):

```
Undo-SoftDeletedMailbox -PublicFolder
```

### NOTE

Wurde ein primärer öffentlicher Ordner aus einer Organisation gelöscht, können ihm zugeordnete sekundäre Postfächer nicht wiederhergestellt werden.

# Verwenden bevorzugter öffentlicher Ordner in Outlook im Web

18.12.2018 • 3 minutes to read

Im Outlook-Client können Benutzer in Ihrer Organisation Ihren **Favoriten**-Ordnern öffentliche Ordner hinzufügen. Danach können sie je nach den Richtlinien Ihrer Organisation Outlook im Web verwenden, um diese öffentlichen Ordner zu ihren Favoriten hinzuzufügen und bestimmte Funktionen in Outlook im Web auszuführen, die sie im Outlook-Client verwenden.

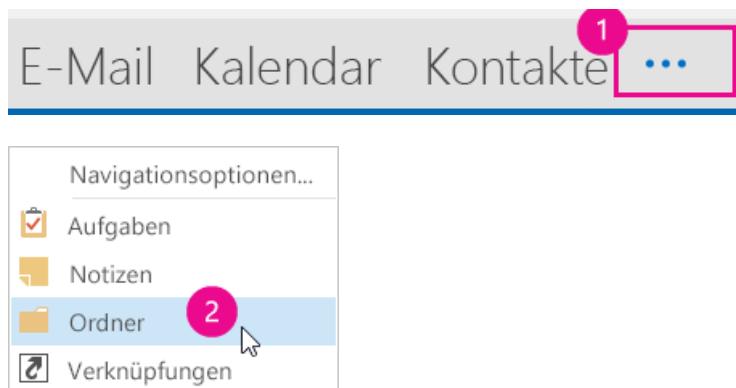
## Hinzufügen von öffentlichen Ordnern zu Favoriten in Outlook

Damit Benutzer bestimmte Aufgaben in öffentlichen Ordnern in ihren **Favoriten**-Ordnern vornehmen können, müssen sie zunächst den Outlook-Client verwenden, um dem Ordner **Favoriten** öffentliche Ordner hinzuzufügen.

### NOTE

Weitere Informationen zum Erstellen und Konfigurieren öffentlicher Ordner und Benutzer in Ihrer Organisation finden Sie unter [Erstellen eines öffentlichen Ordners in Outlook](#).

1. Wechseln Sie in Outlook zur Ansicht **Ordner**. Klicken Sie auf der Navigationsleiste auf die drei Punkte, und klicken Sie dann auf **Ordner**.



Benutzer, die über Outlook 2010-Clients verfügen, können unten im Navigationsbereich auf **Ordner** klicken.

2. Scrollen Sie ggf. zum Knoten **Öffentliche Ordner** im Navigationsbereich. Klicken Sie, um den Ordner **Alle Öffentlichen Ordner** zu erweitern.
3. Klicken Sie mit der rechten Maustaste auf den öffentlichen Ordner, den Sie zu **Favoriten** hinzufügen möchten. Wählen Sie dann **Zu Favoriten hinzufügen** aus.

### NOTE

Standardmäßig befindet sich der Ordner **Favoriten** direkt unter dem Ordner **Alle Öffentlichen Ordner** auf der Navigationsleiste.

4. Im Dialogfeld **Zu Favoriten hinzufügen** haben Sie die Möglichkeit, den Ordner nur für Ihre **Favoriten** umzubenennen. Klicken Sie auf **Hinzufügen**, um den Ordner zu **Favoriten** hinzuzufügen.

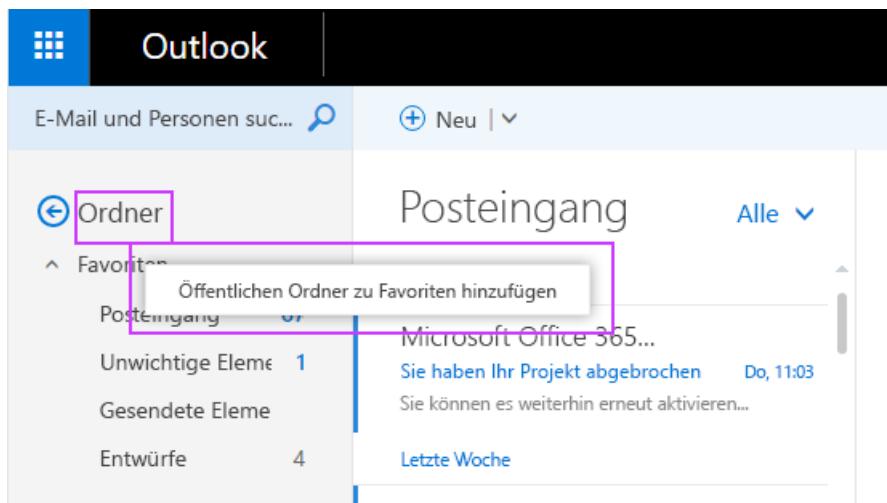
## IMPORTANT

Es gibt verschiedene Typen öffentlicher Ordner. Damit Benutzer einen bevorzugten öffentlichen Ordner in Outlook im Web verwenden können, muss der Ordner vom Typ „E-Mail- oder Bereitstellungselemente“, „Kalenderelemente“ oder „Kontaktelemente“ sein.

## Hinzufügen von öffentlichen Favoritenordnern in Outlook im Web

Damit Benutzer auf ihre öffentlichen Outlook-Favoritenordner zugreifen können, müssen sie diese auf zu ihren Favoriten in Outlook im Web hinzufügen. Der Outlook-Client synchronisiert öffentliche Ordner mit Outlook im Web nicht automatisch.

- Zum Hinzufügen eines öffentlichen Ordners in Outlook im Web klicken Sie mit der rechten Maustaste auf **Ordner**, und wählen Sie dann **Öffentlichen Ordner zu Favoriten hinzufügen** aus. Suchen Sie den Ordner, und klicken Sie auf **Hinzufügen**.



Die Benutzer können jetzt Outlook im Web für die folgenden Aufgaben in ihren bevorzugten öffentlichen Ordner für Kalender, Kontakt, E-Mail oder Beiträge ausführen:

- Erstellen von Elementen in den öffentlichen Ordnern
- Abrufen von Elementen
- Aktualisieren von Elementen
- Löschen von Elementen

## See also

[Erstellen eines öffentlichen Ordners in Outlook](#)

# E-Mail-Aktivierung oder E-Mail-Deaktivierung von öffentlichen Ordner

18.12.2018 • 6 minutes to read

Öffentliche Ordner für gemeinsamen Zugriff vorgesehen sind, und geben Sie ein einfaches und effektives Mittel zum Sammeln, organisieren und Freigeben von Informationen für andere Personen in Ihrer Arbeitsgruppe oder Organisation. E-Mail-Aktivieren eines öffentlichen Ordners ermöglicht Benutzern den öffentlichen Ordner für die Bereitstellung durch Senden einer e-Mail-Nachricht hinzu. Wenn ein öffentlicher Ordner ist verfügbar, e-Mail-aktivierte zusätzliche Einstellungen für den öffentlichen Ordner in der Exchange-Verwaltungskonsole (EAC), wie e-Mail-Adressen und Mail Kontingente. In der Exchange Online PowerShell vor ein öffentlicher Ordner e-Mail-aktiviert ist, verwenden Sie das Cmdlet **Set-PublicFolder** alle betreffenden Einstellungen verwalten. Nach dem e-Mail-aktivierte Öffentliche Ordner ist, verwenden Sie das **Set-PublicFolder** und **Set-MailPublicFolder** - Cmdlets zum Verwalten der Einstellungen.

Wenn Sie möchten, dass die Benutzer im Internet E-Mails an einen E-Mail-aktivierten öffentlichen Ordner senden, müssen Sie zusätzliche Berechtigungen mit dem Cmdlet **Add-PublicFolderClientPermission** festlegen.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit öffentlichen Ordner finden Sie unter [Public Folder Procedures](#).

Weiteren Verwaltungsaufgaben in Bezug auf Öffentliche Ordner finden Sie unter [Verfahren der Öffentliche Ordner in Office 365 und Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten
- Um sicherzustellen, dass Benutzer im Internet E-Mail-Nachrichten an E-Mail-aktivierte öffentliche Ordner senden können, muss dem anonymen Konto im öffentlichen Ordner mindestens das Zugriffsrecht *CreateItems* erteilt werden. Wenn Sie wissen möchten, wie das geht, gehen Sie zu [Allow anonymous users to send email to a mail-enabled public folder](#).
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Öffentliche Ordner" im Thema [Freigabe- und Zusammenarbeitsberechtigungen](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Was möchten Sie machen?

### E-Mail-Aktivierung oder -Deaktivierung eines öffentlichen Ordners mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie zu **Öffentliche Ordner > Öffentliche Ordner**.
2. Wählen Sie in der Listenansicht den öffentlichen Ordner aus, den Sie für E-Mails aktivieren oder

deaktivieren möchten.

3. Klicken Sie im Detailbereich unter **E-Mail-Einstellungen** auf **Aktivieren** oder **Deaktivieren**.
4. Sie werden in einem Warnungsfeld gefragt, ob Sie wirklich E-Mails für den öffentlichen Ordner aktivieren oder deaktivieren möchten. Klicken Sie auf **Ja**, um den Vorgang fortzusetzen.

Wenn Sie möchten, dass externe Benutzer E-Mails an diesen öffentlichen Ordner senden, führen Sie die Schritte unter [Zulassen, dass anonyme Benutzer E-Mails an einen E-Mail-aktivierten öffentlichen Ordner senden](#) aus.

### **Verwenden Sie Exchange Online PowerShell, um e-Mail-Aktivieren eines öffentlichen Ordners**

In diesem Beispiel wird der öffentliche Ordner "Help Desk" für E-Mails aktiviert.

```
Enable-MailPublicFolder -Identity "\Help Desk"
```

In diesem Beispiel wird der öffentliche Ordner "Reports" unterhalb des öffentlichen Ordners "Marketing" zwar E-Mail-aktiviert, in den Adresslisten jedoch ausgeblendet.

```
Enable-MailPublicFolder -Identity "\Marketing\Reports" -HiddenFromAddressListsEnabled $True
```

Wenn Sie möchten, dass externe Benutzer E-Mails an diesen öffentlichen Ordner senden, führen Sie die Schritte unter [Zulassen, dass anonyme Benutzer E-Mails an einen E-Mail-aktivierten öffentlichen Ordner senden](#) aus.

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Enable-MailPublicFolder](#).

### **Verwenden Sie Exchange Online PowerShell, um e-Mail-eines öffentlichen Ordners deaktivieren**

In diesem Beispiel wird der öffentliche Ordner "Marketing\Reports" für E-Mails deaktiviert.

```
Disable-MailPublicFolder -Identity "\Marketing\Reports"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Disable-MailPublicFolder](#).

### **Zulassen, dass anonyme Benutzer E-Mails an einen E-Mail-aktivierten öffentlichen Ordner senden**

Sie können Outlook oder Exchange Online PowerShell Festlegen von Berechtigungen für einen öffentlichen Ordner anonymes Konto verwenden. Sie können nicht der Exchange-Verwaltungskonsole zum Festlegen von Berechtigungen für das anonyme Konto verwenden.

### **Verwenden von Outlook für das Festlegen von Berechtigungen für das anonyme Konto**

1. Öffnen Sie Outlook, indem Sie ein Konto verwenden, das über Besitzerrechte für den E-Mail-aktivierten öffentlichen Ordner verfügt, der E-Mails von anonymen Benutzern akzeptieren soll.
2. Navigieren Sie zu **Öffentliche Ordner - <Benutzername>**.
3. Navigieren Sie zu dem öffentlichen Ordner, den Sie ändern möchten.
4. Klicken Sie mit der rechten Maustaste auf den öffentlichen Ordner, dann auf **Eigenschaften**, und wählen Sie die Registerkarte **Berechtigungen** aus.
5. Wählen Sie das Konto **Anonym** und dann **Elemente erstellen** unter **Schreiben**, und klicken Sie dann auf **OK**.

### **Verwenden von Exchange Online PowerShell zum Festlegen von Berechtigungen für das anonyme Konto**

In diesem Beispiel wird die `CreateItems` Berechtigung für das anonyme Konto für den "Customer Feedback" e-

Mail-aktivierten Öffentlichen Ordner.

```
Add-PublicFolderClientPermission "\Customer Feedback" -AccessRights CreateItems -User Anonymous
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Add-PublicFolderClientPermission](#).

# Aktualisieren der Öffentliche Ordner-Hierarchie

18.12.2018 • 2 minutes to read

Sie müssen die Hierarchie öffentlicher Ordner nur aktualisieren, wenn Sie die Hierarchiesynchronisierung und den Postfach-Assistenten manuell aufrufen möchten. Beide werden für jedes Postfach für öffentliche Ordner in der Organisation mindestens alle 24 Stunden aufgerufen. Die Hierarchiesynchronisierung wird alle 15 Minuten aufgerufen, wenn Benutzer über Microsoft Outlook oder einen Microsoft Exchange-Webdienstclient an einem sekundären Postfach angemeldet sind.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Öffentliche Ordner" im Thema [Freigabe- und Zusammenarbeitsberechtigungen](#).
- Sie können nicht in der Exchange-Verwaltungskonsole dieses Verfahren ausführen. Sie müssen Exchange Online PowerShell verwenden.
- Es wird empfohlen, dass beim Ausführen dieses Befehls mit dem Parameter *InvokeSynchronizer* den *SuppressStatus*-Parameter verwenden. Wenn dieser Parameter nicht in den Befehl verwendet wird, wird die Ausgabe Statusnachrichten alle 3 Sekunden bis zu einer Minute angezeigt. Bis die Minute übergibt, können Sie diese Instanz von Exchange Online PowerShell verwenden.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktualisieren der Öffentliche Ordner-Hierarchie

In diesem Beispiel wird die Hierarchie öffentlicher Ordner für das Postfach für öffentliche Ordner "PF\_marketing" aktualisiert, und die Ausgabe des Befehls wird unterdrückt.

```
Update-PublicFolderMailbox -Identity PF_marketing -InvokeSynchronizer -SuppressStatus
```

In diesem Beispiel werden alle Postfächer für öffentliche Ordner aktualisiert, und die Ausgabe des Befehls wird unterdrückt.

```
Get-Mailbox -PublicFolder | Update-PublicFolderMailbox -InvokeSynchronizer -SuppressStatus
```

# Entfernen eines öffentlichen Ordners

18.12.2018 • 3 minutes to read

Sie müssen möglicherweise öffentliche Ordner entfernen, die nicht länger in Ihrer Organisation verwendet werden. Informationen dazu, welche Öffentlichen Ordner entfernt werden sollten, finden Sie unter [Anzeigen von Statistiken für öffentliche Ordner und Elemente öffentlicher Ordner](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Öffentliche Ordner" im Thema [Freigabe- und Zusammenarbeitsberechtigungen](#).
- Sie können einen E-Mail-aktivierten öffentlichen Ordner nicht löschen. Bevor Sie den Ordner löschen können, müssen Sie E-Mails für den öffentlichen Ordner deaktivieren. Weitere Informationen finden Sie unter [E-Mail-Aktivierung oder E-Mail-Deaktivierung von öffentlichen Ordnern](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Was möchten Sie machen?

### Entfernen eines öffentlichen Ordners mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie zu **Öffentliche Ordner > Öffentliche Ordner**.
2. Wählen Sie in der Listenansicht den öffentlichen Ordner aus, den Sie löschen möchten. Beim Klicken auf den Ordnernamen werden Unterordner innerhalb dieses Ordners angezeigt, sofern welche vorhanden sind. An diesem Punkt können Sie durch Klicken einen bestimmten Unterordner zum Entfernen auswählen.

Um einen Ordner oder Unterordner zu löschen, klicken Sie auf eine beliebige Stelle auf den Ordner Zeile bis auf den unterstrichenen Namen des Ordners, und klicken Sie dann auf **Löschen**. Wenn Sie auf den unterstrichenen Namen des Ordners klicken, werden die Option **Löschen** nicht zur Verfügung.



## Exchange-Verwaltungskonsole

- Dashboard
- Empfänger
- Berechtigungen
- Verwaltung der Compliance
- Organisation
- Schutz
- Erweiterte Bedrohungen
- Nachrichtenfluss
- Mobil
- Öffentliche Ordner**

Öffentliche Ordner Postfächer für öffentliche Ordner

+ ⎯ ↑ ⏪ ⏴ ⏵

\

NAME DES UNTERORDNERS	HAT UNTERORDNER	E-MAIL-AKTIVIERT
Marketing – Kampagne	Nein	Nein
<b>Vertrieb – Leiter</b>	Nein	Nein

3. Sie werden in einem Warnungsfeld gefragt, ob Sie den öffentlichen Ordner wirklich löschen möchten.  
Klicken Sie auf **Ja**, um den Vorgang fortzusetzen.

### Verwenden Sie Exchange Online PowerShell, um einen öffentlichen Ordner zu löschen.

In diesem Beispiel wird der öffentliche Ordner "Help Desk\Resolved" gelöscht. Bei diesem Befehl wird vorausgesetzt, dass der öffentliche Ordner "Resolved" keine Unterordner umfasst.

```
Remove-PublicFolder -Identity "\Help Desk\Resolved"
```

In diesem Beispiel wird der vorherige Befehl ohne Änderungen getestet.

```
Remove-PublicFolder -Identity "\HelpDesk\Resolved" -WhatIf
```

In diesem Beispiel wird der öffentliche Ordner "Marketing" mit allen Unterordnern entfernt, da der Befehl rekursiv ausgeführt wird.

```
Remove-PublicFolder -Identity "\Marketing" -Recurse:$True
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Remove-PublicFolder](#).

# Anzeigen von Statistiken für öffentliche Ordner und Elemente öffentlicher Ordner

18.12.2018 • 5 minutes to read

In diesem Thema wird das Abrufen von Statistikdaten zu öffentlichen Ordnern (z. B. Anzeigename, Erstellungszeitpunkt, Zeitpunkt der letzten Änderung, letzter Benutzerzugriff und Elementgröße) erläutert. Anhand dieser Informationen können Sie Entscheidungen zum Löschen oder Aufbewahren von öffentlichen Ordnern treffen.

## NOTE

Sie können einige der Kontingent und Verwendungsanalyse Informationen für Öffentliche Ordner in der Exchange-Verwaltungskonsole (EAC), navigieren Sie zu **Öffentliche Ordner anzeigen** > **Bearbeiten**  > **postfachnutzung**. Allerdings diese Informationen sind unvollständig, und es wird empfohlen, dass Sie Exchange Online PowerShell verwenden, um Statistiken öffentlicher Ordner anzuzeigen.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 1 Minute.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Öffentliche Ordner" im Thema [Freigabe- und Zusammenarbeitsberechtigungen](#).
- Statistikdaten von öffentlichen Ordnern können nicht in der Exchange-Verwaltungskonsole abgerufen werden.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Was möchten Sie tun?

### Verwenden Sie Exchange Online PowerShell, um Statistiken öffentlicher Ordner abzurufen

In diesem Beispiel werden die Statistikdaten für den Öffentlichen Ordner "Marketing" mit einem anschließenden Befehl (hinter dem senkrechten Strich) zum Formatieren der Liste abgerufen.

```
Get-PublicFolderStatistics -Identity \Marketing | Format-List
```

#### **NOTE**

Der Wert für den Parameter *Identity* muss den Pfad zu dem öffentlichen Ordner enthalten. Angenommen, wenn Sie den öffentlichen Ordner "Marketing" unter dem übergeordneten Ordner Business schon, den folgenden Wert bereitstellen möchten: `\Business\Marketing`

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-PublicFolderStatistics](#).

#### **Verwenden Sie Exchange Online PowerShell, um Statistiken für Elemente öffentlicher Ordner anzuzeigen**

Sie können die folgenden Informationen zu Elementen in einem öffentlichen Ordner anzeigen:

- Typ des Elements
- Betreff
- Uhrzeit der letzten Änderung durch einen Benutzer
- Zeitpunkt des letzten Benutzerzugriffs
- Erstellungszeit
- Anlagen
- Nachrichtengröße

Mithilfe dieser Informationen können Sie Entscheidungen dazu treffen, welche Aktionen für Ihre Öffentlichen Ordner durchgeführt werden sollen, wie z. B., welche Öffentlichen Ordner gelöscht werden sollen. Beispielsweise können Sie festlegen, dass ein Öffentlicher Ordner gelöscht werden soll, wenn für mehr als 2 Jahre nicht auf die enthaltenen Elemente zugegriffen wurde, oder Sie können einen Öffentlichen Ordner, der als Dokumentrepository verwendet wird, für eine andere Clientzugriffsanwendung konvertieren.

In diesem Beispiel werden Standardstatistiken zu allen Elementen im öffentlichen Ordner "Pamphlets" im Pfad "\Marketing\2013" zurückgegeben. Standardinformationen sind u. a. Identität, Erstellungszeit und Betreff.

```
Get-PublicFolderItemStatistics -Identity "\Marketing\2013\Pamphlets"
```

In diesem Beispiel werden zusätzliche Informationen zu den Elementen im öffentlichen Ordner "Pamphlets" zurückgegeben, z. B. Betreff, Zeitpunkt der letzten Änderung, Erstellungszeit, Anlagen, Nachrichtengröße und Elementtyp. Darüber hinaus umfasst es einen weitergeleiteten Befehl zum Formatieren der Liste.

```
Get-PublicFolderItemStatistics -Identity "\Marketing\2010\Pamphlets" | Format-List
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-PublicFolderItemStatistics](#).

#### **Verwenden Sie Exchange Online PowerShell, um die Ausgabe des Cmdlets Get-PublicFolderItemStatistics in einer CSV-Datei exportieren**

In diesem Beispiel wird die Ausgabe des Cmdlets in die Datei "PFIItemStats.csv" exportiert, die die folgenden Informationen für alle Elemente im öffentlichen Ordner "\Marketing\Reports" enthält:

- Betreff der Nachricht (`Subject`)
- Datum und Uhrzeit der letzten Änderung des Elements (`LastModificationTime`)
- Information, ob das Element Anlagen enthält (`HasAttachments`)
- Typ des Elements (`ItemType`)

- Größe des Elements ( `MessageSize` )

```
Get-PublicFolderItemStatistics -Identity "\Marketing\Reports" | Select  
Subject,LastModificationTime,HasAttachments,ItemType,MessageSize | Export-Csv C:\PFIItemStats.csv
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-PublicFolderItemStatistics](#).

# Freigegebene Postfächer in Exchange Online

18.12.2018 • 7 minutes to read

**Zusammenfassung:** Informationen zu freigegebenen Postfächern in Exchange Online und deren Erstellung.

Freigegebene Postfächer erleichtern es einer Gruppe von Personen in Ihrem Unternehmen, E-Mails von einem allgemeinen Konto wie "info@contoso.com" oder "support@contoso.com" zu überwachen und zu senden. Wenn eine Person in der Gruppe auf eine Nachricht antwortet, die an das gemeinsam genutzte Postfach gesendet wurde, sieht es so aus, als sei die E-Mail von dem gemeinsamen Postfach und nicht von dem speziellen Benutzer gesendet worden.

## IMPORTANT

Wenn Sie Office 365 für Unternehmen verwenden, sollten Sie Ihre freigegebene Postfach in der Office 365-Verwaltungskonsole erstellen. Finden Sie unter [freigegebene Postfächer in Office 365 erstellen](#).

Wenn Ihre Organisation eine Exchange-Hybridumgebung verwendet, sollten Sie das lokale Exchange Admin Center (EAC) zum Erstellen und Verwalten von freigegebenen Postfächern verwenden. Weitere Informationen zu freigegebenen Postfächern finden Sie unter [Shared Mailboxes](#).

## Erstellen eines freigegebenen Postfachs mithilfe der Exchange-Verwaltungskonsole

Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Benutzerpostfächer" im Thema [Recipients Permissions](#).

1. Navigieren Sie zu **Empfänger > Shared > neue** .

2. Füllen Sie die erforderlichen Felder aus:

- **Anzeigename**

- **E-Mail-Adresse**

3. Klicken Sie auf **Hinzufügen**, um Vollzugriff oder Senden als Berechtigungen erteilen,  und wählen Sie dann die Benutzer, die Sie Berechtigungen erteilen möchten. Die STRG-Taste können Sie mehrere Benutzer auswählen. Verwirren Sie die Berechtigung zur Verwendung? Finden Sie unter [die Berechtigung, die Sie verwenden sollten?](#) weiter unten in diesem Thema.

## NOTE

Die Berechtigung "Vollzugriff" erlaubt es einem Benutzer, das Postfach zu öffnen sowie die darin gespeicherten Elemente zu erstellen und zu ändern. Die Berechtigung "Senden als" erlaubt es jeder anderen Person als dem Postfachbesitzer, E-Mails aus diesem freigegebenen Postfach zu senden. Beide Berechtigungen sind für den erfolgreichen Betrieb eines freigegebenen Postfachs erforderlich.

4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern und das freigegebene Postfach zu erstellen.

## Verwenden des EAC zum Bearbeiten der Stellvertretung für das freigegebene Postfach

1. Navigieren Sie zu **Empfänger > Shared > Bearbeiten** .

2. Klicken Sie auf **Postfachstellvertretung**.
3. Klicken Sie auf **Hinzufügen**, um gewähren oder Entfernen von Berechtigungen für Vollzugriff "und" Senden als,  oder **Entfernen von**  und wählen Sie dann die Benutzer, die Sie Berechtigungen erteilen möchten.

**NOTE**

Die Berechtigung "Vollzugriff" erlaubt es einem Benutzer, das Postfach zu öffnen sowie die darin gespeicherten Elemente zu erstellen und zu ändern. Die Berechtigung "Senden als" erlaubt es jeder anderen Person als dem Postfachbesitzer, E-Mails aus diesem freigegebenen Postfach zu senden. Beide Berechtigungen sind für den erfolgreichen Betrieb eines freigegebenen Postfachs erforderlich.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

## Verwenden eines freigegebenen Postfachs

Um zu erfahren, wie Benutzer auf freigegebene Postfächer zugreifen und diese verwenden, lesen Sie die folgenden Informationen:

- [Öffnen und Verwenden eines freigegebenen Postfachs in Outlook 2016 und Outlook 2013](#)
- [Öffnen und Verwenden eines freigegebenen Postfachs in Outlook im Web für Unternehmen](#)

## Verwenden von Exchange Online PowerShell zum Erstellen eines freigegebenen Postfachs

In diesem Beispiel wird das freigegebene Postfach "Sales Department" erstellt, und der Sicherheitsgruppe "MarketingSG" werden Vollzugriff und "Senden im Auftrag von"-Berechtigungen erteilt. Benutzern, die Mitglied der Sicherheitsgruppe sind, werden die Berechtigungen für das Postfach erteilt.

**NOTE**

In diesem Beispiel wird davon ausgegangen, dass Sie bereits die Sicherheitsgruppe MarketingSG erstellt haben und dass die Sicherheitsgruppe für E-Mail aktiviert ist. Weitere Informationen finden Sie unter [Verwalten von E-Mail-aktivierten Sicherheitsgruppen](#).

```
New-Mailbox -Shared -Name "Sales Department" -DisplayName "Sales Department" -Alias Sales | Set-Mailbox -GrantSendOnBehalfTo MarketingSG | Add-MailboxPermission -User MarketingSG -AccessRights FullAccess -InheritanceType All
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [new-Mailbox](#).

## Welche Berechtigungen sollten Sie verwenden?

Sie können die folgenden Berechtigungen mit einem freigegebenen Postfach verwenden.

- **Vollzugriff auf:** die Vollzugriff ermöglicht dem Benutzer das freigegebene Postfach öffnen und fungieren als Besitzer des Postfachs. Nach dem Zugriff auf das freigegebene Postfach, kann ein Benutzer Kalenderelemente erstellen. Lesen, anzeigen, löschen und Ändern von e-Mail-Nachrichten; Erstellen von Aufgaben und Kalender Kontakte. Ein Benutzer mit der Berechtigung "Vollzugriff" kann nicht jedoch keine e-Mail aus dem freigegebenen Postfach senden, sofern diese auch als senden haben oder im Auftrag senden.
- **Senden als:** Die Berechtigung "Senden als" ermöglicht es einem Benutzer, das freigegebene Postfach beim

Senden von E-Mails zu imitieren. Beispiel: Kweku meldet sich beim freigegebenen Postfach der Marketing-Abteilung an und sendet eine E-Mail. Diese wird so angezeigt, als ob die Marketing-Abteilung die E-Mail gesendet hätte.

- **Senden im Auftrag von:** die Senden im Auftrag ermöglicht dem Benutzer die e-Mails im Auftrag des freigegebenen Postfachs zu senden. Beispielsweise wenn John anmeldet, das das freigegebene Postfach Empfang Gebäude 32 und sendet eine e-Mail, es Aussehen von "John im Namen Empfang Gebäude 32" die e-Mail-Nachricht gesendet wurde. Der Exchange-Verwaltungskonsole können Sie senden Auftrag Berechtigungen erteilen Cmdlet **Set-Mailbox** mit dem Parameter *GrantSendOnBehalf* verwendet werden muss.

## Weitere Informationen

Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Adressbücher in Exchange Online

18.12.2018 • 2 minutes to read

Exchange Online-Adressbücher organisieren und Speichern von e-Mail-Adressinformationen für Empfänger in der Organisation verwendet wird. Die Themen, in denen Sie erfahren Sie mehr über und Konfigurieren von e-Mail-Adressen und Adressbüchern in Exchange Online in der folgenden Tabelle beschrieben.

WICHTIGE TERMINOLOGIE	BESCHREIBUNG	THEMA
<b>Adressbuchrichtlinien</b>	Die globalen Adressliste (GAL) ist die Masterliste der alle Empfänger in Ihrer Exchange Online-Organisation. Adressbuchrichtlinien (Adressbuchrichtlinien) bieten einen einfacheren Mechanismus zum GAL Segmentierung in Organisationen, die mehrere globale Adresslisten erfordern. Eine ABP definiert eine globale Adressliste eines Offlineadressbuchs (OAB), eine Raumliste und einen oder mehrere Adresslisten. Sie können dann die ABP Benutzern zuweisen.	<a href="#">Adressbuchrichtlinien Sie in Exchange Online</a>
<b>Adresslisten</b>	Eine Adressliste ist eine Teilmenge einer globalen Adressliste. Jede Adressliste ist eine dynamische Sammlung eines oder mehrerer Empfängertypen. Mit Adresslisten können Benutzer die Empfänger und Ressourcen suchen, die sie benötigen.	<a href="#">Adresslisten</a>
<b>E-Mail-Adressrichtlinien</b>	E-Mail-Adressrichtlinien sind die Regeln, die e-Mail-Adressen für Exchange Online-Empfänger zu erstellen.	
<b>Hierarchische Adressbücher</b>	Hierarchische Adressbücher (HAB) geben die Empfänger in der globalen Adressliste mithilfe der eindeutigen Geschäftsstruktur Ihrer Organisation an (z. B. Rang oder Verwaltungshierarchie), was eine effiziente Methode für die Suche nach internen Empfängern darstellt.	<a href="#">Hierarchische Adressbücher</a>
<b>Offlineadressbücher</b>	Ein Offlineadressbuch (OAB) ist eine Auflistung von Adresslisten, die heruntergeladen und von Benutzern, die von der Exchange Online-Organisation verbunden sind in Outlook verwendet werden können.	<a href="#">Offlineadressbücher in Exchange Online</a>

Hilfe bei täglichen E-Mail-Aufgaben, z. B. dem Organisieren von Kontakten in Outlook, finden Sie im [Office 365 Learning Center](#). Dort werden unter anderem folgende Hilfethemen behandelt:

- [Hinzufügen eines E-Mail-Kontakts](#)

- Importieren von Kontakten
- Erstellen einer Kontaktgruppe
- Senden einer E-Mail-Nachricht an eine Kontaktgruppe

# Adressbuchrichtlinien Sie in Exchange Online

18.12.2018 • 6 minutes to read

Adressbuchrichtlinien (Adressbuchrichtlinien) ermöglicht Benutzern das Admins Segment in bestimmten Gruppen können Sie benutzerdefinierte Ansichten der globalen Adressliste (GAL) der Organisation bereitstellen. Die Ziel gesetzt, um eine ABP ist einen einfacheren Mechanismus für GAL Segmentierung (auch bekannt als *Trennung GAL*) bereitstellen, in Organisationen, die mehrere globale Adresslisten erfordern.

Eine Adressbuchrichtlinie enthält diese Elemente:

- Eine globale Adressliste. Weitere Informationen zu Adresslisten finden Sie unter [Default Adresslisten in Exchange Online](#).
- Ein Offlineadressbuch (OAB). Weitere Informationen zu OABs finden Sie unter [Offline Adressbücher in Exchange Online](#).
- Eine Raumliste. Beachten Sie, dass diese Raumliste einer benutzerdefinierten Adressliste ist, der angibt, Räume (enthält den Filter `RecipientDisplayType -eq 'ConferenceRoomMailbox'`). Es ist keine raumsuche, die Sie mit der Option `RoomList` im Cmdlet **New-DistributionGroup** oder **Set-DistributionGroup** erstellen. Weitere Informationen finden Sie unter [Erstellen und Verwalten von Besprechungsraum-Postfächern in Exchange Online](#).
- Eine oder mehrere Adresslisten. Weitere Informationen zu Adresslisten finden Sie unter [benutzerdefinierte Adresslisten in Exchange Online](#).

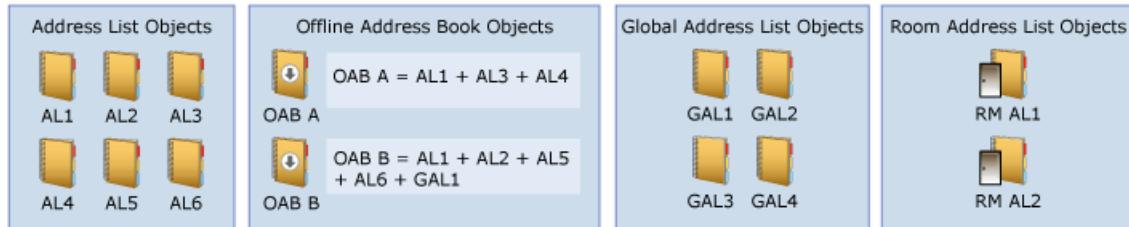
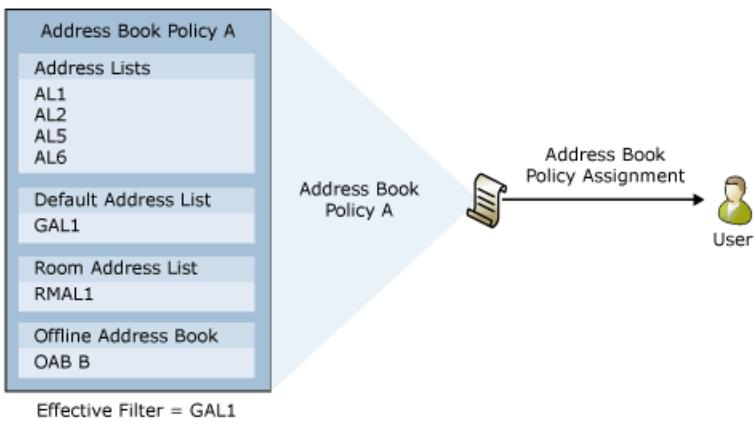
Im Zusammenhang mit Adressbuchrichtlinien finden Sie unter [Adressbuch Richtlinie Verfahren im Exchange Online](#).

## Hinweise:

- Adressbuchrichtlinien trennen Benutzer nur virtuell in der Form von Verzeichnissen, nicht in rechtlichem Sinn.
- Implementieren eine ABP ist mehreren Schritten, die Planung erforderlich sind. Weitere Informationen finden Sie unter [Szenario: Bereitstellen von Adressbuchrichtlinien](#).

## Funktionsweise von Adressbuchrichtlinien

Das folgende Diagramm veranschaulicht die Funktionsweise von Adressbuchrichtlinien. Dem Benutzer wird die Adressbuchrichtlinie A zugewiesen, die eine Teilmenge der Adresslisten enthält, die in der Organisation verfügbar sind. Wenn die Adressbuchrichtlinie erstellt und dem Benutzer zugewiesen wird, wird die Adressbuchrichtlinie der Umfang der Adresslisten, die der Benutzer anzeigen kann.



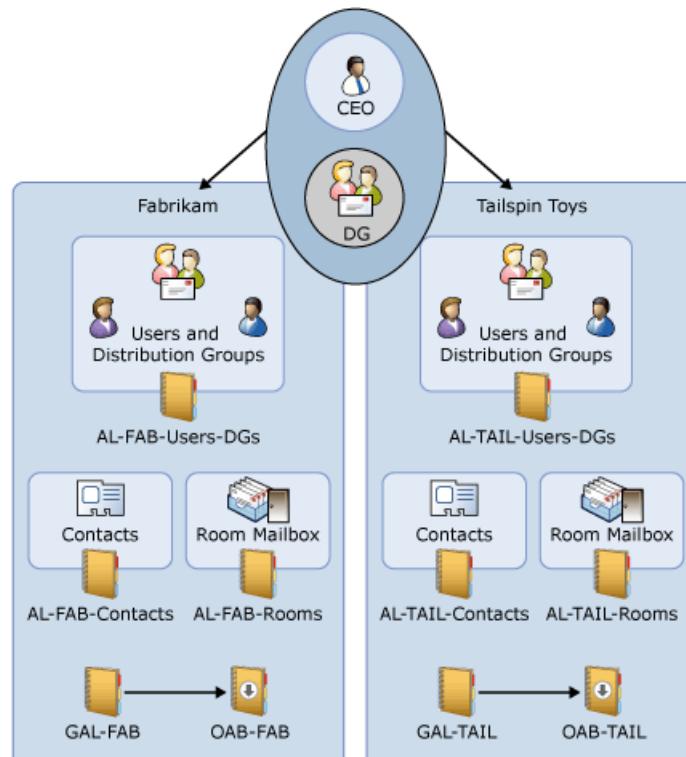
Um ABP e-Mail-routing in Exchange Online-Organisation zu aktivieren, finden Sie unter [adressbuchrichtlinie routing in Exchange Online zu aktivieren](#).

Um Adressbuchrichtlinien Benutzern zuweisen möchten, finden Sie unter [Zuweisen einer adressbuchrichtlinie zu Benutzern im Exchange Online](#).

APBs wirksam, wenn ein Benutzer in ihrer Exchange Online-Postfach eine Verbindung herstellt. Wenn Sie eine ABP ändern, wird das aktualisierte APB wirksam, wenn ein Benutzer neu gestartet oder erneut eine Verbindung her ihre e-Mail-Client-app.

## Adressbuchrichtlinie - Beispiel

Im folgenden Diagramm Freigeben von Fabrikam und Tailspin Toys der gleichen Exchange Online-Organisation und den gleichen CEO. CEO ist der einzige Mitarbeiter, die für beide Unternehmen.



Die vorgeschlagene Konfiguration umfasst drei Adressbuchrichtlinien:

- Mitarbeiter von Fabrikam wird eine ABP zugewiesen. Die GAL und Adresse Listen in der ABP zählen Fabrikam-Mitarbeiter und CEO.
- Eine ABP ist Tailspin Toys Mitarbeitern zugewiesen. Die GAL und Adresse Listen in der ABP zählen Tailspin Toys Mitarbeiter und CEO.
- Eine ABP wird nur CEO zugewiesen. (Standardeinstellung) GAL und Adresse Listen in der ABP enthalten alle Mitarbeiter (Fabrikam, Tailspin Toys und CEO).

Auf Basis dieser Konfiguration sind die Adressbuchrichtlinien hilfreich, um diese Anforderungen zu erzwingen:

- Die Benutzer bei Tailspin Toys können nur die Tailspin Toys-Mitarbeiter und den CEO anzeigen, wenn sie die GAL durchsuchen.
- Die Benutzer bei Fabrikam können nur die Fabrikam-Mitarbeiter und den CEO anzeigen, wenn sie die GAL durchsuchen.
- Der CEO kann alle Fabrikam- und Tailspin Toys-Mitarbeiter anzeigen, wenn er die GAL durchsucht.
- Benutzer, die die Mitgliedschaft des CEO in Gruppen anzeigen, sehen nur Gruppen, die zum Unternehmen gehören. Sie sehen nicht die Gruppen, die dem anderen Unternehmen gehören.

## Adressbuchrichtlinien für Entourage- und Outlook für Mac-Benutzer

Exchange-Webdienste (EWS), d. h., sie zum Suchen der globalen Adressliste basierend auf der zugewiesenen ABP. oder Entourage und Outlook für Mac-Clients, die Verbindung mit Exchange Online-Postfächer können ein OAB

In hybridumgebungen, in denen das Benutzerkonto in Ihrer lokalen Organisation ist und das Postfach befindet sich in Exchange Online, Adressbuchrichtlinien funktionieren nicht für Entourage und Outlook für Mac-Benutzer, die auf ihre Postfächer aus dem Unternehmensnetzwerk herstellen, da Entourage und Outlook für Mac verbinden direkt mit globalen einen Katalogserver zum Abfragen von Active Directory (die die Adressbuchrichtlinien umgeht). Außerhalb des Firmennetzwerks befinden können Sie ein OAB oder Exchange-Webdienste (EWS), d. h., sie zum Suchen der globalen Adressliste basierend auf der zugewiesenen ABP.

Weitere Informationen zum Verwalten von Outlook für Mac 2011 finden Sie unter [Planning for Outlook für Mac 2011](#).

# Address Book Policy Verfahren in Exchange Online

18.12.2018 • 2 minutes to read

[Aktivieren der adressbuchrichtlinie routing in Exchange Online](#)

[Erstellen Sie eine adressbuchrichtlinie in Exchange Online](#)

[Zuweisen einer adressbuchrichtlinie zu Benutzern in Exchange Online](#)

[Ändern der Einstellungen einer adressbuchrichtlinie in Exchange Online](#)

[Entfernen einer adressbuchrichtlinie in Exchange Online](#)

# Aktivieren der adressbuchrichtlinie routing in Exchange Online

18.12.2018 • 3 minutes to read

Adressbuchrichtlinien (Adressbuchrichtlinien) ermöglichen, dass Sie für Benutzer in spezifischen Gruppen geben Segment globale Adresslisten (GALs) in Outlook und Outlook im Web (vormals Outlook Web App) angepasst. Weitere Informationen zu Adressbuchrichtlinien finden Sie unter [Adressbuch Richtlinien im Exchange Online](#).

Routing von Adressbuchrichtlinien erstellt die virtuellen Organisationen innerhalb einer einzelnen Exchange Online-Organisation. Organisationsinterne virtuellen ist abhängig von der globalen Adressliste (GAL), in dem Sie sich befinden. Wenn ABP routing aktiviert ist, wird Benutzern, die verschiedene GALs zugewiesen sind, werden als externe Empfänger angezeigt und nicht des jeweils anderen Visitenkarten anzeigen.

In Exchange Online schalten Sie können nur ABP routing in Exchange Online PowerShell.

Suchen Sie die Exchange Server-Version dieses Themas? Weitere Informationen finden Sie unter [Install and Configure the Address Book Policy Routing Agent](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Sie müssen ein Mitglied der Verwaltungsrolle Organisation werden in Exchange Online (oder ein Office 365 globaler Administrator) gruppieren, bevor Sie das Verfahren in diesem Thema ausführen können.
- Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell, ABP routing aktivieren

Um ABP routing in Exchange Online-Organisation zu aktivieren, führen Sie den folgenden Befehl aus:

```
Set-TransportConfig -AddressBookPolicyRoutingEnabled $true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-TransportConfig](#).

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Verwenden Sie zum bestätigen, dass Sie erfolgreich ABP routing aktiviert haben, können die folgenden Schritte aus:

- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um sicherzustellen, dass ABP routing für die Organisation aktiviert ist:

```
Get-TransportConfig | Format-List AddressBookPolicyRoutingEnabled
```

- Sorgen Sie dafür, dass ein Benutzer, dem eine Adressbuchrichtlinie zugewiesen wurde, eine E-Mail-Nachricht an einen Benutzer sendet, dem eine andere Adressbuchrichtlinie zugewiesen wurde, und stellen Sie sicher, dass die E-Mail-Adresse des Absenders nicht in dessen Anzeigenamen aufgelöst wird.

# Erstellen Sie eine Adressbuchrichtlinie in Exchange Online

18.12.2018 • 4 minutes to read

Adressbuchrichtlinien (Adressbuchrichtlinien) ermöglichen, dass Sie für Benutzer in spezifischen Gruppen geben Segment globale Adresslisten (GALs) in Outlook und Outlook im Web (vormals Outlook Web App) angepasst. Weitere Informationen zu Adressbuchrichtlinien finden Sie unter [Adressbuch Richtlinien im Exchange Online](#).

In Exchange Online können Sie nur Adressbuchrichtlinien in Exchange Online PowerShell erstellen.

Ein Adressbuchrichtlinie erfordert eine globale Adressliste (GAL), ein Offlineaddressbuch (OAB), eine Raumliste und mindestens eine Adressliste. Um die verfügbaren Objekte anzuzeigen, verwenden Sie die Cmdlets **Get-GlobalAddressList**, **Get-OfflineAddressBook** und **Get-AddressList**.

**Hinweis:** die Raumliste, die für eine ABP eine Adressliste ist, der angibt, Chatrooms erforderlich ist (enthält den Filter `RecipientDisplayType -eq 'ConferenceRoomMailbox'`). Es ist nicht Finder-Raum Verteilergruppe, die Sie mit der Option `RoomList` in den Cmdlets **New-DistributionGroup** oder **Set-DistributionGroup** erstellen.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 5 Minuten.
- Standardmäßig ist nicht die Adressliste Rolle alle Rollengruppen in Exchange Online zugewiesen. Um-Cmdlets oder Features, die die Rolle Adressliste erfordern zu verwenden, müssen Sie die Rolle zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie unter [Rollengruppen ändern](#).
- Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Erstellen eine ABP für eine Organisation ist mehreren Schritten, die Planung erforderlich sind. Weitere Informationen finden Sie unter [Szenario: Bereitstellen von Adressbuchrichtlinien](#).
- Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um eine ABP erstellen

Verwenden Sie folgende Syntax, um eine Adressbuchrichtlinie zu erstellen:

```
New-AddressBookPolicy -Name "<Unique Name>" -GlobalAddressList "<GAL>" -OfflineAddressBook "<OAB>" -RoomList "<RoomList>" -AddressLists "<AddressList1>","<AddressList2>"...
```

In diesem Beispiel wird eine Adressbuchrichtlinie mit den folgenden Einstellungen erstellt:

- **Name:** All Fabrikam ABP
- **GAL:** All Fabrikam
- **OAB:** Fabrikam-All-OAB
- **Raumliste:** All Fabrikam Rooms
- **Adresslisten:** "All Fabrikam", "All Fabrikam Mailboxes", "All Fabrikam DLs" und "All Fabrikam Contacts"

```
New-AddressBookPolicy -Name "All Fabrikam ABP" -AddressLists "\All Fabrikam","\All Fabrikam Mailboxes","\All Fabrikam DLS","\All Fabrikam Contacts" -OfflineAddressBook \Fabrikam-All-OAB -GlobalAddressList "\All Fabrikam" -RoomList "\All Fabrikam Rooms"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-AddressBookPolicy](#).

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Um zu überprüfen, ob eine ABP erfolgreich erstellt wurde, verwenden Sie eine der folgenden Vorgehensweisen in Exchange Online PowerShell:

- Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die ABP aufgeführt wird:

```
Get-AddressBookPolicy
```

- Ersetzen Sie \_ <ABPName> \_ mit dem Namen der ABP und führen den Befehl zum Überprüfen der Eigenschaftswerte:

```
Get-AddressBookPolicy -Identity "<ABPName>" | Format-List
```

## Weitere Informationen

Nachdem Sie eine ABP erstellt haben, müssen Sie die ABP Benutzern zuweisen. Anweisungen finden Sie unter [Zuweisen einer adressbuchrichtlinie zu Benutzern in Exchange Online](#).

# Zuweisen einer Adressbuchrichtlinie zu Benutzern in Exchange Online

18.12.2018 • 10 minutes to read

Adressbuchrichtlinien (Adressbuchrichtlinien) ermöglichen, dass Sie für Benutzer in spezifischen Gruppen geben Segment globale Adresslisten (GALs) in Outlook und Outlook im Web (vormals Outlook Web App) angepasst. Weitere Informationen zu Adressbuchrichtlinien finden Sie unter [Adressbuch Richtlinien im Exchange Online](#).

Benutzer werden bei der Erstellung von Postfächern nicht automatisch einer Adressbuchrichtlinie zugewiesen. Wenn Sie einem Postfach keine Adressbuchrichtlinie zuweisen, ist die globale Adressliste für die gesamte Organisation für den Benutzer in Outlook und Outlook im Web sichtbar.

Um Ihre virtuellen Organisationen für Adressbuchrichtlinien identifiziert haben, wird empfohlen, auf Postfächer, Kontakte und Gruppen, die **CustomAttribute1 - CustomAttribute15** -Attributen zu verwenden, da diese Attribute, die am häufigsten verfügbar und einfach zu verwaltende für werden alle Empfängertypen. Weitere Informationen finden Sie unter [Szenario: Bereitstellen von Adressbuchrichtlinien](#).

Um Adressbuchrichtlinien Postfächer zuzuweisen, wählen Sie im Exchange Administrationscenter (EAC) die ABP aus, oder geben Sie die ABP in Exchange Online PowerShell.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 5 Minuten.
- Standardmäßig ist nicht die Adressliste Rolle alle Rollengruppen in Exchange Online zugewiesen. Um Cmdlets oder Features, die die Rolle Adressliste erfordern zu verwenden, müssen Sie die Rolle zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie unter [Rollengruppen ändern](#).
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole eine ABP einem Postfach zuweisen

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Klicken Sie in der Liste der Benutzerpostfächer auf das Postfach, das Sie ändern möchten. Sie können:
  - Einen Bildlauf durch die Liste von Benutzerpostfächern ausführen.
  - Klicken Sie auf **Suche**  , und geben Sie Teil Name, e-Mail-Adresse oder Alias des Benutzers.

- Klicken Sie auf **Weitere Optionen**  > **Erweiterte Suche**, auf das Postfach zu finden.

Wenn Sie das Postfach, die Sie ändern möchten gefunden haben, wählen Sie sie aus, und klicken Sie dann auf **Bearbeiten** .

3. Klicken Sie auf der Eigenschaftenseite des Postfachs auf **Postfachfunktionen**.
4. Klicken Sie auf den Dropdownpfeil in **adressbuchrichtlinie**, und wählen Sie die ADP, die Sie anwenden möchten.

Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

## Weisen Sie eine ABP auf mehrere Postfächer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger** > **Postfächer**.
2. Klicken Sie in der Liste der Postfächer auf das Postfach, das Sie ändern möchten. Zum Beispiel:
  - a. Klicken Sie auf **Weitere Optionen**  > **Erweiterte Suche**.
  - b. Wählen Sie im Fenster **Erweiterte Suche**, das geöffnet wird, **Empfängertypen** aus, und überprüfen Sie den Standardwert **Benutzerpostfach**.
  - c. Klicken Sie auf **Weitere Optionen**, und klicken Sie dann auf **Bedingung hinzufügen**.
  - d. **Wählen Sie eine** Dropdown-Liste, die angezeigt wird, wählen Sie im die entsprechende **benutzerdefinierte Attribut 1** auf **benutzerdefiniertes Attribut 15** Werte, die Ihre virtuellen Organisationen definiert.
  - e. Geben Sie im dann angezeigten Dialogfeld **Wörter oder Ausdrücke angeben** den Wert ein, den Sie suchen möchten, und klicken Sie dann auf **OK**.
  - f. Klicken Sie wieder auf das Fenster **Erweiterte Suche** auf **OK**. In der Exchange-Verwaltungskonsole auf **Empfänger** > **Postfächer**, klicken Sie auf **Weitere Optionen** > **Erweiterte Suche**, Benutzerpostfächer zu erhalten.

3. Wählen Sie in der Liste der Postfächer mehrere Postfächer desselben Typs aus (z. B. **Benutzer**) aus der Liste aus. Beispiel:

- Wählen Sie ein Postfach, halten Sie die UMSCHALTTASTE gedrückt, und wählen Sie ein anderes Postfach aus, das sich in der Liste weiter unten befindet.
- Halten Sie die STRG-Taste gedrückt, während Sie die einzelnen Postfächer auswählen.

Nachdem Sie mehrere Postfächer desselben Typs ausgewählt haben, ändert sich der Titel des Detailbereichs zu **Massenbearbeitung**.

4. Klicken Sie im Detailbereich einen Bildlauf nach unten und klicken Sie auf **Weitere Optionen**, führen Sie einen Bildlauf nach unten zu **Adressbuchrichtlinie** und klicken Sie dann auf **Aktualisieren**.

5. Wählen Sie in **Massen zuweisen adressbuchrichtlinie** Fenster, das geöffnet wird die ABP durch Klicken auf den Dropdownpfeil in **Adressbuchrichtlinie wählen Sie** aus, und klicken Sie dann auf **Speichern**.

## Verwenden von Exchange Online PowerShell Postfachbenutzer eine

## ABP zuweisen

Es gibt drei grundlegende Methoden, die Sie verwenden können, um eine ABP auf Postfächer anzuwenden:

- **Einzelne Postfächer:** Verwenden Sie die folgende Syntax:

```
Set-Mailbox -Identity <MailboxIdentity> -AddressBookPolicy <ABPIdentity>
```

In diesem Beispiel wird die mit dem Namen der Postfach-joe@fabrikam.com All Fabrikam ABP.

```
Set-Mailbox -Identity joe@fabrikam.com -AddressBookPolicy "All Fabrikam"
```

- **Filtern von Postfächern von Attributen:** Diese Methode verwendet das eindeutige filterbare-Attribut, das die virtuelle Organisation (beispielsweise die **CustomAttribute1** über Attributwert **CustomAttribute15**) definiert.

Die Syntax verwendet die folgenden zwei Befehle (eins zum Identifizieren der Postfächer, und ein weiterer die ABP auf die Postfächer angewendet):

```
$<VariableName> = Get-Mailbox -ResultSize unlimited -Filter <Filter>
```

```
$<VariableName> | foreach {Set-Mailbox -Identity $_.MicrosoftOnlineServicesID -AddressBookPolicy <ABPIdentity>}
```

In diesem Beispiel wird die ABP namens "All Fabrikam" auf alle Postfachbenutzer, dessen Wert **CustomAttribute15** ist **FAB**.

```
$Fabrikam = Get-Mailbox -Filter {((CustomAttribute15 -eq 'FAB'))}
```

```
$Fabrikam | foreach {Set-Mailbox -Identity $_.MicrosoftOnlineServicesID -AddressBookPolicy "All Fabrikam"}
```

- **Verwenden einer Liste von bestimmte Postfächer:** Diese Methode erfordert eine Textdatei, um die Postfächer zu identifizieren. Werte, die keine Leerzeichen (beispielsweise das Benutzerkonto) enthalten am besten. Die Textdatei muss ein Benutzerkonto in jeder Zeile wie die folgende enthalten:

```
akol@contoso.com
```

```
tjohnston@contoso.com
```

```
kakers@contoso.com
```

Die Syntax verwendet die folgenden zwei Befehle (eine, um die Benutzerkonten und andere anwenden die Richtlinie auf die Benutzer identifizieren):

```
$<VariableName> = Get-Content "<text file>"
```

```
$<VariableName> | foreach {Set-Mailbox -Identity $_.MicrosoftOnlineServicesID -AddressBookPolicy <ABPIdentity>}
```

In diesem Beispiel wird die ABP-Richtlinie mit dem Namen "All Fabrikam" auf die Postfächer in der Datei

C:\My Documents\Fabrikam.txt angegeben.

```
$Fab = Get-Content "C:\My Documents\Fabrikam.txt"
```

```
$Fab | foreach {Set-Mailbox -Identity $_.MicrosoftOnlineServicesID -AddressBookPolicy "All Fabrikam"}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailbox](#) und [Get-Mailbox](#).

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Verwenden Sie zum bestätigen, dass Sie erfolgreich eine ABP einem Postfach angewendet haben, können die folgenden Schritte aus:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**, wählen Sie das Postfach aus, und klicken Sie auf **Bearbeiten**. Klicken Sie in den Eigenschaften des Fensters Postfach, das geöffnet wird, klicken Sie auf **Postfachfunktionen**, und überprüfen Sie die ABP im Feld **adressbuchrichtlinie**.
- Ersetzen Sie in Exchange Online PowerShell <MailboxIdentity> mit dem Namen alias, e-Mail-Adresse oder den Kontonamen des Postfachs und führen Sie den folgenden Befehl aus, um den Wert der Eigenschaft **AddressBookPolicy** überprüfen:

```
Get-Mailbox -Identity "<MailboxIdentity>" | Format-List AddressBookPolicy
```

- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um den Wert der Eigenschaft **AddressBookPolicy** überprüfen:

```
Get-Mailbox -ResultSize unlimited | Format-Table -Auto Name,AddressBookPolicy
```

## Weitere Informationen

Wenn die Zuordnung ABP aus einem Postfach entfernen möchten, wählen Sie den Wert **[No Richtlinie]** in der Exchange-Verwaltungskonsole, oder verwenden Sie den Wert **\$null** für den Parameter *AddressBookPolicy* in Exchange Online PowerShell.

# Ändern der Einstellungen einer Adressbuchrichtlinie

18.12.2018 • 4 minutes to read

Adressbuchrichtlinien (Adressbuchrichtlinien) ermöglichen, dass Sie für Benutzer in spezifischen Gruppen geben Segment globale Adresslisten (GALs) in Outlook und Outlook im Web (vormals Outlook Web App) angepasst. Weitere Informationen zu Adressbuchrichtlinien finden Sie unter [Adressbuch Richtlinien im Exchange Online](#).

Nachdem Sie eine ABP erstellt haben, können Sie anzeigen oder ändern Sie den Namen und die zugeordneten Adresslisten: die globale Adressliste (GAL), Offlineaddressbuch (OAB), Raumliste und Adresslisten.

In Exchange Online können Sie nur Adressbuchrichtlinien in Exchange Online PowerShell ändern.

Weitere Verwaltungsaufgaben in Bezug auf Adressbuchrichtlinien finden Sie unter [Adressbuch Richtlinie Verfahren im Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 5 Minuten.
- Standardmäßig ist nicht die Adressliste Rolle alle Rollengruppen in Exchange Online zugewiesen. Um Cmdlets oder Features, die die Rolle Adressliste erfordern zu verwenden, müssen Sie die Rolle zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie unter [Rollengruppen ändern](#).
- Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um adressbuchrichtlinien zu ändern.

Verwenden Sie folgende Syntax, um eine ABP zu ändern:

```
Set-AddressBookPolicy -Identity "<ABPName>" [-Name "<Unique Name>"] [-GlobalAddressList "<GAL>"] [-OfflineAddressBook "<OAB>"] [-RoomList "<RoomList>"] [-AddressLists <AddressLists>]
```

- Der Parameter *Name*, *GlobalAddressList*, *OfflineAddressBook* und *RoomList* dauern einzelne Werte, die von den Ihnen angegebenen Wert den vorhandenen Wert ersetzt.

In diesem Beispiel wird die Adressbuchrichtlinie namens "All Fabrikam ABP" geändert, indem das OAB durch das angegebene OAB ersetzt wird.

```
Set-AddressBookPolicy -Identity "All Fabrikam ABP" -OfflineAddressBook \Fabrikam-OAB-2
```

- Der Parameter *AddressLists* mehrere Werte akzeptiert, müssen Sie entscheiden, ob Sie *Ersetzen* möchten die vorhandenen in die ABP Adresslisten oder *Hinzufügen und Entfernen* von Adresslisten wirkt sich die anderen Adresslisten in der ABP.

In diesem Beispiel werden die vorhandenen Adresslisten in der Adressbuchrichtlinie namens „Government Agency A“ durch die angegebenen Adresslisten ersetzt.

```
Set-AddressBookPolicy -Identity "Government Agency A" -AddressLists "GovernmentAgencyA-Atlanta","GovernmentAgencyA-Moscow"
```

Um eine ABP Adresslisten hinzuzufügen, müssen Sie angeben, dass die neue Adresse *und* alle vorhandenen Adresslisten aufgeführt werden, die Sie beibehalten möchten.

In diesem Beispiel wird die Adressliste mit dem Namen „Contoso-Chicago“ der Adressbuchrichtlinie mit dem Namen „ABP Contoso“ hinzugefügt, die bereits so konfiguriert ist, dass die Adressliste mit dem Namen „Contoso-Seattle“ verwendet wird.

```
Set-AddressBookPolicy -Identity "ABP Contoso" -AddressLists "Contoso-Chicago","Contoso-Seattle"
```

Um Adresslisten aus einer Adressbuchrichtlinie zu entfernen, müssen Sie die vorhandenen Adresslisten angeben, die Sie behalten möchten, und die Adresslisten weglassen, die Sie entfernen möchten.

Die Adressbuchrichtlinie „ABP Fabrikam“ verwendet beispielsweise die Adresslisten mit dem Namen „Fabrikam-HR“ und „Fabrikam-Finance“. Geben Sie zum Entfernen der Adressliste „Fabrikam-HR“ nur die Fabrikam-Finance-Adressliste an.

```
Set-AddressBookPolicy -Identity "ABP Fabrikam" -AddressLists Fabrikam-Finance
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-AddressBookPolicy](#).

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Ersetzen Sie zum bestätigen, dass haben Sie erfolgreich eine ABP ändern, \_ <ABPName> \_ durch den Namen des der ABP, und führen Sie den folgenden Befehl in Exchange Online PowerShell so überprüfen Sie die Eigenschaftswerte:

```
Get-AddressBookPolicy -Identity "<ABPName>" | Format-List
```

# Entfernen einer Adressbuchrichtlinie

18.12.2018 • 4 minutes to read

Adressbuchrichtlinien (Adressbuchrichtlinien) ermöglichen, dass Sie für Benutzer in spezifischen Gruppen geben Segment globale Adresslisten (GALs) in Outlook und Outlook im Web (vormals Outlook Web App) angepasst. Weitere Informationen zu Adressbuchrichtlinien finden Sie unter [Adressbuch Richtlinien im Exchange Online](#).

Sie können nur Adressbuchrichtlinien aus Ihrer Exchange Online-Organisation mit Exchange Online PowerShell, entfernen und nur, wenn die ABP zugewiesen wird nicht an ein Postfach, (aktive Postfächer oder vorläufig gelöschten Postfächer, die noch wiederhergestellt werden).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 5 Minuten.
- Standardmäßig ist nicht die Adressliste Rolle alle Rollengruppen in Exchange Online zugewiesen. Um Cmdlets oder Features, die die Rolle Adressliste erfordern zu verwenden, müssen Sie die Rolle zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie unter [Rollengruppen ändern](#).
- Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Entfernen einer ABP mithilfe von Exchange Online PowerShell

### Schritt 1: Stellen Sie sicher, dass die ABP für ein Postfach zugewiesen ist nicht

1. Ersetzen Sie <ABPName> mit dem Namen der ABP und führen den folgenden Befehl, um den Wert **DistinguishedName** (DN) der ABP abzurufen, die Sie entfernen möchten:

```
Get-AddressBookPolicy -Identity "<ABPName>" | Format-List DistinguishedName
```

2. Um herauszufinden, ob die ABP einem aktiven Postfach zugewiesen ist, ersetzen Sie <ABPDistinguishedName> mit dem DN der ABP und den folgenden Befehl ausführen:

```
Get-Mailbox -ResultSize unlimited -Filter {AddressBookPolicy -eq '<ABPDistinguishedName>'}
```

Um die Zuordnung ABP aus aktiven Postfächern zu entfernen, die hilfreich, ersetzen <ABPDistinguishedName> mit dem DN der die ABP und führen Sie die folgenden Befehle aus:

```
$a = Get-Mailbox -ResultSize unlimited -Filter {AddressBookPolicy -eq '<ABPDistinguishedName>'}
```

```
$a | foreach {Set-Mailbox -Identity $_.MicrosoftOnlineServicesID -AddressBookPolicy $null}
```

3. Um herauszufinden, ob die ABP einem vorläufig gelöschten (wiederherstellbare) Postfach zugewiesen ist,

ersetzen Sie <ABPDistinguishedName> mit dem DN der ABP und den folgenden Befehl ausführen:

```
Get-Mailbox -SoftDeletedMailbox -ResultSize unlimited -Filter {AddressBookPolicy -eq ''}
```

Um die Zuordnung ABP aus vorläufig gelöschten Postfächern zu entfernen, die hilfreich, ersetzen <ABPDistinguishedName> mit dem DN der die ABP und führen Sie die folgenden Befehle aus:

```
$s = Get-Mailbox -SoftDeletedMailbox -ResultSize unlimited -Filter {AddressBookPolicy -eq ''}
```

```
$s | foreach {Set-Mailbox -Identity $_.MicrosoftOnlineServicesID -AddressBookPolicy $null}
```

**Hinweis:** Wenn Sie eine ABP einem Postfach zuweisen nicht, wird die GAL, global für die gesamte Organisation für den Benutzer in Outlook und Outlook im Web sichtbar werden. Anstatt mit dem Wert \$null, Sie können den Namen einer anderen ABP (eingeschlossen in Anführungszeichen ein, wenn der Name Leerzeichen enthält) angeben.

## Schritt 2: Entfernen der ABP

Verwenden Sie folgende Syntax, um eine Adressbuchrichtlinie zu entfernen:

```
Remove-AddressBookPolicy -Identity <ABPIdentity>
```

Dieses Beispiel entfernt die ABP ABP TailspinToys Namens.

```
Remove-AddressBookPolicy -Identity "ABP TailspinToys"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Remove-AddressBookPolicy](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie eine ABP erfolgreich entfernt haben, verwenden Sie eine der folgenden Vorgehensweisen in Exchange Online PowerShell:

- Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die ABP nicht aufgeführt ist:

```
Get-AddressBookPolicy
```

- Ersetzen Sie \_ <ABPName> \_ mit dem Namen der ABP und führen den folgenden Befehl, um zu bestätigen, dass ein Fehler zurückgegeben wird:

```
Get-AddressBookPolicy -Identity "<ABPName>"
```

# Adresslisten in Exchange Online

18.12.2018 • 11 minutes to read

Eine Adressliste ist eine Auflistung von e-Mail-aktivierten Empfängerobjekten in Exchange Online. Adresslisten basieren auf Empfängerfiltern. Sie können nach Empfängertyp (beispielsweise Postfächer und e-Mail-Kontakte), Empfängereigenschaften (z. B. Unternehmen oder Bundesland oder Kanton) oder beides filtern. Adresslisten werden nicht statische; Sie sind dynamisch aktualisiert. Beim Erstellen oder Ändern von Empfängern in Ihrer Organisation werden automatisch die entsprechenden Adresslisten hinzugefügt. Dies sind die verschiedenen Typen von Adresslisten, die verfügbar sind:

- **Globale Adresslisten (GALs):** die integrierte GAL, das automatisch von Exchange Online erstellt enthält alle e-Mail-aktivierte Objekte in der Organisation. Sie können zusätzliche GALs zum Trennen von Benutzern nach Organisation oder Standort erstellen, aber ein Benutzer kann nur finden Sie unter und Verwenden einer globalen Adressliste.
- **Adresslisten:** Adresslisten sind Teilmengen von Empfängern, die in einer Liste weshalb sie leichter zusammengefasst sind zu von Benutzern zu finden sind. Exchange Online ist mit mehreren integrierten Adresslisten, und Sie können mehr basierend auf Anforderungen der Organisation erstellen.
- **Offlineadressbücher (OABs):** OABs Adresslisten und globale Adresslisten enthalten. OABs werden für den lokalen Zugriff zu Adresslisten und globale Adresslisten für Empfänger suchen von Outlook-Clients im Exchange-Cache-Modus verwendet. Weitere Informationen finden Sie unter [Offlineadressbücher in Exchange Online].

Benutzer in Ihrer Organisation verwenden Sie Adresslisten und der globalen Adressliste an Empfänger für e-Mail-Nachrichten suchen. Es folgt ein Beispiel für welche Adresse Listen aussehen wie in Outlook 2016:



Im Zusammenhang mit Adresslisten finden Sie unter [der Adressliste Verfahren im Exchange Online](#).

## Hinweise:

- Standardmäßig ist nicht die Adressliste Rolle alle Rollengruppen in Exchange Online zugewiesen. Um-Cmdlets oder Features, die die Rolle Adressliste erfordern zu verwenden, müssen Sie die Rolle zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie unter [Rollengruppen ändern](#).
- Musterfiltern Empfängerfiltern oder benutzerdefinierten Empfängerfiltern identifizieren die Empfänger, die in Adresslisten und globale Adresslisten enthalten sind. Weitere Informationen finden Sie unter [Empfängerfilter für Adresslisten in Exchange Online PowerShell](#).
- Sie können den Empfänger aus allen Adresslisten und globale Adresslisten ausblenden. Weitere Informationen finden Sie unter [Empfänger aus Adresslisten ausgeblendet](#).

## Globale Adresslisten

Standardmäßig weist eine neue Exchange Online-Organisation eine GAL mit der standardmäßigen globalen Adressliste ab, das das primäre Repository von allen Empfängern in der Organisation ist. Die meisten Organisationen haben in der Regel nur eine GAL, da Benutzer nur anzeigen und einer globalen Adressliste in Outlook und Outlook im Web verwenden (vormals Outlook Web App) können. Sie müssen möglicherweise mehrere globale Adresslisten zu erstellen, wenn Sie verhindern, dass Gruppen von Empfängern miteinander (beispielsweise einzelne Sie, dass Exchange Online-Organisation zwei separate Unternehmen enthält) sehen möchten. Wenn Sie zum Erstellen von Adresslisten planen, berücksichtigen Sie die folgenden Aspekte:

- Sie können nur mithilfe der Exchange-Online-PowerShell erstellen, ändern, entfernen und Aktualisieren von GALs.
- Die globale Adressliste, die Benutzer in Outlook und Outlook im Web finden Sie unter heißt Global Address List, obwohl die Standard-GAL globale Standardadressliste heißt und erfordern neuen globale Adresslisten, die Sie erstellen einen eindeutigen Namen (Benutzer können nicht feststellen, welche globale Adressliste, dass Sie ihre nach Namen verwenden).
- Die Benutzer sehen nur eine globale Adressliste, der sie angehören (des Empfängerfilters der globalen Adressliste enthält diese). Wenn ein Benutzer mehrere GALs angehört, wird weiterhin angezeigt, dass nur eine GAL auf die folgenden Bedingungen basieren:
  - Der Benutzer benötigt die Berechtigung zum Anzeigen der globalen Adressliste. Sie können globale Adresslisten Benutzerberechtigungen zuweisen, mithilfe von adressbuchrichtlinien (Adressbuchrichtlinien). Weitere Informationen finden Sie unter [Adressbuch Richtlinien im Exchange Online](#).
  - Wenn ein Benutzer weiterhin mehrere globale Adresslisten angezeigt werden kann, wird nur die größte globale Adressliste (GAL, die die meisten Empfänger enthält).
  - Jede GAL benötigt eine entsprechende Offlineaddressbuch (OAB), die die globalen Adressliste enthält. Erstellen von OABs finden Sie unter [Erstellen eines Offlineaddressbuchs Buch im Exchange Online](#).

## Standardadresslisten

Standardmäßig im Lieferumfang von Exchange Online fünf integrierten Adresslisten und einer globalen Adressliste. Diese Adresslisten werden in der folgenden Tabelle beschrieben. Beachten Sie, dass standardmäßig Postfächer System betreffen, wie vermittlungspostfächer und Postfächer für Öffentliche Ordner ausgeblendet sind Listen beheben.

NAME	TYP	BESCHREIBUNG	EMPFÄNGERFILTER VERWENDET
Alle Kontakte	Adressliste	Enthält alle e-Mail-Kontakte in der Organisation. Weitere Informationen zum e-Mail-Kontakten finden Sie unter <a href="#">Recipients in Exchange Online</a> .	{Alias -ne \$null -and (ObjectCategory -like 'person' -and ObjectClass -eq 'contact')}
Alle Verteilerlisten	Adressliste	Enthält alle Verteilergruppen, e-Mail-aktivierte Sicherheitsgruppen und dynamische Verteilergruppen in der Organisation. Weitere Informationen zum e-Mail-aktivierte Gruppen finden Sie unter <a href="#">Recipients in Exchange Online</a> .	{Alias -ne \$null -and ObjectCategory -like 'group'}

NAME	TYP	BESCHREIBUNG	EMPFÄNGERFILTER VERWENDET
Alle Räume	Adressliste	Enthält alle raumpostfächer. Gerätepostfächer nicht enthalten sein. Weitere Informationen zu Raum- und Geräte (Ressourcenpostfächer) finden, finden Sie unter <a href="#">Recipients in Exchange Online</a> .	{Alias -ne \$null -and (RecipientDisplayType -eq 'ConferenceRoomMailbox' -or RecipientDisplayType -eq 'SyncedConferenceRoomMailbox')}
Alle Benutzer	Adressliste	Enthält alle Benutzerpostfächer, verknüpfte Postfächer, remotepostfächer (Office 365-Postfächer), freigegebene Postfächer, raumpostfächer, gerätepostfächer und e-Mail-Benutzer in der Organisation. Weitere Informationen zu diesen Empfängertypen finden Sie unter <a href="#">Recipients in Exchange Online</a> .	(((Alias -ne \$null) -and (((((ObjectCategory -like 'person') -and (ObjectClass -eq 'user')) -and (-not(Database -ne \$null)) -and (-not(ServerLegacyDN -ne \$null)))) -or (((ObjectCategory -like 'person') -and (ObjectClass -eq 'user')) -and ((Database -ne \$null) -or (ServerLegacyDN -ne \$null)))))) -and (-not(RecipientTypeDetailsValue -eq 'GroupMailbox'))))}
Globale Standardadressliste	GAL	Enthält alle e-Mail-aktivierten Empfängerobjekte in der Organisation (Benutzer, Kontakte, Gruppen, dynamische Verteilergruppen und Öffentliche Ordner).	(((Alias -ne \$null) -and (((ObjectClass -eq 'user') -or (ObjectClass -eq 'contact')) -or (ObjectClass -eq 'msExchSystemMailbox') -or (ObjectClass -eq 'msExchDynamicDistributionList') -or (ObjectClass -eq 'group') -or (ObjectClass -eq 'publicFolder'))))}
Öffentliche Ordner	Adressliste	Enthält alle e-Mail-aktivierten Öffentlichen Ordner in Ihrer Organisation. Zugriffsberechtigungen bestimmen, wer anzeigen und Öffentliche Ordner verwenden können. Weitere Informationen zu öffentlichen Ordnern finden Sie unter <a href="#">Öffentliche Ordner in Office 365 und Exchange Online</a> .	{Alias -ne \$null -and ObjectCategory -like 'publicFolder'}

## Benutzerdefinierte Adresslisten

Exchange Online-Organisation kann Tausende von Empfängern, enthalten, damit die integrierten Adresslisten äußerst umfangreich werden konnte. Um dies zu verhindern, können Sie benutzerdefinierte Adresslisten, mit denen Benutzer gefunden, wonach sie suchen erstellen.

Angenommen Sie, ein Unternehmen, das zwei Unternehmensbereiche in einer Exchange Online-Organisation hat:

- Fourth Coffee, die importiert und verkauft Kaffeebohnen.
- Contoso, Ltd, die Insurance Richtlinien abschließt.

Bei den meisten alltäglichen Aktivitäten kommunizieren nicht Mitarbeiter von Fourth Coffee mit Mitarbeitern bei Contoso, Ltd.. Aus diesem Grund damit einfacher für Mitarbeiter, die nur in ihrer Abteilung Empfänger suchen können, erstellen Sie zwei neue benutzerdefinierte Adresslisten – eine für Fourth Coffee und eine für Contoso, Ltd. Jedoch ist ein Mitarbeiter wissen, wenn der Empfänger vorhanden ist, können sie in der globalen Adressliste suchen, die alle Empfänger aus beiden Abteilungen enthält.

In Exchange Online können Sie nur PowerShell verwenden, um benutzerdefinierte Adresslisten zu erstellen.

## Bewährte Methoden für das Erstellen von Adresslisten

Adresslisten können nützliche Tools für Benutzer darstellen, doch sie können auch frustrieren, wenn sie schlecht geplant sind. Beachten Sie die folgenden bewährten Methoden, damit sichergestellt ist, dass die Adresslisten den praktischen Anforderungen Ihrer Benutzer genügen:

- Adresslisten sollten Benutzern das Auffinden von Empfängern erleichtern.
- Vermeiden Sie so viele Adresslisten, die Benutzer erstellen welchen Listen Sie können nicht feststellen.
- Verwenden Sie eine Namenskonvention und Speicherort Hierarchie für Ihre Adresslisten, damit Benutzer sofort erkennen können, welche die Liste ist für (der Empfänger in der Liste enthalten sind). Wenn Sie Probleme beim Benennen von Ihrer Adresslisten verfügen, erstellen Sie weniger Listen und erinnern Sie Benutzer, dass sie in der globalen Adressliste jede Person in Ihrer Organisation finden können.

Ausführliche Informationen über das Erstellen von Adresslisten in Exchange Server finden Sie unter [finden Sie unter der Adressliste Verfahren im Exchange Online](#).

# Verfahren für Adresslisten in Exchange Online

18.12.2018 • 2 minutes to read

[Verwalten von Adresslisten in Exchange Online](#)

[Erstellen einer Adressliste in Exchange Online mithilfe von Empfängerfiltern](#)

[Entfernen einer globalen Adressliste in Exchange Online](#)

[Konfigurieren von Eigenschaften der globalen Adressliste in Exchange Online](#)

[Erstellen einer globalen Adressliste in Exchange Online](#)

# Verwalten von Adresslisten in Exchange Online

18.12.2018 • 16 minutes to read

Eine Adressliste ist eine Auflistung von e-Mail-aktivierten Empfängerobjekten in Exchange Online. Adresslisten basieren auf Empfängerfiltern. Weitere Informationen zu Adresslisten finden Sie unter [Address lists in Exchange Online](#).

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit Adresslisten finden Sie unter [Verfahren für Adresslisten in Exchange Online](#).

Suchen Sie die Exchange Server-Version dieses Themas? Finden Sie unter [Erstellen einer Adressliste](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Standardmäßig ist nicht die Adressliste Rolle alle Rollengruppen in Exchange Online zugewiesen. Um keine Cmdlets verwenden, die die Rolle Adressliste erfordern, müssen Sie die Rolle zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie unter [Rollengruppen ändern](#).
- Exchange Online PowerShell können nur die meisten der Verfahren in diesem Thema ausführen. Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell zum Erstellen von Adresslisten

Sie können Adresslisten mit oder ohne Empfängerfiltern erstellen. Ausführliche Informationen zu Empfängerfiltern finden Sie unter [Empfängerfilter für Adresslisten in Exchange Online PowerShell](#).

Verwenden Sie die folgende Syntax, um eine Adressliste zu erstellen:

```
New-AddressList -Name "<Address List Name>" [-Container <ExistingAddressListPath>] [<Precanned recipient filter | Custom recipient filter>] [-RecipientContainer <OrganizationalUnit>]
```

In diesem Beispiel wird eine Adressliste mit einem Musterfiltern Empfängerfilter erstellt:

- **Name:** Südosten Büros
- **Speicherort:** unter dem Stammverzeichnis ("\"), auch als "alle Adresslisten" bezeichnet, da es nicht den **Container**-Parameter verwenden, und der Standardwert ist "\".
- **Musterfiltern Empfängerfilter:** alle Benutzer mit Postfächern der Wert **Bundesland/Kanton**, in dem ist, GA, AL oder LA (Georgien, Alabama oder Louisiana).

```
New-AddressList -Name "Southeast Offices" -IncludedRecipients MailboxUsers -ConditionalStateorProvince "GA", "AL", "LA"
```

In diesem Beispiel wird eine Adressliste mit einer benutzerdefinierten Empfängerfilter erstellt:

- **Name:** Nordwesten Führungskräfte
- **Speicherort:** unter der vorhandenen Adresse Liste mit dem Namen North America an.
- **Benutzerdefinierte Empfänger filtern:** alle Benutzer mit Postfächern, wobei der **Title** -Wert enthält, Director oder Manager und der **Bundesland oder den Kanton** Wert WA, OR, oder die ID (Washington, Oregon oder Idaho).

```
New-AddressList -Name "Northwest Executives" -Container "\North America"-RecipientFilter {((RecipientType -eq 'UserMailbox') -and (Title -like '*Director*' -or Title -like '*Manager*') -and (StateOrProvince -eq 'WA' -or StateOrProvince -eq 'OR' -or StateOrProvince -eq 'ID'))}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-AddressList](#).

In diesem Beispiel wird die Adressliste mit dem Namen Oregon und Washington Benutzer mithilfe des *Parameters recipientfilter* erstellt und enthält Empfänger, die Postfachbenutzer und **StateOrProvince** auf festgelegt haben **Washington** oder **Oregon**.

```
New-AddressList -Name "Oregon and Washington" -RecipientFilter {{{(RecipientType -eq 'UserMailbox') -and ((StateOrProvince -eq 'Washington') -or (StateOrProvince -eq 'Oregon'))}}}
```

In diesem Beispiel wird durch die Verwendung vordefinierter Bedingungen eine untergeordnete Adressliste mit dem Namen "Building 34 Meeting Rooms" im übergeordneten Container "All Rooms" erstellt.

```
New-AddressList -Name "Building 34 Meeting Rooms" -Container "\All Rooms" -IncludedRecipients Resources - ConditionalCustomAttribute1 "Building 34"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-AddressList](#).

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Ersetzen Sie zum bestätigen, dass Sie erfolgreich eine Adressliste erstellt haben, `_ <AddressListIdentity> _` mit der Pfad\Name der der Adressliste, und führen den folgenden Befehl in Exchange Online Powershell So überprüfen Sie die Eigenschaftswerte:

```
Get-AddressList -Identity "<AddressListIdentity>" | Format-List  
Name,RecipientFilterType,RecipientFilter,IncludedRecipients,Conditional*
```

## Verwenden von Exchange Online Powershell, Mitglieder der Adresse anzeigen enthält

Technisch gesehen, gibt dieses Verfahrens **Alle** Empfänger (einschließlich verborgene Empfänger), die mit der Empfängerfilter für die Adressliste übereinstimmen. Die Empfänger, die tatsächlich in der Adressliste angezeigt werden haben den Eigenschaftswert **HiddenFromAddressListsEnabled** `False`.

Um die Mitglieder einer Adressliste anzeigen möchten, verwenden Sie die folgende Syntax:

```
$<VariableName> = Get-AddressList -Identity <AddressListIdentity>; Get-Recipient -ResultSize unlimited -  
RecipientPreviewFilter $<VariableName>.RecipientFilter | select  
Name,PrimarySmtpAddress,HiddenFromAddressListsEnabled
```

Dieses Beispiel gibt die Mitglieder der Adressliste mit dem Namen Südost Büros.

```
$AL = Get-AddressList -Identity "Southeast Offices"; Get-Recipient -ResultSize unlimited -  
RecipientPreviewFilter $AL.RecipientFilter | select Name,PrimarySmtpAddress,HiddenFromAddressListsEnabled
```

In diesem Beispiel werden die Ergebnisse in die Datei C:\My Documents\Southeast Büros Export.csv exportiert.

```
$AL = Get-AddressList -Identity "Southeast Offices"; Get-Recipient -ResultSize unlimited -  
RecipientPreviewFilter $AL.RecipientFilter | select Name,PrimarySmtpAddress,HiddenFromAddressListsEnabled |  
Export-Csv -NoTypeInformation -Path "C:\My Documents\Southeast Offices Export.csv"
```

## Verwenden von Exchange Online PowerShell zum Aktualisieren von Adresslisten

Das Cmdlet **Update-AddressList** (oder **Update-GlobalAddressList**) nicht in Exchange Online PowerShell zur Verfügung. Wenn der Empfänger an, die eine Adressliste angezeigt werden soll nicht der Fall ist, müssen Sie den Wert der required-Eigenschaft für diese Benutzer auf einen temporären Wert ändern, und dann wieder auf den Wert, der der Adressliste erforderlich ist. Sie können die Benutzer-Eigenschaftswerte im Aktualisieren der im Exchange Administrationscenter (EAC) oder Exchange Online PowerShell, aber es des schnellere Vorgänge in PowerShell massenbearbeitung.

Nehmen wir beispielsweise bei der Adressliste mit dem Namen Oregon und Washington Benutzer verwendet den Filter

```
((RecipientType -eq 'UserMailbox') -and ((StateOrProvince -eq 'Washington') -or (StateOrProvince -eq  
'Oregon')))
```

, aber die Adressliste nicht einschließen, jeder, dessen Eigenschaftswerte **StateOrProvince** richtig eingestellt sind. Führen Sie zum Aktualisieren der Adressliste die folgenden Schritte aus:

1. Verwenden Sie die Abfrage aus der Adressliste, um alle Benutzer zu suchen, die in der Adressliste enthalten sein sollten. Beispiel:

```
$Before = Get-User -Filter ((RecipientType -eq 'UserMailbox') -and ((StateOrProvince -eq 'Oregon') -or  
(StateOrProvince -eq 'Washington'))) -ResultSize Unlimited
```

2. Ändern Sie die required-Eigenschaft auf einen temporären Wert. Ändern Sie beispielsweise die **StateOrProvince**-Werte aus **Oregon** auf **OR**, und **Washington** auf **WA**:

```
$Before | where {$_._StateOrProvince -eq 'Oregon'} | foreach {Set-User $_.Identity -StateOrProvince OR}
```

```
$Before | where {$_._StateOrProvince -eq 'Washington'} | foreach {Set-User $_.Identity -StateOrProvince  
WA}
```

3. Suchen Sie erneut nach den gleichen Benutzern, indem Sie die temporären Eigenschaftswerte verwenden. Beispiel:

```
$After = Get-User -Filter {((RecipientType -eq 'UserMailbox') -and ((StateOrProvince -eq 'OR') -or (StateOrProvince -eq 'WA')))} -ResultSize Unlimited
```

4. Ändern Sie den temporären Wert wieder auf den gewünschten Wert ein. Ändern Sie beispielsweise die **StateOrProvince**-Werte aus **OR** auf **Oregon**, und **WA** auf **Washington**:

```
$After | where {$_.StateOrProvince -eq 'OR'} | foreach {Set-User $_.Identity -StateOrProvince Oregon}
```

```
$After | where {$_.StateOrProvince -eq 'WA'} | foreach {Set-User $_.Identity -StateOrProvince Washington}
```

#### Hinweise:

- Titel, Abteilung und Adresseigenschaften benötigen die Cmdlets **Get-User** und **Set-User**. CustomAttribute1 über CustomAttribute15 Eigenschaften erfordern die Cmdlets **Get-Mailbox** und **Set-Mailbox**. Weitere Informationen dazu, welche Eigenschaften auf welche Cmdlets zur Verfügung stehen finden Sie unter den folgenden Themen:
  - [Set-User](#)
  - [Set-Mailbox](#)
- Wenn in der Adressliste nicht nur wenige Benutzer angezeigt werden, können Sie den Wert der required-Eigenschaft für jeden Benutzer ändern. Zum Beispiel:

1. Legen Sie einen temporären Eigenschaftswert für den Benutzerfest:

```
Set-User -Identity <UserIdentity> -StateOrProvince WA
```

2. Ändern Sie den temporären Wert auf den erforderlichen Wert zurück:

```
Set-User -Identity <Identity> -StateOrProvince Washington
```

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Ersetzen Sie zum bestätigen, dass Sie erfolgreich eine Adressliste aktualisiert haben, `_ <AddressListIdentity> _` durch den Namen des der Adressliste, und führen den folgenden Befehl in Exchange Online PowerShell so überprüfen Sie die **RecipientFilterApplied** Wert der Eigenschaft:

```
Get-AddressList -Identity <AddressListIdentity> | Format-Table -Auto Name,RecipientFilterApplied
```

## Verwenden von Exchange Online PowerShell Adresslisten ändern

Die gleichen grundlegenden Einstellungen sind verfügbar als beim Erstellen der Adressliste. Weitere Informationen finden Sie im Abschnitt "[Verwenden von Exchange Online PowerShell, Adresslisten erstellen](#)" in diesem Thema.

Um eine vorhandene Adressliste ändern möchten, verwenden Sie die folgende Syntax:

```
Set-AddressList -Identity <AddressListIdentity> [-Name <Name>] [<Precanned recipient filter | Custom recipient filter>] [-RecipientContainer <OrganizationalUnit>]
```

Wenn Sie die *bedingten* Parameterwerte ändern, verwenden Sie die folgende Syntax zum Hinzufügen oder Entfernen von Werten ohne Auswirkungen auf andere vorhandenen Werte:

```
@{Add="","<Value2>"...; Remove="","<Value2>"...} .
```

In diesem Beispiel wird die vorhandene Adressliste namens Südost Büros mithilfe des musterfiltern Empfängerfilters den **Bundesland oder den Kanton** Wert TX (Texas) hinzugefügt.

```
Set-AddressList -Identity "Southeast Offices" -ConditionalStateOrProvince @{Add="TX"}
```

Ausführliche Parameterinformationen zu Syntax und finden Sie unter [Set-AddressList](#).

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Ersetzen Sie zum bestätigen, dass Sie erfolgreich eine Adressliste geändert haben, \_ <AddressListIdentity> \_ mit der Pfad\Name der der Adressliste, und führen den folgenden Befehl in Exchange Online Powershell So überprüfen Sie die Eigenschaftswerte:

```
Get-AddressList -Identity "<AddressListIdentity>" | Format-List  
Name,RecipientFilterType,RecipientFilter,IncludedRecipients,Conditional*
```

## Verwenden von Exchange Online PowerShell Adresslisten löschen

Um eine Adressliste entfernen möchten, verwenden Sie die folgende Syntax:

```
Remove-AddressList -Identity "<AddressListName>"
```

In diesem Beispiel wird die Adressliste "Sales Department" entfernt, die keine untergeordneten Adresslisten enthält.

```
Remove-AddressList -Identity "Sales Department"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Remove-AddressList](#).

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Zum bestätigen, dass Sie eine Adressliste erfolgreich entfernt haben, führen Sie den folgenden Befehl in Exchange Online Powershell, um sicherzustellen, dass die Adressliste nicht aufgeführt ist:

```
Get-AddressList
```

## Ausblenden von Empfängern in Adresslisten

Ausblenden eines Empfängers in Adresslisten verhindert nicht, dass den Empfänger empfangen von e-Mail-Nachrichten; Es wird verhindert, dass Benutzer suchen den Empfänger in Adresslisten. Der Empfänger ist für **Alle** Adresslisten und globale Adresslisten ausgeblendet (effektiv, sie sind Ausnahmen für die Empfängerfiltern in alle Adresslisten). Wenn selektiv umfassen soll der Empfänger in einigen Adressen enthalten, aber andere nicht, Sie müssen die Empfängerfiltern in den Adresslisten ein-oder Ausschließen des Empfängers anpassen.

Ein Postfach in Adresslisten ausgeblendet verhindert, dass auch Outlook das Postfach in der globalen Adressliste suchen, wenn Sie ein neues Profil erstellen, oder ein zusätzliches Postfach eines vorhandenen Profils hinzufügen. Um das verborgene Postfach in Outlook hinzuzufügen, können Sie vorübergehend das Postfach in Adresslisten sichtbar machen, Konfigurieren von Outlook und blenden Sie das Postfach in Adresslisten wieder aus.

## **Verwenden der Exchange-Verwaltungskonsole Empfänger aus Adresslisten ausgeblendet**

Klicken Sie zum Öffnen von der Exchange-Verwaltungskonsole finden Sie unter [Exchange Admin center in Exchange Online](#).

Der Exchange-Verwaltungskonsole können Sie Office 365-Gruppen aus Adresslisten ausgeblendet.

1. Wechseln Sie zu einem der folgenden Speicherorte basierend auf den Empfängertyp, in der Exchange-Verwaltungskonsole:

- **Empfänger > Postfächer:** Postfächer, verknüpfte Postfächer und remote postfächer Benutzer.
- **Empfänger > Gruppen:** Verteilung Gruppen, e-Mail-aktivierte Sicherheitsgruppen und dynamische Verteilergruppen.
- **Empfänger > Ressourcen:** Raum- und Equipment Mailboxes.
- **Empfänger > Kontakte:** Postfachbenutzer und e-Mail-Kontakte.
- **Empfänger > Shared:** freigegebene Postfächer.
- **Öffentliche Ordner > Öffentliche Ordner:** E-Mail-aktivierte Öffentliche Ordner.

2. Wählen Sie den Empfänger, die Sie in Adresslisten ausblenden möchten, und klicken Sie dann auf **Bearbeiten** (  ).

3. Das Fenster Eigenschaften wird geöffnet. Der nächste Schritt hängt von den Empfängertyp ab:

- **Postfächer, Kontakte und Shared:** Wählen Sie auf der Registerkarte **Allgemein aus Adresslisten ausgeblendet**.
- **Gruppen:** Wählen Sie auf der Registerkarte **Allgemein aus dieser Gruppe in Adresslisten ausgeblendet**.
- **Ressourcen:** auf der Registerkarte **Allgemein**, klicken Sie auf **Weitere Optionen**, und wählen Sie dann auf **aus Adresslisten ausgeblendet**.
- **Öffentliche Ordner:** Wählen Sie auf der Registerkarte **Allgemeine Eigenschaften Mail Ausblenden von Exchange-Adressenliste**.

Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

## **Verwenden von Exchange Online PowerShell, ausblenden Empfänger von-Adresse enthält.**

Um einen Empfänger aus Adresslisten ausblenden möchten, verwenden Sie die folgende Syntax:

```
Set-<RecipientType> -Identity <RecipientIdentity> -HiddenFromAddressListsEnabled $true
```

\_ <RecipientType> \_ hat einen der folgenden Werte:

- 
- 
- 
- 
- 
- 
-

- **UnifiedGroup**

In diesem Beispiel werden die Verteilergruppe namens interne Affairs aus Adresslisten ausgeblendet.

```
Set-DistributionGroup -Identity "Internal Affairs" -HiddenFromAddressListsEnabled $true
```

In diesem Beispiel werden die michelle@contoso.com Postfach in Adresslisten ausgeblendet.

```
Set-Mailbox -Identity michelle@contoso.com -HiddenFromAddressListsEnabled $true
```

**Hinweis:** Wenn Sie um den Empfänger wieder in Adresslisten sichtbar zu machen, verwenden Sie den Wert `$false` für den Parameter *HiddenFromAddressListsEnabled*.

**Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Sie können überprüfen, ob Sie erfolgreich einen Empfänger aus Adresslisten ausgeblendet haben, mithilfe der folgenden Verfahren:

- In der Exchange-Verwaltungskonsole, wählen Sie den Empfänger aus, klicken Sie auf **Bearbeiten** (  ) und vergewissern Sie sich die Ausblenden von Adresslisten Einstellung ausgewählt ist.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, und stellen Sie sicher, dass der Empfänger aufgeführt ist:

```
Get-Recipient -ResultSize unlimited -Filter {HiddenFromAddressListsEnabled -eq $true}
```

- Öffnen Sie die globale Adressliste in Outlook oder Outlook im Web (vormals Outlook Web App), und stellen Sie sicher, dass der Empfänger nicht sichtbar ist.

# Empfänger filtern für Adresslisten in Exchange Online PowerShell

18.12.2018 • 2 minutes to read

Empfängerfiltern identifizieren Sie die Empfänger, die in Adresslisten und globale Adresslisten enthalten sind. Es gibt zwei grundlegende Optionen: **musterfiltern Empfängerfiltern** und **benutzerdefinierten**

**Empfängerfiltern.** Dies sind im Wesentlichen die gleichen Empfänger Filteroptionen, die durch dynamische Verteilergruppen und e-Mail-Adressrichtlinien verwendet werden.

- **Musterempfängerfilter**

- Verwendet den erforderlichen Parameter *IncludedRecipient* mit der `AllRecipients` -Wert oder einen oder mehrere der folgenden Werte: `MailboxUsers`, `MailContacts`, `MailGroups`, `MailUsers`, oder `Resources`. Sie können mehrere Werte durch Kommas getrennt angeben.
- Sie können auch keines der optionale- *bedingte* Filterparameter: `ConditionalCompany`, `ConditionalCustomAttribute [1to15]`, `_ConditionalDepartment` und `_ConditionalStateOrProvince`.

Geben Sie mehrere Werte für eine *bedingte* Parameter mithilfe der Syntax `"<Value1>","<Value2>"...`.

Mehrere Werte des dieselbe Eigenschaft impliziert **oder** -Operator. Beispielsweise "ist gleich Abteilung Sales" oder "Marketing" oder "Finance".

- **Benutzerdefinierte Empfängerfiltern:** verwendet den erforderlichen Parameter *RecipientFilter* mit OPATH-Filter.

- Die grundlegende Syntax der OPATH-Filter ist  
`{<Property1> -<Operator> '<Value1>' <Property2> -<Operator> '<Value2>'...}`.
- Geschweifte Klammern `{ }` sind erforderlich, um das gesamte OPATH-Filter.
- Bindestriche (`-`) sind erforderlich, bevor alle Operatoren. Hier sind einige der am häufigsten verwendeten Operatoren:
  - `and`, `or`, und `not`.
  - `eq` und `ne` (entspricht, ist nicht gleich; nicht Groß-/Kleinschreibung).
  - `lt` und `gt` (kleiner als und größer als).
  - `like` und `notlike` (Zeichenfolge enthält und enthält keine; erfordert mindestens einen Platzhalter in der Zeichenfolge. Beispielsweise `{Department -like 'Sales*'}`).
- Verwenden Sie Klammern zum Gruppieren `<Property> -<Operator> '<Value>'` Anweisungen in komplexe Filter zusammen. Beispielsweise  
`{(Department -like 'Sales*' -or Department -like 'Marketing*') -and (Company -eq 'Contoso' -or Company -eq 'Fabrikam')}`
  - . Exchange speichert den Filter in der **RecipientFilter** -Eigenschaft mit jedem einzelnen-Anweisung in Klammern eingeschlossen, aber Sie müssen nicht auf diese Weise eingeben.

Weitere Informationen zu Adresslisten finden Sie unter [Address lists in Exchange Online](#).

Verfahren für Adresse, die Empfängerfilter verwenden, finden Sie unter [der Adressliste Verfahren im Exchange Online](#).

# Entfernen einer globalen Adressliste in Exchange Online

18.12.2018 • 3 minutes to read

Die integrierten globalen Adressliste (GAL), die automatisch von Exchange Online erstellt enthält alle e-Mail-aktivierte Objekte in der Organisation. Sie können zusätzliche GALs zum Trennen von Benutzern nach Organisation oder Standort erstellen, aber ein Benutzer kann nur finden Sie unter und Verwenden einer globalen Adressliste. Weitere Informationen zu Adresslisten finden Sie unter [Address lists in Exchange Online](#).

Sie können die Verfahren in diesem Thema alle benutzerdefinierten GALs entfernen, die Sie erstellt haben. Kann nicht entfernt werden:

- Die globale Adressliste mit der Standard-Offlineaddressbuch, den der integrierten GAL, die in Exchange Online verfügbar ist, und nur die globale Adressliste, den Wert der **IsDefaultGlobalAddressList** - Eigenschaft hat `True` .
- Eine globale Adressliste, die in einem Offlineaddressbuch (OAB) definiert ist. OAB-Verfahren finden Sie unter [Offline Address Book-Verfahren](#).

Zusätzliche GAL-Verwaltungsaufgaben finden Sie unter [der Adressliste Verfahren im Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Standardmäßig ist nicht die Adressliste Rolle alle Rollengruppen in Exchange Online zugewiesen. Um keine Cmdlets verwenden, die die Rolle Adressliste erfordern, müssen Sie die Rolle zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie unter [Rollengruppen ändern](#).
- Exchange Online PowerShell können nur die Verfahren in diesem Thema ausführen. Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um eine globale Adressliste entfernen

Wenn Sie eine globale Adressliste entfernen möchten, verwenden Sie die folgende Syntax:

```
Remove-GlobalAddressList -Identity <GALIdentity>
```

Dieses Beispiel entfernt die Adressliste mit dem Namen Agency eine GAL an.

```
Remove-GlobalAddressList -Identity "Agency A GAL"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Remove-GlobalAddressList](#).

**Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Zum bestätigen, dass Sie eine globale Adressliste erfolgreich entfernt haben, führen Sie den folgenden Befehl in Exchange Online PowerShell, um sicherzustellen, dass die globalen Adressliste nicht aufgeführt ist:

```
Get-GlobalAddressList
```

# Konfigurieren von Eigenschaften der globalen Adressliste in Exchange Online

18.12.2018 • 3 minutes to read

Die integrierten globalen Adressliste (GAL), die automatisch von Exchange Online erstellt enthält alle e-Mail-aktivierte Objekte in der Organisation. Sie können zusätzliche GALs zum Trennen von Benutzern nach Organisation oder Standort erstellen, aber ein Benutzer kann nur finden Sie unter und Verwenden einer globalen Adressliste. Weitere Informationen zu Adresslisten finden Sie unter [Address lists in Exchange Online](#).

So konfigurieren Sie eine globale Adressliste denselben Einstellungen sind verfügbar als beim Erstellen der globalen Adressliste. Weitere Informationen finden Sie unter [Erstellen einer globalen Adressliste aufgelistet in Exchange Online](#). Zusätzliche GAL-Verwaltungsaufgaben finden Sie unter [der Adressliste Verfahren im Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Standardmäßig ist nicht die Adressliste Rolle alle Rollengruppen in Exchange Online zugewiesen. Um keine Cmdlets verwenden, die die Rolle Adressliste erfordern, müssen Sie die Rolle zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie unter [Rollengruppen ändern](#).
- Die globale Adressliste können nicht geändert werden mit dem Namen Standard-Offlineaddressbuch, der integrierten GAL, die in Exchange Online verfügbar ist, und nur die globale Adressliste, den Wert der **IsDefaultGlobalAddressList** -Eigenschaft hat `True`.
- Einen benutzerdefinierten Empfängerfilter kann nicht mit einem musterfiltern Empfängerfilter oder umgekehrt in einer vorhandenen GAL ersetzt werden.
- Exchange Online PowerShell können nur die Verfahren in diesem Thema ausführen. Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Ausführliche Informationen zu Empfängerfiltern in der Exchange Online PowerShell finden Sie unter [Empfängerfilter für Adresslisten in Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie die Exchange Online PowerShell so ändern Sie globale Adresslisten

Verwenden Sie die folgende Syntax, um eine globale Adressliste zu ändern:

```
Set-GlobalAddressList -Identity <GALIdentity> [-Name <Name>] [<Precanned recipient filter | Custom recipient filter>]
```

Wenn Sie die musterfiltern ändern *bedingte* Parameterwerte, können die folgende Syntax zum Hinzufügen oder Entfernen von Werte ohne Auswirkungen auf andere vorhandenen Werte:

```
@{Add="<Value1>","<Value2>"...; Remove="<Value1>","<Value2>"...} .
```

In diesem Beispiel wird die vorhandene globale Adressliste mit dem Namen "Contoso" GAL, indem Sie den Wert **Unternehmen** Fabrikam des Empfängerfilters musterfiltern hinzufügen.

```
Set-GlobalAddressList -Identity "Contoso GAL" -ConditionalCompany @{Add="Fabrikam"}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-GlobalAddressList](#).

**Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Ersetzen Sie zum bestätigen, dass Sie erfolgreich eine globale Adressliste geändert haben, \_ <GAL-Name> \_ mit dem Namen der GAL und Ausführen den folgenden Befehl in Exchange Online PowerShell so überprüfen Sie die Eigenschaftswerte:

```
Get-GlobalAddressList -Identity "<GAL Name>" | Format-List  
Name,RecipientFilterType,RecipientFilter,IncludedRecipients,Conditional*
```

# Erstellen einer globalen Adressliste in Exchange Online

18.12.2018 • 3 minutes to read

Die integrierten globalen Adressliste (GAL), die automatisch von Exchange Online erstellt enthält alle e-Mail-aktivierte Objekte in der Organisation. Sie können zusätzliche GALs zum Trennen von Benutzern nach Organisation oder Standort erstellen, aber ein Benutzer kann nur finden Sie unter und Verwenden einer globalen Adressliste. Weitere Informationen zu Adresslisten finden Sie unter [Address lists in Exchange Online](#).

Wenn Ihre Organisation adressbuchrichtlinien (Adressbuchrichtlinien) verwendet, müssen Sie globale Adresslisten erstellen. Weitere Informationen finden Sie unter [Adressbuch Richtlinien im Exchange Online](#).

Zusätzliche GAL-Verwaltungsaufgaben finden Sie unter [der Adressliste Verfahren im Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Standardmäßig ist nicht die Adressliste Rolle alle Rollengruppen in Exchange Online zugewiesen. Um keine Cmdlets verwenden, die die Rolle Adressliste erfordern, müssen Sie die Rolle zu einer Rollengruppe hinzufügen. Weitere Informationen finden Sie unter [Rollengruppen ändern](#).
- Exchange Online PowerShell können nur die Verfahren in diesem Thema ausführen. Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Ausführliche Informationen zu Empfängerfiltern in der Exchange Online PowerShell finden Sie unter [Empfängerfilter für Adresslisten in Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell, Erstellen der globalen Adressliste enthält

Verwenden Sie die folgende Syntax, um eine globale Adressliste zu erstellen:

```
New-GlobalAddressList -Name "<GAL Name>" [<Precanned recipient filter | Custom recipient filter>]
```

In diesem Beispiel wird eine globale Adressliste mit einer musterfiltern Empfängerfilter erstellt:

- **Name:** Contoso GAL
- **Musterfiltern Empfängerfilter:** alle Empfängertypen, wobei der Wert **Unternehmen** Contoso ist.

```
New-GlobalAddressList -Name "Contoso GAL" -IncludedRecipients AllRecipients -ConditionalCompany Contoso
```

In diesem Beispiel wird eine globale Adressliste mit einer benutzerdefinierten Empfängerfilter erstellt:

- **Name:** Agency einer globalen Adressliste
- **Benutzerdefinierte Empfänger filtern:** alle Empfängertypen, bei denen die CustomAttribute15-Eigenschaft den Wert AgencyA enthält.

```
New-GlobalAddressList -Name "Agency A GAL" -RecipientFilter {CustomAttribute15 -like "*AgencyA*"}  
Ausführliche Informationen zu Syntax und Parametern finden Sie unter New-GlobalAddressList.
```

#### **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Ersetzen Sie zum bestätigen, dass Sie eine globale Adressliste erfolgreich erstellt wurde, \_ <GAL-Name> \_ mit dem Namen der GAL und Ausführen den folgenden Befehl in Exchange Online PowerShell so überprüfen Sie die Eigenschaftswerte:

```
Get-GlobalAddressList -Identity "<GAL Name>" | Format-List  
Name,RecipientFilterType,RecipientFilter,IncludedRecipients,Conditional*
```

# Hierarchische Adressbücher

18.12.2018 • 4 minutes to read

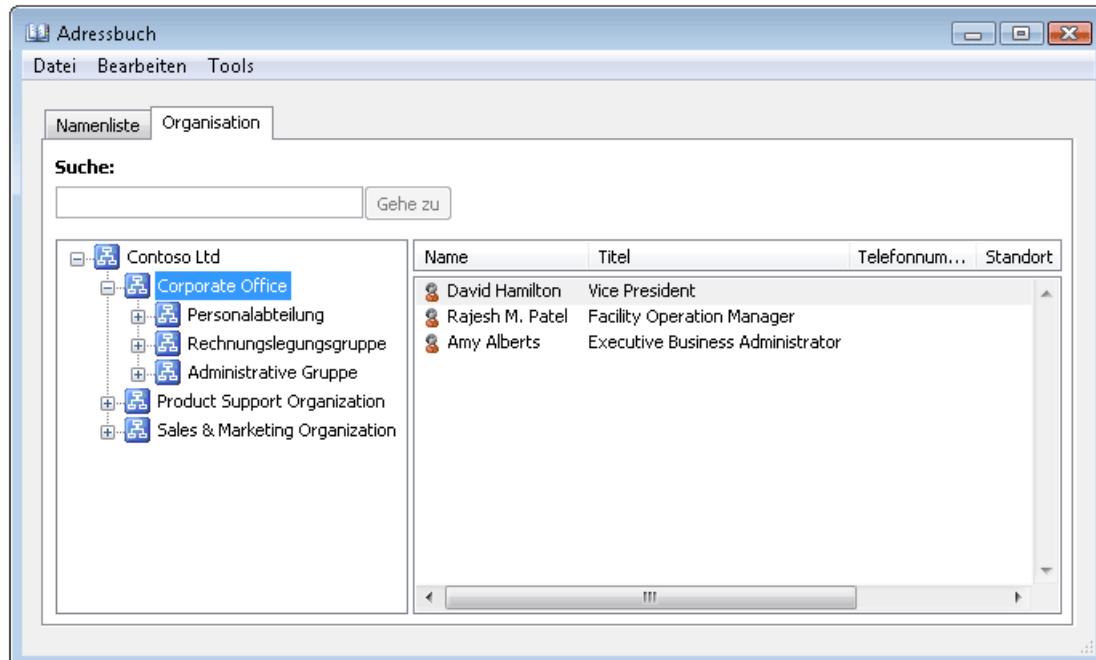
Das hierarchische Adressbuch (HAB) ermöglicht es Endbenutzern, in ihrem Adressbuch über eine Organisationshierarchie nach Empfängern zu suchen. In der Regel sind die Benutzer auf die standardmäßige globale Adressliste und die dazugehörigen Empfängereigenschaften begrenzt, und die Struktur der globalen Adressliste gibt häufig die Hierarchie unter den Empfängern in Ihrer Organisation nicht wieder. Dadurch, dass ein hierarchisches Adressbuch entsprechend den besonderen geschäftlichen Strukturen Ihrer Organisation angepasst werden kann, können Sie den Benutzern eine effiziente Möglichkeit zum Auffinden interner Empfänger bieten.

## Verwenden hierarchischer Adressbücher

In einem hierarchischen Adressbuch wird Ihre Stammorganisation (z. B. Contoso, Ltd) als oberste Ebene verwendet. Unter dieser obersten Ebene können Sie mehrere untergeordnete Ebenen hinzufügen, um ein angepasstes hierarchisches Adressbuch zu erstellen, das gemäß Geschäftsbereich, Abteilung oder einer beliebigen anderen gewählten Organisationsebene segmentiert ist. Die folgende Abbildung veranschaulicht ein hierarchisches Adressbuch für Contoso, Ltd mit folgender Struktur:

- Die oberste Ebene stellt die Stammorganisation Contoso, Ltd dar.
- Die zweite Ebene enthält die Geschäftsbereiche von Contoso, Ltd: "Corporate Office", "Product Support Organization" und "Sales & Marketing Organization".
- Die dritte Ebene enthält die Abteilungen im Geschäftsbereich "Corporate Office": "Human Resources", "Accounting Group" und "Administration Group".

### Beispiel eines hierarchischen Adressbuchs für Contoso, Ltd



Sie können ein höheres Maß an hierarchische Struktur mithilfe des Parameters *SeniorityIndex* bereitstellen. Beim Erstellen einer eines hierarchischen Adressbuchs verwenden Sie *SeniorityIndex* Parameter Rank einzelne Empfänger oder organisatorische Gruppen von Unternehmen innerhalb dieser Organisationseinheiten Ebenen. Dieser Rangfolge gibt die Reihenfolge, in der die Empfänger oder Gruppen angezeigt werden, in das hierarchische Adressbuch. Im vorstehenden Beispiel wird der Parameter *SeniorityIndex* für Empfänger in der

Unternehmenszentrale Division beispielsweise wie folgt festgelegt:

- 100 für David Hamilton
- 50 für Rajesh M. Patel
- 25 für Amy Alberts

#### NOTE

Wenn der *SeniorityIndex*-Parameter nicht festgelegt oder gleich für zwei oder mehr Benutzer ist, verwendet die Sortierreihenfolge eines hierarchischen Adressbuchs den Wert des Parameters *PhoneticDisplayName* an die Benutzer alphabetisch sortierte Liste. Wenn der Wert des Parameters *PhoneticDisplayName* nicht festgelegt ist, wird die Sortierreihenfolge eines hierarchischen Adressbuchs wird standardmäßig auf den Wert des Parameters *DisplayName* und führt die Benutzer in alphabetischer Reihenfolge aufsteigender.

## Konfigurieren hierarchischer Adressbücher

Detaillierte Anweisung zum Erstellen hierarchischer Adressbücher finden Sie im Thema [Aktivieren oder Deaktivieren von hierarchischen Adressbüchern](#). Die allgemeinen Schritte sind wie folgt:

1. Erstellen Sie eine Verteilergruppe, die für die Stammorganisation (oberste Ebene) verwendet wird. Nach Wunsch können Sie eine in der Exchange-Gesamtstruktur vorhandene Organisationseinheit als Verteilergruppe verwenden.
2. Erstellen von Verteilergruppen für die enthält und diese zu kennzeichnen als Mitglieder von das hierarchische Adressbuch. Ändern des Parameters *SeniorityIndex* dieser Gruppen, damit sie in der ordnungsgemäßen hierarchischen Reihenfolge innerhalb der Stammorganisation aufgeführt werden.
3. Hinzufügen von Mitgliedern der Organisation. Ändern Sie den *SeniorityIndex*-Parameter der Member, damit sie in der ordnungsgemäßen hierarchischen Reihenfolge innerhalb der untergeordneten Ebenen aufgeführt werden.
4. Aus Gründen der Eingabehilfen können Sie den Parameter *PhoneticDisplayName* verwenden, der eine phonetische Aussprache des Parameters *DisplayName* angibt.

# Aktivieren oder Deaktivieren von hierarchischen Adressbüchern

18.12.2018 • 12 minutes to read

Sie können ein hierarchischen Adressbuchs (eines hierarchischen Adressbuchs), konfigurieren, das ein Feature für Endbenutzer in Microsoft Outlook 2010 oder höher verfügbar ist. Mit einer eines hierarchischen Adressbuchs können Benutzer mithilfe einer Organisationshierarchie basierend auf den Status des Mitarbeiters oder Managementstruktur für Empfänger in ihrer Exchange-Organisation suchen. Weitere Informationen zum HABs finden Sie unter [hierarchische Adressbücher](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 1 Stunde.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Verteilergruppen" im Thema [Recipients Permissions](#).
- Sie können nicht im Exchange Administrationscenter (EAC) verwenden Sie zum Ausführen dieses Verfahrens. Sie müssen Exchange Online PowerShell verwenden.
- Bevor Sie beginnen, lesen Sie das Thema [hierarchische Adressbücher](#). Sie sollten verstehen, ob ein hierarchischen Adressbuchs für Ihre Exchange-Organisation geeignet ist.
- Machen Sie sich mit der aktuellen Konfiguration von Organisationseinheiten, Gruppen, Benutzern und Kontakten in Ihrer Exchange-Organisation vertraut.
- Machen Sie sich mit den Cmdlets und den zugehörigen Parametern in der folgenden Tabelle vertraut, die zur Konfiguration eines hierarchischen Adressbuchs erforderlich sind.

CMDLET	PARAMETER
<a href="#">Set-OrganizationConfig</a>	<i>HierarchicalAddressBookRoot</i>
<a href="#">Set-Group</a>	<i>IsHierarchicalGroup</i> <i>SeniorityIndex</i> <i>PhoneticDisplayName</i>
<a href="#">Set-User</a>	<i>SeniorityIndex</i> <i>PhoneticDisplayName</i>
<a href="#">Set-Contact</a>	<i>SeniorityIndex</i> <i>PhoneticDisplayName</i>

- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Was möchten Sie tun?

## Verwenden von Exchange Online PowerShell Aktivieren eines hierarchischen Adressbuchs

### NOTE

Ein hierarchisches Adressbuch kann nicht mit der Exchange-Verwaltungskonsole aktiviert werden. Nach der Aktivierung des Adressbuchs kann die Exchange-Verwaltungskonsole aber dazu verwendet werden, die Mitgliedschaft der Gruppen in der Organisationshierarchie zu verwalten.

In diesem Beispiel wird eine OU mit dem Namen eines hierarchischen Adressbuchs erstellt für das hierarchische Adressbuch. Der Name der Domäne für die Organisation ist Contoso-Dom und Contoso, Ltd wird der Name der Organisation auf oberster Ebene in der Hierarchie (Stammorganisation) sein. Untergeordnete Gruppen mit dem Namen Unternehmenszentrale, Product Support Organization und Sales & Marketing Organization werden als untergeordnete Organisationen unter Contoso, Ltd. darüber, die Gruppen Personalabteilung, "Accounting Group" und Verwaltungsgruppe erstellt werden wird als untergeordnete Organisationen unter Unternehmenszentrale erstellt werden.

Ausführliche Informationen zum Erstellen von Verteilergruppen finden Sie unter [Erstellen und Verwalten von Verteilergruppen](#).

1. Erstellen einer Organisationseinheit "HAB" in der Organisation "Contoso". Sie können Active Directory-Benutzer und -Computer verwenden oder an einer Eingabeaufforderung den folgenden Befehl eingeben.

### NOTE

Alternativ können Sie eine vorhandene Organisationseinheit in Ihrer Exchange-Gesamtstruktur verwenden.

```
dsadd ou "OU=HAB,DC=Contoso-dom,DC=Contoso,DC=com"
```

```
> [ !NOTE ]
> <span data-ttu-id="ba819-147">Weitere Informationen finden Sie unter [Erstellen einer neuen
Organisationseinheit](https://go.microsoft.com/fwlink/?LinkId=198986).</span><span class="sxs-lookup"><span
data-stu-id="ba819-147">For details, see [Create a New Organizational Unit]
(https://go.microsoft.com/fwlink/?LinkId=198986).</span></span>
```

2. Erstellen der Stammverteilergruppe "Contoso,Ltd" für das hierarchische Adressbuch.

### NOTE

Ein Beispiel für Exchange Online PowerShell wird im Rahmen dieses Themas bereitgestellt. Jedoch können Sie die Exchange-Verwaltungskonsole verwenden, um eine Verteilergruppe zu erstellen. Weitere Informationen hierzu finden Sie unter [Erstellen und Verwalten von Verteilergruppen](#).

```
New-DistributionGroup -Name "Contoso,Ltd" -DisplayName "Contoso,Ltd" -Alias "ContosoRoot" -OrganizationalUnit
"Contoso-dom.Contoso.com/HAB" -SamAccountName "ContosoRoot" -Type "Distribution"
```

3. Festlegen von "Contoso,Ltd" als Stammorganisation für das hierarchische Adressbuch.

```
Set-OrganizationConfig -HierarchicalAddressBookRoot "Contoso,Ltd"
```

4. Erstellen von Verteilergruppen für die anderen Ebenen innerhalb des hierarchischen Adressbuchs. Für dieses Beispiel würden Sie die folgenden Gruppen erstellen: "Corporate Office", "Product Support Organization", "Sales & Marketing Organization", "Human Resources", "Accounting Group" und "Administration Group". In diesem Beispiel wird die Verteilergruppe "Corporate Office" erstellt.

**NOTE**

Ein Beispiel für Exchange Online PowerShell wird im Rahmen dieses Themas bereitgestellt. Sie können jedoch auch der Exchange-Verwaltungskonsole verwenden, zum Erstellen von Verteilergruppen. Weitere Informationen hierzu finden Sie unter [Erstellen und Verwalten von Verteilergruppen](#).

```
New-DistributionGroup -Name "Corporate Office" -DisplayName "Corporate Office" -Alias "CorporateOffice" -OrganizationalUnit "Contoso-dom.Contoso.com/HAB" -SamAccountName "CorporateOffice" -Type "Distribution"
```

5. Festlegen der einzelnen Gruppen als Mitglieder des hierarchischen Adressbuchs. Für dieses Beispiel würden die folgenden Gruppen als hierarchische Gruppen festgelegt: "Contoso,Ltd", "Corporate Office", "Product Support Organization", "Sales & Marketing Organization", "Human Resources", "Accounting Group" und "Administration Group". In diesem Beispiel wird die Verteilergruppe "Contoso,Ltd" als Mitglied des hierarchischen Adressbuchs festgelegt.

```
Set-Group -Identity "Contoso,Ltd" -IsHierarchicalGroup $true
```

6. Hinzufügen aller untergeordneten Gruppen als Mitglieder der Stammorganisation. In diesem Beispiel werden die Verteilergruppen "Corporate Office", "Product Support Organization" und "Sales & Marketing Organization" als Mitglieder der Stammorganisation "Contoso,Ltd" im hierarchischen Adressbuch hinzugefügt. In diesem Beispiel wird die Verteilergruppe "Corporate Office" als Mitglied der Stammverteilergruppe "Contoso,Ltd" hinzugefügt.

**NOTE**

In diesem Beispiel wird der Alias der Verteilergruppen verwendet.

```
Add-DistributionGroupMember -Identity "ContosoRoot" -Member "CorporateOffice"
```

7. Hinzufügen aller untergeordneten Gruppen der Verteilergruppe "Corporate Office" als Mitglieder dieser Gruppe. Für dieses Beispiel werden die Verteilergruppen "Human Resources", "Accounting Group" und "Administration Group" als Mitglieder der Verteilergruppe "Corporate Office" hinzugefügt. In diesem Beispiel wird die Verteilergruppe "Human Resources" als Mitglied der Verteilergruppe "Corporate Office" hinzugefügt.

**NOTE**

In diesem Beispiel wird der Alias der Verteilergruppen verwendet, und es wird davon ausgegangen, dass "HumanResources" der Alias der Verteilergruppe "Human Resources" ist.

```
Add-DistributionGroupMember -Identity "CorporateOffice" -Member "HumanResources"
```

8. Hinzufügen von Benutzern zu den Gruppen im hierarchischen Adressbuch. Für dieses Beispiel ist "David Hamilton" (SMTP-Adresse "DHamilton@contoso.com") ein vorhandener Benutzer in der Organisationseinheit

"Contoso-dom.Contoso.com/Users" und wird zur Gruppe "Corporate Office" hinzugefügt. Wiederholen Sie diesen Schritt, um andere Benutzer zu Gruppen im hierarchischen Adressbuch hinzuzufügen.

```
Add-DistributionGroupMember -Identity "CorporateOffice" -Member "DHamilton"
```

9. Legen Sie den Parameter *SeniorityIndex* für Gruppen in das hierarchische Adressbuch. In diesem Beispiel die Unternehmenszentrale-Gruppe enthält drei untergeordneten Gruppen: Personalabteilung, "Accounting Group" und der Gruppe Verwaltung. Anstelle der die Gruppen alphabetisch sortierte, wird der Standardwert der bevorzugten Sortierung werden Personalabteilung ( *SeniorityIndex* = 100), "Accounting Group" ( *SeniorityIndex* = 50), und klicken Sie dann Verwaltungsgruppe ( *\_SeniorityIndex\_* = 25). In diesem Beispiel wird der *SeniorityIndex* -Parameter für die Personalabteilung auf 100 festgelegt.

```
Set-Group -Identity "Human Resources" -SeniorityIndex 100
```

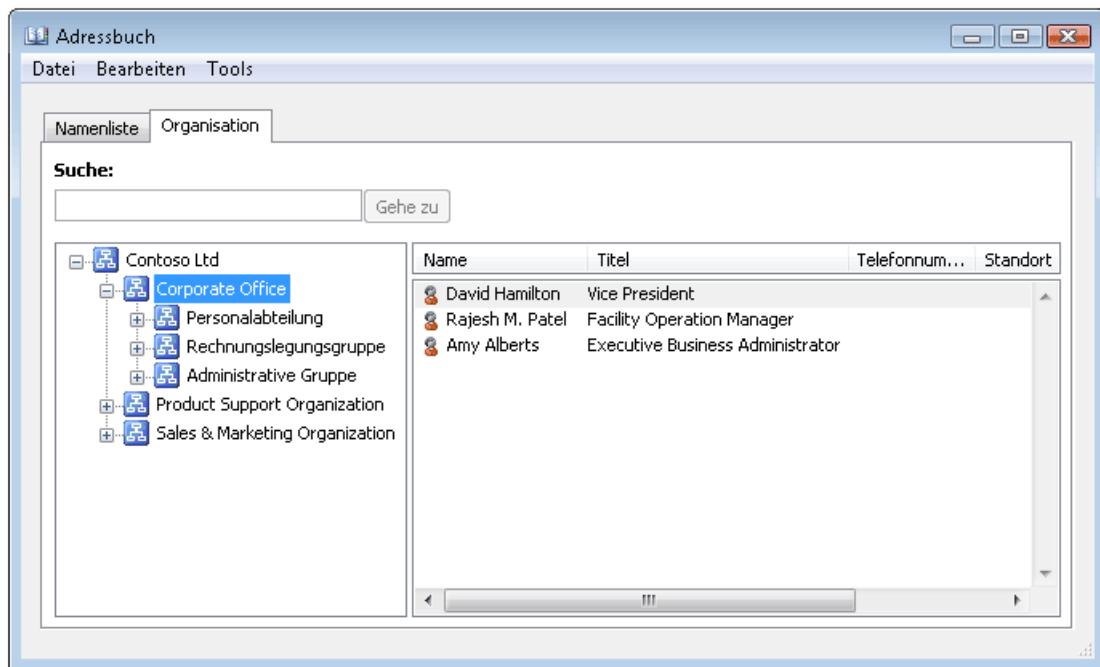
> [ !NOTE ]  
> <span data-ttu-id="ba819-p117">Der Parameter *\_SeniorityIndex\_* ist einen numerischen Wert zum Sortieren von Gruppen oder Benutzer in absteigender numerische Reihenfolge in eine hierarchische Adressbuch. Wenn der *\_SeniorityIndex\_* -Parameter nicht festgelegt oder gleich für zwei oder mehr Benutzer ist, verwendet die Sortierreihenfolge eines hierarchischen Adressbuchs den Wert des Parameters *\_PhoneticDisplayName\_* an die Benutzer alphabetisch sortierte Liste. Wenn der *\_PhoneticDisplayName\_* Wert nicht festgelegt ist, wird die Sortierreihenfolge eines hierarchischen Adressbuchs wird standardmäßig auf den Wert des Parameters *\_DisplayName\_* und führt die Benutzer in alphabetischer Reihenfolge aufsteigender.</span><span class="sxs-lookup"><span data-stu-id="ba819-p117">The *\_SeniorityIndex\_* parameter is a numerical value used to sort groups or users in descending numerical order in a HAB. If the *\_SeniorityIndex\_* parameter isn't set or is equal for two or more users, the HAB sorting order uses the *\_PhoneticDisplayName\_* parameter value to list the users in ascending alphabetical order. If the *\_PhoneticDisplayName\_* value isn't set, the HAB sorting order defaults to the *\_DisplayName\_* parameter value and lists the users in ascending alphabetical order.</span></span>

10. Festlegen Sie den Parameter *SeniorityIndex* für Benutzer in den Gruppen eines hierarchischen Adressbuchs. In diesem Beispiel die Unternehmenszentrale Gruppe enthält drei Benutzer: Amy Alberts und David Hamilton Rajesh M. Patel. Anstatt die Benutzer, die standardmäßig in aufsteigender alphabetischen Reihenfolge aufgeführt, die bevorzugte Sortierung werden David Hamilton ( *SeniorityIndex* = 100), Rajesh M. Patel ( *SeniorityIndex* = 50), und klicken Sie dann Amy Alberts ( *SeniorityIndex* = 25). In diesem Beispiel wird der *SeniorityIndex* -Parameter für den Benutzer David Hamilton auf 100 festgelegt.

```
Set-User -Identity "DHamilton@contoso.com" -SeniorityIndex 100
```

Nach dem Ausführen der vorangehenden Schritte ist das hierarchische Adressbuch in Outlook sichtbar. Öffnen Sie Outlook, und klicken Sie auf **Adressbuch**, um das hierarchische Adressbuchs anzuzeigen. Das hierarchische Adressbuch wird auf der Registerkarte **Organisation** angezeigt und entspricht in etwa der folgenden Abbildung.

#### **Beispiel eines hierarchischen Adressbuchs für "Contoso,Ltd"**



Nach dem Erstellen der eines hierarchischen Adressbuchs können Sie der Exchange-Verwaltungskonsole verwenden, um die Mitgliedschaft der Gruppen in der Organisationshierarchie zu verwalten. Allerdings müssen Sie Exchange Online PowerShell verwenden, um den Parameter *SeniorityIndex* für neue Gruppen oder Benutzer ändern.

Ausführliche Informationen zu Syntax und Parametern finden Sie in den folgenden Themen:

- [New-DistributionGroup](#)
- [Set-OrganizationConfig](#)
- [Set-Group](#)
- [Add-DistributionGroupMember](#)
- [Set-User](#)

#### Deaktivieren ein hierarchischen Adressbuchs mithilfe von Exchange Online PowerShell

In diesem Beispiel wird die für das hierarchische Adressbuch verwendete Stammorganisation deaktiviert.

```
Set-OrganizationConfig -HierarchicalAddressBookRoot $null
```

#### NOTE

Mit diesem Befehl wird die Stammorganisation nicht gelöscht oder untergeordneten Gruppen in der Struktur eines hierarchischen Adressbuchs verwendeten oder Zurücksetzen der *SeniorityIndex* Werte für Gruppen oder Benutzer. Es wird nur verhindert, dass die eines hierarchischen Adressbuchs in Outlook angezeigt wird. Zum Aktivieren der eines hierarchischen Adressbuchs mit denselben Konfigurationseinstellungen wieder müssen, Sie nur die Stammorganisation erneut aktivieren.

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-OrganizationConfig](#).

# Offlineadressbücher in Exchange Online

18.12.2018 • 3 minutes to read

Ein Offlineadressbuch (OAB) ist eine herunterladbare Adresse Liste-Auflistung, die Outlook-Benutzer zugreifen können, während Exchange Online getrennt. Administratoren können entscheiden, welche Adresslisten Benutzern zur Verfügung gestellt werden, die offline arbeiten.

Offlineadressbücher werden alle 8 Stunden generiert.

Weitere Informationen zu Adressen im Exchange Online sind, finden Sie unter [Address lists](#).

Vorgehensweisen mit OABs finden Sie unter [Verfahren für Offlineadressbücher](#).

Suchen Sie die Exchange Server-Version dieses Themas? Finden Sie unter [Offline Adressbücher in Exchange Server](#).

## Wie Benutzer offline-Adressbuch downloaden

1. Klicken Sie in Outlook auf **Datei > Kontoeinstellungen > Adressbuch downloaden**.
2. **Offline-Adressbuch** im Dialogfeld, das angezeigt wird, stellen Sie die folgende Auswahl:
  - **Herunterladen von Änderungen seit dem letzten senden/empfangen:** Standardmäßig ist dieses Kontrollkästchen aktiviert. Führt zu einem vollständigen Download des OAB Sie dieses Kontrollkästchen deaktivieren.
  - **Adressbuch auswählen:** in diesem Dropdown-Listenfeld zeigt die Offlineadressbücher, die Ihnen zur Verfügung stehen. Abhängig davon, was ein Administrator konfiguriert hat können Sie hier nur einen Wert (beispielsweise die globale Adressliste) finden Sie unter.
3. Klicken Sie auf **OK**. Das Offlineadressbuch heruntergeladen und auf Ihrem Computer gespeichert.

### Bedingungen, unter denen ein vollständiger Download des OAB angestoßen wird

Es gibt Situationen, in dem Outlook immer einen vollständigen OAB-Download ausführen. Zum Beispiel:

- Auf dem Clientcomputer keine OAB vorhanden ist (beispielsweise Dies ist der ersten Sie eine mit Ihrer Exchange Online-Postfachs in Outlook auf diesem Computer Verbindung haben).
- Die Version des OAB auf dem Server und dem Client stimmen nicht überein (eine aktuellere Version des OAB auf dem Server vorhanden ist).
- Eine oder mehrere OAB-Dateien sind auf dem Clientcomputer nicht vorhanden.
- Fehler bei ein vorherigen vollständiger Download und Outlook hat von vorne beginnen.
- Verfügt ein Benutzer über mehrere MAPI-Profilen auf demselben Outlook-Clientcomputer und wechselt er zwischen den beiden Profilen, die beide den Exchange-Cachemodus verwenden, finden mehrere vollständige Downloads derselben OAB-Dateien statt. Outlook unterstützt nur ein OAB pro Benutzerkonto auf einem Computer. Wenn Sie über mehrere Profile verfügen, kann nur ein Profil das OAB herunterladen. Wenn Sie mindestens zwei Profile verwenden müssen, die den Exchange-Cachemodus verwenden, müssen Sie eines der Profile so konfigurieren, dass es das OAB nicht herunterlädt.

# Verfahren für Offlineadressbücher

18.12.2018 • 2 minutes to read

[Erstellen eines Offlineadressbuchs](#)

[Hinzufügen einer Adressliste zu oder Entfernen einer Adressliste aus einem Offlineadressbuch](#)

[Ändern des Standard-Offlineadressbuchs](#)

[Zuordnen von Empfängern für Downloads von Offlineadressbüchern](#)

[Entfernen eines Offlineadressbuchs](#)

# Erstellen eines Offlineadressbuchs

18.12.2018 • 2 minutes to read

Ein Offlineadressbuch (OAB) ist eine herunterladbare Adresse Liste-Auflistung, die Outlook-Benutzer zugreifen können, während Exchange Online getrennt. Ein OAB ermöglicht Outlook-Benutzern Zugriff auf die Informationen in der angegebenen Adresslisten während getrennt von Exchange Online. Administratoren können entscheiden, welche Adresslisten Benutzern zur Verfügung gestellt werden, die offline arbeiten.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf OABs finden Sie unter [Verfahren für Offlineadressbücher](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Offlineadressbücher" im Thema [Email Address and Address Book Permissions](#).
- Standardmäßig wird die Adresslistenrolle in Exchange Online keiner Rollengruppe zugewiesen. Für die Verwendung von Cmdlets, die Adresslistenrolle benötigen, müssen Sie die Rolle einer Rollengruppe hinzufügen. Weitere Informationen finden Sie im Abschnitt „Hinzufügen einer Rolle zu einer Rollengruppe“ im Thema [Verwalten von Rollengruppen](#).
- Sie können nicht im Exchange Administrationscenter (EAC) verwenden Sie zum Ausführen dieses Verfahrens. Sie können nur Exchange Online PowerShell verwenden. Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell mit der webbasierten Verteilung ein OAB erstellen

Dieses Beispiel erstellt ein OAB namens OAB\_Contoso, die die globale Standardadressliste enthält.

```
New-OfflineAddressBook -Name "OAB_Contoso" -AddressLists "\Default Global Address List"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-OfflineAddressBook](#).

# Hinzufügen einer Adressliste an oder Entfernen einer Adressliste eines Offlineaddressbuchs in Exchange Online

18.12.2018 • 4 minutes to read

Exchange Online PowerShell können Sie hinzufügen oder Entfernen einer Adressliste eines Offlineaddressbuchs (OAB). Es wird standardmäßig ein OAB Namens der Standard-Offlineaddressbuch, die die globalen Adressliste (GAL) enthält. OABs werden basierend auf der Adresslisten, die darin enthaltenen generiert. Um benutzerdefinierte OABs erstellen, die Benutzer herunterladen können, können Sie hinzufügen oder Entfernen von Adresslisten aus OABs.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf OABs finden Sie unter [Verfahren für Offlineaddressbücher](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Offlineaddressbücher" im Thema [Mailbox Permissions](#) .
- Standardmäßig wird die Adresslistenrolle in Exchange Online keiner Rollengruppe zugewiesen. Für die Verwendung von Cmdlets, die Adresslistenrolle benötigen, müssen Sie die Rolle einer Rollengruppe hinzufügen. Weitere Informationen finden Sie im Abschnitt „Hinzufügen einer Rolle zu einer Rollengruppe“ im Thema [Verwalten von Rollengruppen](#).
- Änderungen an der Adressliste stehen erst für den Clientdownload zur Verfügung, nachdem das OAB, in dem die Adressliste gespeichert ist, generiert wurde.
- Sie können nicht im Exchange Administrationscenter (EAC) verwenden Sie zum Ausführen dieses Verfahrens. Sie können nur Exchange Online PowerShell verwenden. Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie die Exchange-Verwaltungsshell zum Hinzufügen und Entfernen von Adresslisten von Offlineaddressbüchern

Wenn Sie die Adresslisten, die in ein OAB konfiguriert sind ändern, enthält die Werte, die Sie angeben, wird *Ersetzen* einer beliebigen Adresse im Offlineaddressbuch. Um das OAB Adresslisten hinzuzufügen, geben Sie den aktuellen plus die Adresslisten, den Sie hinzufügen möchten. Um Adresslisten aus dem OAB zu entfernen, geben Sie den aktuellen minus diejenigen Adresslisten, den Sie entfernen möchten.

In diesem Beispiel wird das OAB namens Marketing OAB bereits mit Adresse Liste 1 und Liste 2 Adresse konfiguriert. Behält die Adresslisten und Hinzufügen von-Adresse Liste 3, den folgenden Befehl ausführen:

```
Set-OfflineAddressBook -Identity "Marketing OAB" -AddressLists "Address List1","Address List 2","Address List 3"
```

In ähnlicher Weise, um das OAB mit Adresse Liste 1 und 2 Adresse konfiguriert beibehalten und die Liste 3-Adresse zu entfernen, führen Sie den folgenden Befehl ein:

```
Set-OfflineAddressBook -Identity "Marketing OAB" -AddressLists "Address List 1","Address List 2"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-OfflineAddressBook](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie erfolgreich hinzugefügt oder aus einem OAB Adresslisten entfernt haben, führen Sie den folgenden Befehl zum Überprüfen der-Eigenschaft `AddressLists` Eigenschaftswerte:

```
Get-OfflineAddressBook | Format-List Name,AddressLists
```

# Ändern des Standard-Offlineaddressbuchs in Exchange Online

18.12.2018 • 3 minutes to read

Standardmäßig ist mit dem Namen Standard-Offlineaddressbuch automatisch erstellte OAB das Standard-OAB. Sie können eine beliebige OAB in Ihrer Exchange Online-Organisation als Standard-OAB festlegen. Das Standard-OAB wird von verwendet:

- Postfächer ohne Adresse Buch zugewiesene Richtlinie (ABP) oder, auf dem die zugewiesene Richtlinie ABP hat keine OAB definiert (standardmäßig keine Adressbuchrichtlinien vorhanden sind).
- Postfächer ohne ein OAB (standardmäßig alle Postfächer) zugewiesen.

Wenn Sie das Standard-OAB löschen, zuweisen nicht Exchange Online automatisch eine andere OAB als Standard. Sie müssen einen anderen OAB manuell als Standard festlegen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf OABs finden Sie unter [Verfahren für Offlineaddressbücher](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen dieses Verfahrens: 5 Minuten
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Offlineaddressbücher" im Thema [Mailbox Permissions](#) .
- Standardmäßig wird die Adresslistenrolle in Exchange Online keiner Rollengruppe zugewiesen. Für die Verwendung von Cmdlets, die Adresslistenrolle benötigen, müssen Sie die Rolle einer Rollengruppe hinzufügen. Weitere Informationen finden Sie im Abschnitt „Hinzufügen einer Rolle zu einer Rollengruppe“ im Thema [Verwalten von Rollengruppen](#).
- Sie können nicht im Exchange Administrationscenter (EAC) verwenden Sie zum Ausführen dieses Verfahrens. Sie können nur Exchange Online PowerShell verwenden. Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell so ändern Sie das Standard-OAB

In diesem Beispiel wird das Offlineaddressbuch "My OAB" als Standard-OAB festgelegt.

```
Set-OfflineAddressBook -Identity "My OAB" -IsDefault $true
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-OfflineAddressBook](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie das Standard-OAB erfolgreich geändert haben, führen Sie den folgenden Befehl zum Überprüfen der `IsDefault` Eigenschaftswert:

```
Get-OfflineAddressBook | Format-List Name,IsDefault
```

# Empfängern für Downloads von Offlineadressbuch-downloads in Exchange Online

18.12.2018 • 3 minutes to read

Wenn Sie mehrere Offlineadressbücher (OABs) in Ihrer Organisation verwenden, stehen Ihnen verschiedene Optionen für das OAB Benutzern zuordnen:

- **Pro Postfach:** können Sie das Cmdlet **Set-Mailbox** in Exchange Online PowerShell ein Postfach das OAB zugewiesen. Sie können auch eine gefilterte Liste der Postfächer das OAB zuweisen.
- **Pro adressbuchrichtlinie:** Sie können eine adressbuchrichtlinie (ABP) zu einem Benutzer zuweisen, und die ABP gibt das OAB. Wenn Sie eine ABP einem Benutzer, die bereits ein OAB mit ihrem Postfach zugewiesen ist zuweisen, wird das OAB, das dem Postfach zugeordnet ist, Vorrang. Weitere Informationen finden Sie unter [eine adressbuchrichtlinie an e-Mail-Benutzer zuweisen](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf OABs finden Sie unter [Verfahren für Offlineadressbücher](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie müssen finden Sie unter dem Abschnitt "Empfängerbereitstellungsberechtigungen" im Thema [Recipients Permissions](#) .
- Sie können nicht im Exchange Administrationscenter (EAC) verwenden Sie zum Ausführen dieses Verfahrens. Sie können nur Exchange Online PowerShell verwenden. Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell Postfächer OABs zuweisen

Wenn ein OAB an ein Postfach zuweisen möchten, verwenden Sie die folgende Syntax:

```
Set-Mailbox -Identity <MailboxIdentity> -OfflineAddressBook <OfflineAddressBookIdentity>
```

In diesem Beispiel wird das OAB namens "Contoso Executives" auf das Postfach laura@contoso.com.

```
Set-Mailbox -Identity laura@contoso.com -OfflineAddressBook "Contoso Executives OAB"
```

In diesem Beispiel wird das OAB namens Contoso US zu einer gefilterten Liste von Postfächern. Dieser ersten Befehl gibt die Postfächer. Der zweite Befehl weist das OAB an die identifizierten Postfächer.

```
$USContoso = Get-User -ResultSize Unlimited -Filter {RecipientType -eq "UserMailbox" -and Company -eq "Contoso" -and CountryOrRegion -eq "US"}  
$USContoso | foreach {Set-Mailbox $_.Identity -OfflineAddressBook "Contoso United States"}
```

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Ersetzen Sie zum bestätigen, dass Sie ein Postfach erfolgreich ein OAB zugewiesen haben, mit der Identität des Postfachs und führen Sie folgenden Befehl:

```
Get-Mailbox -Identity "<MailboxIdentity>" | Format-Table -Auto Name,OfflineAddressBook
```

# Entfernen eines Offlineaddressbuchs

18.12.2018 • 2 minutes to read

In diesem Thema wird erläutert, wie ein Offlineaddressbuch (OAB) von Exchange Online zu entfernen. Wenn Sie das Standard-OAB entfernen, müssen Sie einen anderen OAB als Standard-OAB zuweisen. Informationen dazu, wie das Standard-OAB zu ändern finden Sie unter [ändern das Standard-Offlineaddressbuch](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf OABs finden Sie unter [Verfahren für Offlineaddressbücher](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Offlineaddressbücher" im Thema [Email Address and Address Book Permissions](#).
- Standardmäßig wird die Adresslistenrolle in Exchange Online keiner Rollengruppe zugewiesen. Für die Verwendung von Cmdlets, die Adresslistenrolle benötigen, müssen Sie die Rolle einer Rollengruppe hinzufügen. Weitere Informationen finden Sie im Abschnitt „Hinzufügen einer Rolle zu einer Rollengruppe“ im Thema [Verwalten von Rollengruppen](#).
- Sie können nicht im Exchange Administrationscenter (EAC) verwenden Sie zum Ausführen dieses Verfahrens. Sie können nur Exchange Online PowerShell verwenden. Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um ein OAB zu entfernen.

In diesem Beispiel wird das Offlineaddressbuch "My OAB" entfernt.

```
Remove-OfflineAddressBook -Identity "My OAB"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Remove-OfflineAddressBook](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie das OAB erfolgreich entfernt haben, führen Sie den folgenden Befehl aus, um sicherzustellen, dass das OAB gelöscht wurde.

```
Get-OfflineAddressBook
```

# Freigabe in Exchange Online

18.12.2018 • 2 minutes to read

Möglicherweise müssen Sie Zeitpläne mit Personen in unterschiedlichen Organisationen oder mit Freunden und Familienmitgliedern koordinieren, so dass Sie gemeinsam an Projekten arbeiten oder gesellschaftliche Veranstaltungen planen können. Mit Office 365 können Administratoren verschiedene Ebenen für den Zugriff auf Kalender in Exchange Online einrichten, damit Unternehmen mit anderen Unternehmen zusammenarbeiten und Benutzer ihre Zeitpläne für andere Personen freigeben können. Die unternehmensübergreifende Kalenderfreigabe wird durch die Erstellung von Organisationsbeziehungen eingerichtet. Die benutzerübergreifende Kalenderfreigabe wird durch die Anwendung von Freigaberichtlinien eingerichtet.

## Freigabeszenarien in Exchange Online

Die folgenden Freigabeszenarien werden in Exchange Online unterstützt:

FREIGABEZIEL	ZU VERWENDENDE EINSTELLUNG	ANFORDERUNGEN
Kalenderfreigabe für eine andere Office 365-Organisation	Organisationsbeziehungen	Keine, konfigurieren
Kalenderfreigabe für eine lokale Exchange-Organisation	Organisationsbeziehungen	Der lokale Exchange-Administrator muss eine Authentifizierungsbeziehung zur Cloud einrichten (auch bekannt als "Verbund") und Mindestsoftwareanforderungen erfüllen
Freigabe des Kalenders eines Office 365-Benutzers für einen anderen Internet-Benutzer	Freigaberichtlinien	Keine, konfigurieren
Freigabe des Kalenders eines Office 365-Benutzers für einen lokalen Exchange-Benutzer	Freigaberichtlinien	Der lokale Exchange-Administrator muss eine Authentifizierungsbeziehung zur Cloud einrichten (auch bekannt als "Verbund") und Mindestsoftwareanforderungen erfüllen

## Dokumentation zur Freigabe

In der folgenden Tabelle sind Links zu Themen enthalten, in denen Sie weitere Informationen zur Freigabe in Exchange Online sowie zur Verwaltung dieser Funktionen finden.

THEMA	BESCHREIBUNG
<a href="#">Organisationsbeziehungen in Exchange Online</a>	Erfahren Sie mehr über 1:1-Beziehungen zwischen Organisationen, die eine Freigabe von Frei/Gebucht-Informationen ermöglichen.
<a href="#">Freigaberichtlinien in Exchange Online</a>	Erfahren Sie mehr über personenbezogene Richtlinien, die eine Freigabe von Kalendern ermöglichen.

# Organisationsbeziehungen in Exchange Online

18.12.2018 • 3 minutes to read

Richten Sie eine Organisationsbeziehung ein, um Kalenderinformationen für externe Geschäftspartner freizugeben. Office 365-Administratoren können eine Organisationsbeziehung mit einer Office 365-Organisation oder einer anderen lokalen Exchange-Organisation einrichten. Wenn Sie Kalender für eine lokale Exchange-Organisation freigeben möchten, muss der Administrator der lokalen Exchange-Organisation eine Authentifizierungsbeziehung mit der Cloud (auch "Verbund" genannt) einrichten und die Mindestsoftwareanforderungen erfüllen.

Eine Organisationsbeziehung ist eine 1:1-Beziehung zwischen Unternehmen, die es den Benutzern in beiden Organisationen ermöglichen soll, die Verfügbarkeitsinformationen im Kalender anzuzeigen. Beim Einrichten einer Organisationsbeziehung konfigurieren Sie Ihre Seite der Beziehung, und legen Sie fest, welche Art von Informationen die Benutzer der externen Organisation anzeigen können. Die externe Organisation kann dieselben oder andere Einstellungen auf ihrer Seite konfigurieren. Wenn beispielsweise Contoso eine Organisationsbeziehung mit Tailspin Toys erstellt, können die Benutzer bei Tailspin Toys Besprechungen mit den Benutzern bei Contoso planen, indem sie ihre E-Mail-Adressen der Besprechungseinladung hinzufügen. Die Verfügbarkeit der eingeladenen Contoso-Benutzer wird dann für die Tailspin Toys-Benutzer angezeigt. Allerdings können die Benutzer bei Contoso die Verfügbarkeit der Benutzer bei Tailspin Toys erst sehen, nachdem deren Administrator eine Organisationsbeziehung mit Contoso eingerichtet hat.

Sie können drei Zugriffsebenen festlegen:

- Kein Zugriff
- Zugriff auf Frei/Gebucht-Kalenderinformationen nur mit Zeit
- Frei/Gebucht-Zugriff mit Zeit plus Betreff und Ort

## NOTE

Wenn Benutzer die eigenen Frei/Gebucht-Informationen nicht für andere Benutzer freigeben möchten, können sie in Outlook den Berechtigungseintrag "Standard" ändern. Dazu müssen sie zur Registerkarte **Kalendereigenschaften > Berechtigungen** wechseln, die Berechtigung **Standard** auswählen und dann in der Liste **Berechtigungsstufe** die Option **Keine** auswählen. Selbst wenn eine Organisationsbeziehung besteht, sind die entsprechenden Frei/Gebucht-Informationen dann weder für interne noch für externe Benutzer sichtbar. Die vom Benutzer festgelegten Berechtigungen gelten.

In den folgenden Themen finden Sie Informationen zum Konfigurieren und Verwalten von Organisationsbeziehungen:

[Erstellen einer Organisationsbeziehung in Exchange Online](#)

[Ändern einer organisationsbeziehung in Exchange Online](#)

[Entfernen einer organisationsbeziehung in Exchange Online](#)

# Erstellen einer Organisationsbeziehung in Exchange Online

18.12.2018 • 5 minutes to read

Richten Sie eine Organisationsbeziehung ein, um Kalenderinformationen für einen externen Geschäftspartner freizugeben. Office 365-Administratoren können eine Organisationsbeziehung mit einer anderen Office 365-Organisation oder mit einer lokalen Exchange-Organisation einrichten.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 15 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter Thema [Berechtigungen in Exchange Online](#).
- Wenn Sie Kalender für eine lokale Exchange-Organisation freigeben möchten, muss der lokale Exchange-Administrator eine Authentifizierungsbeziehung mit der Cloud (auch „Verbund“ genannt) einrichten, und es müssen die Mindestsoftwareanforderungen erfüllt sein.

## Verwenden Sie die Exchange-Verwaltungskonsole, um eine Organisationsbeziehung zu erstellen

1. Gehen Sie vom Dashboard der Office 365-Verwaltungskonsole zu **Administrator > Exchange**.
2. Gehen Sie zu **Organisation > Freigabe**.
3. Klicken Sie unter **Organisationsfreigabe** auf **neu** 
4. Geben Sie im Bereich **Neue Organisationsbeziehung** im Feld **Beziehungsname** einen Anzeigenamen für die Organisationsbeziehung ein.
5. Geben Sie im Feld **Domäne für Freigabe** die Domäne für die externe Office 365- oder lokale Exchange-Organisation ein, die Einsicht in die Kalender haben soll. Wenn Sie mehr als eine Domäne eingeben müssen, trennen Sie die Domänennamen mit einem Komma. Beispiel: contoso.com, service.contoso.com.
6. Aktivieren Sie das Kontrollkästchen **Freigabe von Frei/Gebucht-Kalenderinformationen aktivieren**, um die Kalenderfreigabe mit den angegebenen Domänen zu ermöglichen. Legen Sie die Freigabeebene für Frei/Gebucht-Kalenderinformationen fest und definieren Sie, welche Benutzer Frei/Gebucht-Kalenderinformationen freigeben können.

Wählen Sie eine der folgenden Optionen zur Festlegung der Frei/Gebucht-Zugriffsebene:

- **Frei/Gebucht-Kalenderinformationen nur mit Zeit**
- **Frei/Gebucht-Kalenderinformationen mit Zeit, Betreff und Ort**

Um festzulegen, welche Benutzer die Frei/Gebucht-Kalenderinformationen freigeben können, wählen Sie eine der folgenden Optionen aus:

- **Jeder in Ihrem Unternehmen**
- **Eine bestimmte Sicherheitsgruppe**

Klicken Sie auf **Durchsuchen**, um eine Sicherheitsgruppe aus der Liste auszuwählen, und klicken Sie dann auf **OK**.

7. Klicken Sie auf **Speichern**, um die Organisationsbeziehung zu erstellen.

## Erstellen einer organisationsbeziehung mithilfe von Exchange Online PowerShell

In diesem Beispiel wird eine Organisationsbeziehung mit Contoso, Ltd. erstellt, die folgende Bedingungen erfüllt:

- Die Organisationsbeziehung wird für contoso.com, northamerica.contoso.com und europe.contoso.com aktiviert.
- Frei/Gebucht-Zugriff ist aktiviert.
- Contoso.com und die Unterdomänen erhalten Frei-/Gebucht-Zeit, Betreff und Standortinformation von Ihrer Organisation.

```
New-OrganizationRelationship -Name "Contoso" -DomainNames  
"contoso.com", "northamerica.contoso.com", "europe.contoso.com" -FreeBusyAccessEnabled $true -  
FreeBusyAccessLevel LimitedDetails
```

Wenn Sie unsicher sind, welche Domänen Contoso für die cloudbasierte Authentifizierung festgelegt hat, können Sie diesen Befehl ausführen, um automatisch die Konfigurationsinformationen zu erhalten. Das Cmdlet **Get-FederationInformation** wird verwendet, um die richtigen Informationen zu finden, die dann zum Cmdlet **New-OrganizationRelationship** weitergegeben werden.

```
Get-FederationInformation -DomainName Contoso.com | New-OrganizationRelationship -Name "Contoso" -  
FreeBusyAccessEnabled $true -FreeBusyAccessLevel LimitedDetails
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-FederationInformation](#) und [New-OrganizationRelationship](#).

Wenn Sie eine Organisationsbeziehung mit einer lokalen Exchange-Organisation einrichten, möchten Sie möglicherweise die Verbindungseinstellungen angeben. In diesem Beispiel wird eine Organisationsbeziehung mit Fourth Coffee erstellt und die zu verwendenden Verbindungseinstellungen definiert. Dabei gelten folgenden Bedingungen:

- Die Organisationsbeziehung wird mit der Domäne fourthcoffee.com hergestellt.
- Die Anwendungs-URL für die Exchange-Webdienste lautet "mail.fourthcoffee.com".
- Die AutoErmittlungs-URL ist "https://mail.fourthcoffee.com/autodiscover/autodiscover.svc/wssecurity".
- Frei/Gebucht-Zugriff ist aktiviert.
- Fourth Coffee sieht die Frei/Gebucht-Informationen mit der Zeit.

```
New-OrganizationRelationship -Name "Fourth Coffee" -DomainNames "fourthcoffee.com" -FreeBusyAccessEnabled  
$true -FreeBusyAccessLevel -AvailabilityOnly -TargetAutodiscoverEpr  
"https://mail.fourthcoffee.com/autodiscover/autodiscover.svc/wssecurity" -TargetApplicationUri  
"mail.fourthcoffee.com"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-OrganizationRelationship](#).

Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Der erfolgreiche Abschluss des Assistenten für **Neue Organisationsbeziehungen** weist darauf hin, dass die Organisationsbeziehung erstellt wurde.

Sie können auch den folgenden Befehl zum Überprüfen der organisationsbeziehung ausführen:

```
Get-OrganizationRelationship | format-list
```

**TIP**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Ändern einer Organisationsbeziehung in Exchange Online

18.12.2018 • 5 minutes to read

Mithilfe einer Organisationsbeziehung können Benutzer in Ihrer Office 365-Organisation Frei/Gebucht-Kalenderinformationen für andere Office 365- oder lokale Exchange-Organisationen freigeben. Sie können die Einstellungen einer Organisationsbeziehung ändern. Beispielsweise kann der Name der Organisationsbeziehung geändert, die Freigabe von Frei/Gebucht-Kalenderinformationen temporär deaktiviert, die Zugriffsebene für Frei/Gebucht-Informationen oder die Aktivierung von Sicherheitsgruppen in Ihrer Organisation für die Freigabe von Frei/Gebucht-Kalenderinformationen geändert werden.

Weitere Informationen zu organisationsbeziehungen finden Sie unter [Organization Relationships in Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 15 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter Thema [Berechtigungen in Exchange Online](#).
- Wenn Sie Kalender für eine lokale Exchange-Organisation freigeben möchten, muss der lokale Exchange-Administrator eine Authentifizierungsbeziehung mit der Cloud (auch „Verbund“ genannt) einrichten, und es müssen die Mindestsoftwareanforderungen erfüllt sein.
- Mit den Verfahren in diesem Thema wird die Organisationsbeziehung namens "Contoso" geändert: Die Beispiele zeigen, wie folgende Aufgaben ausgeführt werden:
  - Hinzufügen einer Domäne namens "service.contoso.com" zur Organisationsbeziehung.
  - Deaktivieren der Freigabe der Frei/Gebucht-Informationen für die Organisationsbeziehung.
  - Ändern Sie die Frei/Gebucht-Zugriffsebene von *Frei/Gebucht-Kalenderinformationen mit Zeit, Betreff und Ort* in *Frei/Gebucht-Kalenderinformationen nur mit Zeit*.

## Hinzufügen einer Domäne zur Organisationsbeziehung mithilfe der Exchange-Verwaltungskonsole

1. Wechseln Sie im Office 365 Admin Center zu **Admin > Exchange**.
2. Wechseln Sie zu **Organisation > Freigabe**.
3. In der Listenansicht unter **Organisationsfreigabe**, wählen Sie die organisationsbeziehung "Contoso" aus, und klicken Sie dann auf **Bearbeiten**
4. **Organisationsbeziehung ändern Allgemein** nicht den **Namen** für die organisationsbeziehung.
5. Geben Sie im Feld **Domänen für Freigabe** die Domäne service.contoso.com ein, und klicken Sie auf **Add**
6. Klicken Sie auf **Speichern**, um die Organisationsbeziehung zu aktualisieren.

# Deaktivieren des Zugriffs auf Frei/Gebucht-Informationen für die Organisationsbeziehung mithilfe der Exchange-Verwaltungskonsole

1. Wechseln Sie im Office 365 Admin Center zu **Admin > Exchange**.
2. Wechseln Sie zu **Organisation > Freigabe**.
3. In der Listenansicht unter **Organisationsfreigabe**, wählen Sie die organisationsbeziehung "Contoso" aus, und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie in **organisationsbeziehung** auf **Freigabe**.
5. Deaktivieren Sie das Kontrollkästchen **Freigabe von Frei/Gebucht-Kalenderinformationen aktivieren**, um die Freigabe von Frei/Gebucht-Informationen zu deaktivieren. Die Schaltflächen für die Frei/Gebucht-Zugriffsebene und die Sicherheitsgruppen werden ebenfalls deaktiviert.
6. Klicken Sie auf **Speichern**, um die Organisationsbeziehung zu aktualisieren.

# Ändern der Zugriffsebene für Frei/Gebucht-Informationen für die Organisationsbeziehung mithilfe der Exchange-Verwaltungskonsole

1. Wechseln Sie im Office 365 Admin Center zu **Admin > Exchange**.
2. Wechseln Sie zu **Organisation > Freigabe**.
3. In der Listenansicht unter **Organisationsfreigabe**, wählen Sie die organisationsbeziehung "Contoso" aus, und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie in **organisationsbeziehung** auf **Freigabe**.
5. Wählen Sie **Frei/Gebucht-Kalenderinformationen nur mit Zeit** aus.
6. Klicken Sie auf **Speichern**, um die Organisationsbeziehung zu aktualisieren.

# Verwenden Sie Exchange Online PowerShell, um die organisationsbeziehung zu ändern.

- In diesem Beispiel wird der Organisationsbeziehung "Contoso" der Domänenname "service.contoso.com" hinzugefügt.

```
$domains = (Get-OrganizationRelationship Contoso).DomainNames
$domains += 'service.contoso.com'
Set-OrganizationRelationship -Identity Contoso -DomainNames $domains
```

- In diesem Beispiel wird die Organisationsbeziehung "Contoso" deaktiviert.

```
Set-OrganizationRelationship -Identity Contoso -Enabled $false
```

- Dieses Beispiel ermöglicht Zugriff auf Verfügbarkeitsinformationen für die organisationsbeziehung "woodgrovebank" ermöglicht und legt den Zugriff auf **AvailabilityOnly** (calendar Frei/Gebucht-Kalenderinformationen nur mit Zeit).

```
Set-OrganizationRelationship -Identity Contoso -FreeBusyAccessEnabled $true -FreeBusyAccessLevel
AvailabilityOnly
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-OrganizationRelationship](#) und [Set-OrganizationRelationship](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie die organisationsbeziehung erfolgreich aktualisiert haben, führen Sie den folgenden Befehl aus, und überprüfen Sie die Informationen zur Beziehung.

```
Get-OrganizationRelationship | format-list
```

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Entfernen einer organisationsbeziehung in Exchange Online

18.12.2018 • 2 minutes to read

Mithilfe der Organisationsbeziehung können Benutzer in der Office 365-Organisation Frei/Gebucht-Kalenderinformationen mit anderen Office 365- oder lokalen Exchange-Organisationen gemeinsam nutzen. Sie können eine Organisationsbeziehung entfernen, um die Kalenderfreigabe für die andere Organisation zu deaktivieren.

Weitere Informationen zu organisationsbeziehungen finden Sie unter [Organization Relationships in Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter Thema [Berechtigungen in Exchange Online](#).

## Verwenden der Exchange-Verwaltungskonsole zum Entfernen einer Organisationsbeziehung

1. Wechseln Sie im Office 365 Admin Center zu **Admin > Exchange**.
2. Wechseln Sie zu **Organisation > Freigabe**.
3. Unter **Organisationsfreigabe**, wählen Sie eine organisationsbeziehung aus, und klicken Sie dann auf **Löschen**.
4. Klicken Sie in der Warnung, die angezeigt wird, auf **Ja**.

## Entfernen einer organisationsbeziehung mithilfe von Exchange Online PowerShell

In diesem Beispiel wird die Organisationsbeziehung "Contoso" entfernt.

```
Remove-OrganizationRelationship -Identity "Contoso"
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Remove-OrganizationRelationship](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie eine der folgenden Aktionen aus, um zu überprüfen, dass Sie die Organisationsbeziehung erfolgreich entfernt haben:

- Wechseln Sie in der Exchange-Verwaltungskonsole zu **Organisation > Freigabe** und stellen Sie sicher, dass die organisationsbeziehung in der Listenansicht unter **Organisationsfreigabenicht** angezeigt.
- Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die organisationsbeziehung entfernt wurde.

```
Get-OrganizationRelationship | Format-List
```

**TIP**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Freigaberichtlinien in Exchange Online

18.12.2018 • 2 minutes to read

Mitglieder Ihrer Organisation möchten möglicherweise Kalender an einzelne Geschäftskontakte, Freunde oder Familienmitglieder freigeben. Freigaberichtlinien steuern, wie Benutzer ihre Kalender mit Benutzern außerhalb Ihrer Organisation gemeinsam nutzen können. Die Freigaberichtlinie, die ein Administrator auf das Postfach eines Benutzers anwendet, bestimmt, welche Zugriffsebene ein Benutzer an wen freigeben kann. Wenn Sie nichts ändern, können alle Benutzer jede beliebige Person mit einer E-Mail-Adresse einladen, den Kalender anzusehen. Sie können bei Bedarf eine restriktivere Richtlinie anwenden.

Ein Administrator legt die Regeln fest, aus denen sich die Freigaberichtlinie zusammensetzt. Sie können die Domänen angeben, an die Benutzer Freigaben durchführen können, sowie folgende Zugriffsebenen auf Kalender:

- Frei/Gebucht-Kalenderinformationen nur mit Zeit
- Frei/Gebucht-Kalenderinformationen mit Zeit, Betreff und Ort
- Frei/Gebucht-Informationen, einschließlich Uhrzeit, Betreff, Ort und Titel

Nachdem Sie eine neue Freigaberichtlinie erstellt haben, müssen Sie diese Richtlinie auf die Postfächer anwenden, bevor sie wirksam wird. Freigaberichtlinien gelten für einzelne Benutzerpostfächer. Ein Administrator kann zudem die Freigaberichtlinie eines Benutzers deaktivieren, um den externen Zugriff auf Kalender zu verhindern.

Benutzer geben ihre Kalender frei, indem sie eine E-Mail-Einladung an den externen Benutzer versenden. Diese Art von Einladung kann in Outlook 2010 oder neuer oder Outlook Web App versendet werden. Der Kalender kann über eine URL geöffnet werden oder als zusätzlicher Kalenderordner verwendet werden, wenn der externe Benutzer Outlook 2010 oder neuer hat oder Outlook Web App verwendet.

In diesen Themen wird erklärt, wie Sie Freigaberichtlinien für Ihre Office 365-Organisation verwalten:

[Erstellen einer Freigaberichtlinie in Exchange Online](#)

[Anwenden von Freigaberichtlinien auf Postfächer in Exchange Online](#)

[Ändern, deaktivieren oder Entfernen einer Freigaberichtlinie in Exchange Online](#)

# Erstellen einer Freigaberichtlinie in Exchange Online

18.12.2018 • 5 minutes to read

Erstellen einer neuen Freigaberichtlinie um wie Personen in Ihrer Organisation freigeben mit einzelne Geschäftspartner, Freunde und Familienmitglieder Kalender zu ändern. Freigaberichtlinien steuern, wie die Benutzer ihre Kalender für Personen außerhalb Ihrer Organisation freigeben. Standardmäßig können alle Benutzer alle Benutzer mit einer e-Mail-Adresse zum Anzeigen des Kalenders einladen. Nachdem Sie eine neue Freigaberichtlinie zu erstellen, müssen Sie diese Richtlinie auf Postfächer angewendet werden, bevor sie wirksam wird. Um eine bestimmte Freigaberichtlinie für Benutzer gelten, finden Sie unter [Anwenden von Freigaberichtlinien auf Postfächer in Exchange Online](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 15 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter Thema [Berechtigungen in Exchange Online](#).
- Nur Benutzer von Outlook 2010 oder höher und Outlook Web App können Einladungen zur Freigabe erstellen.

## Erstellen einer Freigaberichtlinie mithilfe des Assistenten

1. Gehen Sie vom Dashboard der Office 365-Verwaltungskonsole zu **Administrator > Exchange**.
2. Gehen Sie zu **Organisation > Freigabe**.
3. Klicken Sie in der Listenansicht unter **Einzelne Freigabe**, auf neu
4. Geben Sie unter **Neue Freigaberichtlinie** einen Anzeigenamen für die Freigaberichtlinie im Feld **Richtlinienname** ein.
5. Klicken Sie auf **Hinzufügen**  um die freigaberegeln für die Richtlinie zu definieren.
6. Wählen Sie im Dialogfeld **Freigaberegel** eine der folgenden Optionen aus, um die Domänen für die Freigabe anzugeben:
  - **Freigabe für alle Domänen**
  - **Freigabe für eine bestimmte Domäne**
7. Wenn Sie **Freigabe für eine bestimmte Domäne** auswählen, geben Sie die Domäne für die Freigabe ein. Wenn Sie mehr als eine Domäne für diese Freigaberichtlinie eingeben müssen, speichern Sie zunächst die Einstellungen für die erste Domäne. Bearbeiten Sie anschließend die Freigaberegeln, um weitere Domänen hinzuzufügen.
8. Zum Angeben der freizugebenden Informationen aktivieren Sie das Kontrollkästchen **Ihre Kalenderordner freigeben**. Wählen Sie anschließend eine der folgenden Optionen aus:
  - **Frei/Gebucht-Kalenderinformationen nur mit Zeit**
  - **Frei/Gebucht-Kalenderinformationen mit Zeit, Betreff und Ort**

- Alle Informationen zum Termin einschließlich Uhrzeit, Betreff, Ort und Titel

9. Klicken Sie auf **Speichern**, um die Regeln für die Freigaberichtlinie festzulegen.
10. Wenn Sie diese Freigaberichtlinie als die neue Standardfreigaberichtlinie für alle Benutzer in Ihrer Office 365-Organisation festlegen möchten, aktivieren Sie das Kontrollkästchen **Diese Richtlinie als meine Standardfreigaberichtlinie verwenden**.
11. Klicken Sie auf **Speichern**, um die Freigaberichtlinie zu erstellen.

## Verwenden von Exchange Online PowerShell zum Erstellen einer Freigaberichtlinie

- In diesem Beispiel wird die Freigaberichtlinie "Contoso" erstellt. Mithilfe dieser Richtlinie können Benutzer in der Domäne "contoso.com" detaillierte Verfügbarkeitsinformationen aus Kalendern (Frei/Gebucht-Informationen) Ihrer Benutzer anzeigen. Diese Richtlinie ist standardmäßig aktiviert.

```
New-SharingPolicy -Name "Contoso" -Domains contoso.com: CalendarSharingFreeBusyDetail
```

- In diesem Beispiel wird die Freigaberichtlinie "ContosoWoodgrove" für zwei verschiedene Domänen ("contoso.com" und "woodgrovebank.com") mit unterschiedlichen Freigabeeinstellungen für jede Domäne konfiguriert. Die Richtlinie wird deaktiviert.

```
New-SharingPolicy -Name "ContosoWoodgrove" -Domains 'contoso.com: CalendarSharingFreeBusySimple', 'woodgrovebank.com: CalendarSharingFreeBusyDetail' -Enabled $false
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-SharingPolicy](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie die Freigaberichtlinie erfolgreich erstellt haben, führen Sie den folgenden Befehl zum Anzeigen der Informationen zur Freigaberichtlinie.

```
Get-SharingPolicy <policy name> | format-list
```

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Anwenden von Freigaberichtlinien auf Postfächer in Exchange Online

18.12.2018 • 5 minutes to read

Freigaberichtlinien steuern, wie Benutzer ihre Kalender mit Benutzern außerhalb Ihrer Organisation gemeinsam nutzen können. Die Freigaberichtlinie, die ein Administrator auf das Postfach eines Benutzers anwendet, bestimmt, welche Zugriffsebene ein Benutzer an wen freigeben kann. Wenn Sie nichts ändern, können alle Benutzer jede beliebige Person mit einer E-Mail-Adresse einladen, den Kalender anzusehen. Wenn Sie eine neue Freigaberichtlinie erstellen, müssen Sie diese Richtlinie auf die Postfächer anwenden, bevor sie wirksam wird. Freigaberichtlinien gelten für einzelne Benutzerpostfächer. Ein Administrator kann zudem die Freigaberichtlinie eines Benutzers deaktivieren, um den externen Zugriff auf Kalender zu verhindern.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter Thema [Berechtigungen in Exchange Online](#).
- Eine Freigaberichtlinie muss vorhanden sein. Weitere Informationen hierzu finden Sie unter [erstellen eine Freigaberichtlinie in Exchange Online](#).

## Verwenden Sie die Exchange-Verwaltungskonsole, um eine Freigaberichtlinie auf ein Postfach anzuwenden

1. Gehen Sie vom Dashboard der Office 365-Verwaltungskonsole zu **Administrator > Exchange**.
2. Gehen Sie zu **Empfänger > Postfächer**.
3. In der Listenansicht, wählen Sie das gewünschte Postfach aus, und klicken Sie dann auf **Bearbeiten**  

4. Klicken Sie in **Benutzerpostfach** auf **Postfachfunktionen**.
5. Wählen Sie in der Liste **Freigaberichtlinie** die Freigaberichtlinie aus, die Sie auf dieses Postfach anwenden möchten.
6. Klicken Sie auf **Speichern**, um die Freigaberichtlinie anzuwenden.

## Verwenden Sie die Exchange-Verwaltungskonsole, um eine Freigaberichtlinie auf mehrere Postfächer anzuwenden

1. Gehen Sie vom Dashboard der Office 365-Verwaltungskonsole zu **Administrator > Exchange**.
2. Gehen Sie zu **Empfänger > Postfächer**.
3. Halten Sie in der Listenansicht die STRG-TASTE gedrückt, um mehrere Postfächer auszuwählen.
4. Im Detailbereich werden die Postfacheigenschaften für die Massenbearbeitung konfiguriert. Führen Sie einen Bildlauf nach unten durch, und klicken Sie auf **Weitere Optionen**.

5. Klicken Sie unter **Freigaberichtlinie** auf **Aktualisieren**.
6. Wählen Sie in **Massenzuweisung von Freigaberichtlinie die Freigaberichtlinie** aus der Liste aus.
7. Klicken Sie auf **Speichern**, um die Freigaberichtlinie auf die ausgewählten Postfächer anzuwenden.

## Verwenden von Exchange Online PowerShell anwenden eine Freigaberichtlinie auf ein oder mehrere Postfächer

In diesem Beispiel wird die Contoso-Freigaberichtlinie auf das Postfach von Barbara angewendet.

```
Set-Mailbox -Identity Barbara -SharingPolicy "Contoso"
```

In diesem Beispiel werden alle Benutzerpostfächer in der Marketing-Abteilung gesucht und anschließend die Freigaberichtlinie "Contoso Marketing" angewendet.

```
Get-Mailbox -Filter {Department -eq "Marketing"} | Set-Mailbox -SharingPolicy "Contoso Marketing"
```

In diesem Beispiel werden alle Postfächer angezeigt, auf die die Freigaberichtlinie "Contoso" angewendet wird. Außerdem werden die Benutzer nur mit Alias und E-Mail-Adressen in einer Tabelle aufgelistet.

```
Get-Mailbox -ResultSize unlimited | Where {$_.SharingPolicy -eq "Contoso"} | format-table Alias,EmailAddresses
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-Mailbox](#) und [Get-Mailbox](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Führen Sie eine der folgenden Aktionen aus, um sich zu vergewissern, dass Sie die Freigaberichtlinie erfolgreich auf ein Benutzerpostfach angewendet haben:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**, und wählen Sie dann auf das Postfach, dem Sie die Freigaberichtlinie angewendet. Klicken Sie auf **Bearbeiten** [ ] , klicken Sie auf **Postfachfunktionen** und stellen dann sicher, dass die richtige Freigaberichtlinie in der **Freigabe Richtlinie** angezeigt.
- Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Freigaberichtlinie auf ein Benutzerpostfach zugewiesen wurde. Stellen Sie sicher, dass die richtige Freigaberichtlinie für den Parameter *SharingPolicy* aufgeführt ist.

```
Get-Mailbox <username> | format-list
```

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Ändern, Deaktivieren oder Entfernen einer Freigaberichtlinie in Exchange Online

18.12.2018 • 4 minutes to read

Freigaberichtlinien steuern, wie Benutzer ihre Kalender mit Benutzern außerhalb Ihrer Organisation gemeinsam nutzen können. Es ist möglicherweise erforderlich, Eigenschaften von Freigaberichtlinien zu ändern, um z. B. Freigaberegeln zu ändern, die Zugriffsebene für Frei/Gebucht-Informationen zu ändern, eine Freigaberichtlinie temporär zu deaktivieren oder eine Freigaberichtlinie ganz zu entfernen.

Ausführliche Informationen zum Erstellen einer Freigaberichtlinie finden Sie unter [erstellen eine Freigaberichtlinie in Exchange Online](#)

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter Thema [Berechtigungen in Exchange Online](#).

## Verwenden Sie die Exchange-Verwaltungskonsole, um eine Freigaberichtlinie zu ändern

1. Gehen Sie vom Dashboard der Office 365-Verwaltungskonsole zu **Administrator > Exchange**.
2. Gehen Sie zu **Organisation > Freigabe**.
3. Unter **Einzelne Freigabe**, wählen Sie eine Freigaberichtlinie aus, und klicken Sie dann auf **Bearbeiten** 
4. Klicken Sie in **Freigaberichtlinie** auf **Bearbeiten** 
5. Ändern Sie in **Freigaberegel** die Einstellungen, wie zum Beispiel die Domäne, für die Informationen freigegeben werden, sowie die Freigabeebene für Kalender. Klicken Sie auf **Speichern**, um die Regel zu aktualisieren.
6. Klicken Sie in **Freigaberichtlinie** auf **Speichern**, um die Richtlinie zu aktualisieren.

## Festlegen einer Freigaberichtlinie als Standardfreigaberichtlinie mithilfe der Exchange-Verwaltungskonsole

1. Gehen Sie vom Dashboard der Office 365-Verwaltungskonsole zu **Administrator > Exchange**.
2. Gehen Sie zu **Organisation > Freigabe**.
3. Unter **Einzelne Freigabe**, wählen Sie eine Freigaberichtlinie aus, und klicken Sie dann auf **Bearbeiten** 
4. Aktivieren Sie in **Freigaberichtlinie** das Kontrollkästchen **Diese Richtlinie als meine Standardfreigaberichtlinie verwenden**.
5. Klicken Sie auf **Speichern**, um die Freigaberichtlinie zu aktualisieren.

## Verwenden der Exchange-Verwaltungskonsole, um eine Freigaberichtlinie zu deaktivieren

1. Gehen Sie vom Dashboard der Office 365-Verwaltungskonsole zu **Administrator > Exchange**.
2. Gehen Sie zu **Organisation > Freigabe**.
3. Wählen Sie unter **Individuelle Freigabe** eine Freigaberichtlinie.
4. Deaktivieren Sie in der Spalte **Ein** das Kontrollkästchen für die Freigaberichtlinie, die Sie deaktivieren möchten.

## Verwenden der Exchange-Verwaltungskonsole, um eine Freigaberichtlinie zu entfernen

### IMPORTANT

Bevor Sie eine Freigaberichtlinie entfernen, muss sie aus allen Benutzerpostfächern entfernt werden.

1. Gehen Sie vom Dashboard der Office 365-Verwaltungskonsole zu **Administrator > Exchange**.
2. Gehen Sie zu **Organisation > Freigabe**.
3. Unter **Einzelne Freigabe**, wählen Sie eine Freigaberichtlinie aus, und klicken Sie dann auf **Löschen**  

4. Klicken Sie im Warnungsdialogfeld auf **Ja**, um die Freigaberichtlinie zu löschen.

## Verwenden von Exchange Online PowerShell ändern, deaktivieren oder Entfernen einer Freigaberichtlinie

- In diesem Beispiel wird die Freigaberichtlinie "Contoso" geändert. Mithilfe dieser Richtlinie können Benutzer in der Domäne "Contoso" nur Frei/Gebucht-Informationen anzeigen.

```
Set-SharingPolicy -Identity Contoso -Domains 'sales.contoso.com: CalendarSharingFreeBusySimple'
```

- In diesem Beispiel wird der Freigaberichtlinie "Contoso" eine zweite Domäne hinzugefügt. Wenn Sie einer vorhandenen Richtlinie eine Domäne hinzufügen, müssen Sie sämtliche zuvor eingeschlossenen Domänen auch einschließen.

```
Set-SharingPolicy -Identity Contoso -Domains 'contoso.com: CalendarSharingFreeBusySimple',  
'atlanta.contoso.com: CalendarSharingFreeBusyReviewer', 'beijing.contoso.com:  
CalendarSharingFreeBusyReviewer'
```

- In diesem Beispiel wird die Freigaberichtlinie "Contoso" als Standardfreigaberichtlinie festgelegt.

```
Set-SharingPolicy -Identity Contoso -Default $True
```

- In diesem Beispiel wird die Freigaberichtlinie "Contoso" deaktiviert.

```
Set-SharingPolicy -Identity "Contoso" -Enabled $False
```

- Im ersten Beispiel wird die Freigaberichtlinie "Contoso" entfernt. Im zweiten Beispiel wird die Freigaberichtlinie "Contoso" entfernt und die Bestätigung unterdrückt, dass die Richtlinie wirklich entfernt

werden soll.

```
Remove-SharingPolicy -Identity Contoso
```

```
Remove-SharingPolicy -Identity Contoso -Confirm
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-SharingPolicy](#) und [Remove-SharingPolicy](#).

# Voicemail in Exchange Online: Unified Messaging

18.12.2018 • 23 minutes to read

Mit Unified Messaging (UM) können Benutzer Voicemail- und andere Features wie u. a. Outlook Voice Access und Mailboxansageregeln verwenden. Unified Messaging kombiniert Voicemessaging und E-Mails in einem Postfach, auf das über verschiedene Geräte zugegriffen werden kann. Benutzer können die Nachrichten über ihren E-Mail-Posteingang oder mit Outlook Voice Access auf einem beliebigen Telefon abhören oder lesen. Sie können steuern, wie Benutzer ausgehende Anrufe tätigen, und festlegen, wie Anrufe bei der Organisation behandelt werden.

Heute werden Voicemail- und E-Mail-Systeme in Organisationen von Messagingadministratoren oft als separate Systeme verwaltet. Voicemailnachrichten und E-Mails befinden sich in separaten Postfächern, die auf unterschiedlichen Servern gehostet sind. Benutzer können E-Mails über den Desktop und Voicemailnachrichten über das Telefon abrufen.

Mit UM in Office 365 können Onlineadministratoren Voicemessaging und E-Mails in einem Postfach kombinieren, sodass Benutzer ihre Voicemailnachrichten sowohl über ihren E-Mail-Posteingang als auch über Outlook Voice Access auf einem beliebigen Telefon lesen bzw. abhören können. UM verwendet ein Benutzerpostfach zum Speichern von E-Mails und Voicemailnachrichten.

## Unified Messaging-Funktionen

Die Voicemailfeatures in UM bieten Vorteile für Benutzer und Administratoren in Ihrer Organisation und in Exchange Online.

### Features für Benutzer

Wenn Sie UM für Ihre Organisation konfigurieren, können Benutzer zugreifen, Voicemail, e-Mail, persönliche Kontakte und Kalenderinformationen, die sich in ihrem Postfach aus einer e-Mail-Client, beispielsweise Microsoft Outlook oder Outlook Web App von einem Mobiltelefon mit Microsoft befindet Exchange ActiveSync festzulegen, nach oben, wie eine Windows Phone oder über ein Telefon. Darüber hinaus können Benutzer die folgenden Features:

- **Zugriff auf ihr Exchange-Postfach:** Benutzer können eine umfassende Auswahl an Voicemail-Features von Internet-fähige Mobiltelefone, Outlook 2007 oder höher, und Outlook Web App zugreifen. Zu diesen Features gehören viele Konfigurationsoptionen für Voicemail und die Möglichkeit, eine Sprachnachricht entweder im Lesebereich, mithilfe der integrierten Windows Media Player oder der Nachrichtenliste mit PC-Lautsprechern wiedergegeben werden sollen.
- **Wiedergabe über Telefon:** die Wiedergabe über Telefon Feature können Benutzer Sprachnachrichten über ein Telefon wiedergeben. Wenn der Benutzer in einer Office-Arbeitsbereich funktioniert, verwendet einen öffentlichen Computer oder einem Computer, der für Multimedia nicht aktiviert, oder auf eine Sprachnachricht, die vertrauliche ist hört, können sie nicht möchten oder in der Lage, eine Sprachnachricht über PC-Lautsprechern zu überwachen. Sie können die über ein beliebiges Telefon, einschließlich einer privaten, Office, oder Mobiltelefon Sprachnachricht wiedergeben.
- **Voice Mail Formular:** das Voice Mail Formular ähnelt das Standard-e-Mail-Formular. Er bietet Benutzern eine Schnittstelle zum Ausführen von Aktionen wie Wiedergabe, beenden oder Anhalten Sprachnachrichten, Wiedergeben von Sprachnachrichten an einem Telefon und hinzufügen und Bearbeiten von Notizen.

Das Voicemailformular enthält den eingebetteten Windows Media Player und ein Feld Audionotizen. Der eingebettete Windows Media Player und das Feld "Audionotizen" werden entweder bei der Vorschau einer Sprachnachricht im Lesebereich angezeigt oder in einem separaten Fenster, wenn die Sprachnachricht vom

Benutzer geöffnet wird. Wenn Benutzer nicht für UM aktiviert sind oder auf dem Clientcomputer kein unterstützter E-Mail-Client installiert ist, werden Sprachnachrichten nur als E-Mail-Anlagen angezeigt, und das Voicemailformular ist nicht verfügbar.

- **Benutzerkonfiguration:** Benutzer können verschiedene Voicemailoptionen mit Outlook Web App UM konfigurieren. Beispielsweise kann der Benutzer persönliche Begrüßung aufzeichnen konfigurieren verpasste Anrufe und Textnachricht Benachrichtigungen und eine VoIP mail-am Telefon wiedergeben, und eine Mail-Sprachzugriff PIN zurücksetzen.
- **Mailboxansage:** Anrufbeantwortung Beantworten eingehender Anrufe im Namen von Benutzern, ihre persönliche Ansage abspielen, Aufzeichnen von Nachrichten und senden Sie dann die Voicemail an ihren Posteingang als e-Mail-Nachricht enthält.
- **Die Mailboxansageregeln:** The die Mailboxansageregeln Feature können Benutzer, die für Voicemail aktiviert sind zu bestimmen, wie ihre eingehende Anruf entgegennehmen von Anrufern verarbeitet werden soll. Der antwortende Regeln auf eingehende Anrufe angewendet werden wie Anruf ist ähnlich wie bei Posteingangsregeln für eingehende e-Mail-Nachrichten angewendet werden. Standardmäßig werden keine Anrufe von mailboxansageregeln konfiguriert. Ein eingehender Anruf entgegengenommen wurde, wird der Aufrufer aufgefordert, eine Sprachnachricht hinterlassen, für die Person, die aufgerufen wird. Mithilfe von Regeln für Anrufbeantwortung, können ein Anrufer:
  - Sprachnachricht für den Benutzer hinterlassen.
  - Umleiten an einen alternativen Kontakt des Benutzers.
  - Umleiten an die Voicemail des alternativen Kontakts.
  - Umleiten an andere Telefonnummern, die der Benutzer konfiguriert hat.
  - Verwenden des Features "Mich suchen" oder Ermitteln des Benutzers per Umleitung von einer Vermittlungsstelle.
- **Voicemailvorschau:** Unified Messaging automatische Spracherkennung Spracherkennung (ASR) auf neu erstellten Voicemailnachrichten verwendet. Wenn Benutzer Sprachnachrichten empfangen, enthalten die Nachrichten an eine Aufzeichnung und den Text, der aus der VoIP-Aufzeichnung erstellt wurde. Benutzer finden Sie unter den VoIP-Nachrichtentext angezeigt, die in einer e-Mail-Nachricht in Outlook Web App oder eine andere unterstützte e-Mail-Client aus.
- **Message Waiting Indicator:** Message Waiting Indicator ist ein Feature in den meisten älteren Voicemail-Systemen gefunden und verweisen auf einen Mechanismus, der das Vorhandensein einer neuen Nachricht angibt. Aktivieren oder Deaktivieren von Message Waiting Indicator erfolgt auf das Postfach des Benutzers oder einer um-Postfachrichtlinie.
- **Verpasste Anrufe und VoIP e-Mail-Benachrichtigungen mithilfe von SMS:** Wenn Benutzer Teil einer hybriden oder Office 365-Bereitstellung sind, und sie konfigurieren Sie ihre Voicemail-Einstellungen mit ihrer Mobiltelefonnummer und die anrufweiterleitung konfigurieren, können sie Benachrichtigungen zu erhalten verpasste Anrufe und neuen Sprachnachrichten auf ihren Mobiltelefonen in einer Textnachricht über die Short Messaging Service (SMS). Um das Risiko dieser Arten von Benachrichtigungen erhalten möchten, müssen die Benutzer zuerst konfigurieren Textnachrichten und dürfen auch aktivieren Sie Benachrichtigungen für ihr Konto.
- **Geschützte Voicemail:** geschützte Voicemail ist ein Feature, mit dem Benutzer private Nachrichten senden kann. Diese Voicemail geschützt ist, und Benutzer dürfen weiterleiten, kopieren oder Extrahieren der VoIP-Datei aus e-Mail. Geschützte Voicemail erhöht die Vertraulichkeit der Voicemailnachrichten, und ermöglicht Benutzern, die die Benutzergruppe für Sprachnachrichten zu begrenzen.
- **Outlook Voice Access:** zwei UM Benutzeroberflächen für Benutzer verfügbar sind: der Telefon-Benutzeroberfläche (TUI) und der VoIP-Benutzeroberfläche (Benutzerschnittstelle für Spracheingabe). Diese

beiden Schnittstellen werden zusammen mit Outlook Voice Access bezeichnet. Outlook Voice Access-Benutzer können Outlook Voice Access beim Zugriff auf das Voicemailsysteem von einer internen oder externen Telefon. Benutzer, die sich in das Voicemailsysteem einwählen können ihr Postfach mithilfe von Outlook Voice Access zugreifen. Jedoch, wenn ein Benutzer das Verzeichnis für Ihre Organisation gesucht werden soll, müssen sie das wichtigsten Pad über ein Telefon verwenden zum Suchen nach einem Benutzer. Verwenden ihre Voicemail-zum Durchsuchen des Verzeichnisses ist nicht verfügbar. Ein Telefon verwenden, können ein UM-aktivierten Benutzer:

- Auf Voicemail zugreifen.
- Abhören, Weiterleiten oder Beantworten von E-Mails.
- Kalenderinformationen abhören.
- Zugreifen auf Kontakte im Verzeichnis der Organisation oder auf einzelne Kontakte bzw. Kontaktgruppen, die in den persönlichen Kontakten des Benutzers gespeichert sind bzw. Wählen der entsprechenden Rufnummern.
- Besprechungsanfragen annehmen oder stornieren.
- Festlegen einer Sprachnachricht, um Anrufer über die Abwesenheit des angerufenen Teilnehmers zu informieren.
- Sicherheitseinstellungen und persönliche Benutzeroptionen festlegen.
- Suchen nach Benutzern im Verzeichnis der Organisation.

- **Gruppe Adressierung über Outlook Voice Access:** Benutzer können eine einzelne e-Mail-Nachricht senden, zu einem einzelnen Benutzer in ihren persönlichen Kontakten, an mehrere Empfänger aus dem Verzeichnis, indem Sie jeden Empfänger einzeln hinzufügen oder indem Sie den Namen einer Verteilerliste hinzufügen aus dem Verzeichnis für Ihre Organisation. UM in Office 365 Wenn ein Benutzer auf ihr Postfach mithilfe von Outlook Voice Access anmeldet können sie auch e-Mail und Voicemail-Nachrichten an Benutzer in einer Gruppe in ihren persönlichen Kontakten gespeichert senden.

## Verwaltungsfunktionen

Derzeit verwalten die meisten Benutzer und IT-Abteilungen ihre Voicemail getrennt von ihrer E-Mail. Voicemail und E-Mail sind als getrennte Posteingänge vorhanden, die auf getrennten Servern gehostet werden und auf die über den Desktop (bei E-Mail) und über ein Telefon (bei Voicemail) zugegriffen wird. UM stellt einen integrierten Informationsspeicher für alle Nachrichten und Zugriff auf Inhalte über den Computer und das Telefon bereit.

Exchange-Administratoren können über dieselbe Oberfläche, mit denen sie die restlichen Exchange, mit der Exchange-Verwaltungskonsole (EAC) und Exchange Online PowerShell verwalten UM verwalten. Sie können:

- Verwalten von Voicemail und E-Mail von einer einzigen Plattform aus.
- UM mithilfe skriptfähiger Befehle verwalten.
- Hochverfügbare und zuverlässige UM-Infrastruktur aufbauen.

Office 365 UM bietet Administratoren folgende Vorteile:

- **Konsolidierung von Voicemail-Systeme:** derzeit die meisten Voice messaging-Systeme erfordern, dass alle VoIP-Messagingkomponenten in jedem physischen Standort in einer Organisation installiert werden. In dieser Art der Anordnung verwaltet der Voicemessaging-Systemen in Branch Büros befinden sich außerhalb des zentralen Büros und müssen vor Ort. Dies führt häufig höhere Verwaltungskosten und Komplexität. UM können Sie Ihre Voicemail-System von einem zentralen Ort zu verwalten. Zum Erstellen einer zentralisierten Management-Systems für UM Integration von VoIP-Gateways, IP-PBX-Anlagen oder PBX-Anlagen und Ihr Telefonsystem und anschließendem bereitstellen Session Border Controller (SBCs), um Ihr Telefonsystem mit der Office 365-Bereitstellung zu verbinden. Bereitstellen einer zentralisierten

Voice messaging-System auf diese Weise kann dazu führen, dass Hardware- und Administrationskosten deutlich zu senken.

#### NOTE

Exchange Online UM Unterstützung für Drittanbieter-Nebenstellenanlage Systeme über direkte Verbindungen von Kunden betrieben SBCs werden im Juli 2018 beendet. Weitere Informationen finden Sie im Exchange-Teamblog [die Einstellung der Unterstützung für Session Border Controller in Exchange Online Unified Messaging](#) für Weitere Informationen.

- **Integrierte UM Administratorrollen:** die UM-spezifische Administratorrollen für die Verwaltung von UM und Voicemail-Features umfassen Folgendes:

- UM-Postfächer
- UM-Telefonansagen
- Unified Messaging

- **Eingehende Faxe unterstützt:** UM bietet integrierte faxunterstützung für eingehende für Benutzer, die ein UM-aktivierten Postfach besitzen. Sie können Faxnachrichten über an ihre Durchwahlnummer getätigte Anrufe empfangen.

Kunden, die eine Faxlösung benötigen, müssen auf eine Faxpartnerlösung zurückgreifen.

Faxpartnerlösungen sind von mehreren Faxpartnern erhältlich. Die Faxpartnerlösungen werden nahtlos in Exchange integriert und ermöglichen UM-aktivierten Benutzern den Empfang eingehender Faxnachrichten. Eine Liste mit Links zu Faxpartnerlösungen finden Sie unter [Microsoft Pinpoint für Faxpartner](#).

- **Unterstützung mehrerer Sprachen:** aller verfügbaren Sprachpakete enthalten Unterstützung für die Sprachsynthese (TTS) Engine und die aufgezeichnete eingabeaufforderungen für eine angegebene Sprache und ASR Support. Unterstützung für Voicemailvorschau können jedoch nur einige Language Packs enthalten.

- **Automatische Telefonzentrale:** eine automatische Telefonzentrale ist ein Satz von Ansagen, die externen und internen Benutzern den Zugriff auf das Voicemailsysteem bereitstellt. Benutzer können die Telefon Tastatur oder Spracherkennung Eingaben über das automatische Telefonzentrale Menü verschieben, einen Anruf an einen Benutzer oder einen Benutzer in Ihrer Organisation zu suchen und platzieren Sie Anrufe verwenden. Eine automatische Telefonzentrale bietet dem Administrator die Möglichkeit:

- Erstellen eines angepassten Menüs für externe Benutzer.
- Definieren von Informationsansagen, von Ansagen während der Geschäftszeiten und von Ansagen außerhalb der Geschäftszeiten.
- Definieren von Urlaubszeitplänen.
- Beschreiben der Suche im Verzeichnis der Organisation.
- Beschreiben der Verbindung mit der Durchwahl eines Benutzers, damit externe Anrufer einen Benutzer durch Angabe seiner Durchwahl anrufen können.
- Beschreiben der Suche im Verzeichnis der Organisation, damit externe Anrufer das Verzeichnis durchsuchen und einen bestimmten Benutzer anrufen können.
- Ermöglichen von Anrufen externer Benutzer bei der Vermittlungsstelle.

## Planen und Bereitstellen von Unified Messaging

Unified Messaging setzt voraus, dass Sie Ihr vorhandenes Telefonsystem für Ihre Organisation mithilfe von SBCs in Office 365 integrieren. Für eine erfolgreiche Bereitstellung ist eine sorgfältige Analyse Ihrer vorhandenen Telefonieinfrastruktur und die Durchführung der richtigen Planungsschritte für die Bereitstellung und Verwaltung von Voicemail in UM erforderlich.

#### **NOTE**

Exchange Online UM Unterstützung für Drittanbieter-Nebenstellenanlage Systeme über direkte Verbindungen von Kunden betrieben SBCs werden im Juli 2018 beendet. Weitere Informationen finden Sie im Exchange-Teamblog [die Einstellung der Unterstützung für Session Border Controller in Exchange Online Unified Messaging](#) für Weitere Informationen.

Wenn Sie UM in Office 365 verwenden möchten, müssen Sie Designprobleme und andere Schwierigkeiten in Betracht ziehen, die sich bei der Konfiguration von UM möglicherweise negativ auf Ihre Unternehmensziele auswirken. Im Allgemeinen gilt: Je einfacher das UM-Setup, umso leichter ist es, UM zu konfigurieren und zu verwalten. Grundsätzlich sollten Sie nur die UM-Komponenten, z. B. UM-Wähleinstellungen, automatische Telefonzentralen und UM-Postfachrichtlinien, erstellen, die unbedingt erforderlich sind, um Ihre Geschäfts- und Unternehmensziele zu unterstützen. Große Unternehmen mit komplexen Netzwerk- und Telefoniumgebungen, mehreren Geschäftseinheiten oder anderen komplizierten Strukturen erfordern eine ausführlichere Planung als kleine Organisationen mit relativ einfachen UM-Anforderungen.

Sie müssen viele Aspekte in Betracht ziehen und auswerten, um UM erfolgreich bereitstellen zu können. Sie müssen die verschiedenen Aspekte von Unified Messaging sowie jeder Komponente und jedes Feature verstehen, damit Sie die UM-Infrastruktur und -Bereitstellung entsprechend planen können. Wenn Sie Zeit für die Planung und die Analyse von Einzelaspekten vorsehen, können Sie Probleme bei der Bereitstellung von UM in Ihrer Organisation verhindern. Die folgenden Bereiche sollten z. B. bei der Planung von UM in Ihrer Organisation berücksichtigt und ausgewertet werden:

- Die Anforderungen Ihrer Organisation.
- Die Sicherheitsanforderungen Ihrer Organisation.
- Ihr vorhandenes leitungsvermitteltes Telefonienetzwerk sowie Ihr Voicemailsysteem.
- Ihr aktuelles paketvermitteltes IP-Netzwerkdesign. Dies umfasst Ihre lokalen LAN- (Local Area Network) und WAN-Verbindungen und -Geräte.
- Die Anzahl von Benutzern, die unterstützt werden müssen.
- Die Frage, ob UM mit Lync Server integriert werden soll, um Enterprise-VoIP in Office 365 zu aktivieren.
- Die Anordnung von VoIP-Gateways, Telefoniegeräten und SBCs.
- Die Speicheranforderungen für Voicemailbenutzer.

## UM mit der Exchange-Verwaltungskonsole und Exchange Online PowerShell verwalten

### **Verwaltung über die Exchange-Verwaltungskonsole**

Office 365 verfügt über eine einzige einheitliche Verwaltungskonsole für Ihre Organisation, die alle UM-Komponenten und -Funktionen umfasst. Die EAC stellt eine optimierte Schnittstelle für die Verwaltung von Exchange Online-Bereitstellungen bereit. Zu den Features der Exchange-Verwaltungskonsole zählen u. a.:

- **Listenansicht:** die Listenansicht in der Exchange-Verwaltungskonsole zum Anzeigen von Einstellungen für Features, die Sie in Ihrer Organisation verwenden, Postfächer und Empfänger arbeitet. Paging in der Listenansicht können Sie Ergebnisse pro Seite angezeigt. Sie können auch konfigurieren Seitengröße und die Anzahl der Einträge und Einträge in einer CSV-Datei exportieren.

- **Hinzufügen/Entfernen von Spalten in der Listenansicht Empfänger:** Sie können auswählen, welche Spalten anzeigen, und Sie können Ihre benutzerdefinierten Listenansichten speichern.
- **Verwaltung öffentlicher Ordner:** Verwaltung öffentlicher Ordner in der Exchange-Verwaltungskonsole verfügbar ist, und nicht benötigen Sie separate Tools zum Verwalten von öffentlicher Ordnern.
- **Benachrichtigungen:** der Exchange-Verwaltungskonsole enthält nun eine Benachrichtigung-Viewers, damit Sie den Status von Prozessen anzeigen und können, wenn Sie auswählen, Benachrichtigung über eine e-Mail-Nachricht erhalten, wenn der Vorgang abgeschlossen ist.
- **Editor für benutzerdefinierte Rolle basierend Access Control (RBAC):** in Office 365 die Editor für benutzerdefinierte RBAC-Funktionalität ist in der Exchange-Verwaltungskonsole, und Sie brauchen ein separates Tool zum Verwalten von RBAC.
- **UM Tools:** In Office 365, Sie Anrufstatistik und Benutzeranrufprotokolle-Tools verwenden können, UM Statistiken und Informationen zu bestimmten Anrufen für einen Benutzer bereitzustellen.

Weitere Informationen zu der Exchange-Verwaltungskonsole finden Sie unter [Exchange Admin center in Exchange Online](#).

### **Exchange Online PowerShell management**

Exchange Online PowerShell ist eine leistungsstarke Befehlszeilenschnittstelle, die die Automatisierung von Verwaltungsaufgaben ermöglicht. Exchange Online PowerShell können alle Aufgaben, die von der Exchange-Verwaltungskonsole ausgeführt werden kann, die plus Aufgaben, bei die nicht möglich ausführen, in der Exchange-Verwaltungskonsole. Wenn etwas in der Exchange-Verwaltungskonsole, ist es tatsächlich Exchange Online PowerShell, die die Arbeit im Hintergrund Aufgaben verwendet wird.

Weitere Informationen zu Exchange Online PowerShell finden Sie unter [Exchange Online PowerShell](#).

# Voicemailbegrüßungen, Ansagen, Menüs und Eingaben in Exchange Online

18.12.2018 • 15 minutes to read

Wenn Sie Unified Messaging (UM) installieren, wird gleichzeitig auch eine Reihe Standardaudiodateien für das Voicemailsystem sowie für Menü- und Informationsansagen installiert. Auch wenn Sie eine vollfunktionsfähige automatische UM-Telefonzentrale oder einen Wählplan einrichten können, die bzw. der ausschließlich die standardmäßigen Audioeingabeaufforderungen verwendet, sind diese Eingabeaufforderungen doch zu generisch, um in zahlreichen Unternehmen als annehmbare öffentliche Schnittstelle zu dienen. In diesem Thema werden die System- und Menüansagen, Begrüßungen und Informationsansagen behandelt, die von UM-Wählplänen und automatischen Telefonzentralen verwendet werden, sowie deren Verwendung beim Zugriff auf das Voicemailsystem durch Anrufer.

## Übersicht über Telefonansagen und Begrüßungen

Diese Systemaudiodateien oder Ansagen sollten niemals ersetzt werden. UM ermöglicht jedoch das Anpassen der Begrüßungen, Hauptmenü- und Informationsansagen der UM-Wähleinstellungen und der automatischen Telefonzentrale.

Die folgende Tabelle zeigt eine Übersicht über die für UM-Wähleinstellungen verwendeten Ansagen und Begrüßungen.

### Telefonansagen für UM-Wähleinstellungen

TELEFONANSAGEN UND BEGRÜSSUNGEN	BESCHREIBUNG
Systemansagen	Dürfen nicht geändert werden.
Begrüßung	Die Standardbegrüßung ist eine Systemansage, die standardmäßig wiedergegeben wird. Sie können jedoch eine von Ihnen erstellte benutzerdefinierte Begrüßungsdatei verwenden.
Informationsansage	Informationsansagen sind standardmäßig deaktiviert. Wenn Sie eine Informationsansage aktivieren, müssen Sie eine benutzerdefinierte Begrüßungsdatei angeben.

Die folgende Tabelle zeigt eine Übersicht über die für automatische UM-Telefonzentralen verwendeten Ansagen und Begrüßungen.

### Telefonansagen für automatische UM-Telefonzentralen

TELEFONANSAGEN UND BEGRÜSSUNGEN	BESCHREIBUNG
Systemansagen	Dürfen nicht geändert werden.
Menüansagen während der Geschäftszeit	Menüansagen während der Geschäftszeit sind standardmäßig aktiviert, und es wird eine Systemansage wiedergegeben. Sie können jedoch eine von Ihnen erstellte benutzerdefinierte Begrüßungsdatei verwenden.

TELEFONANSAGEN UND BEGRÜSSUNGEN	BESCHREIBUNG
Menüansagen außerhalb der Geschäftszeit	Menüansagen außerhalb der Geschäftszeit sind standardmäßig aktiviert, und es wird eine Systemansage wiedergegeben. Sie können jedoch eine von Ihnen erstellte benutzerdefinierte Begrüßungsdatei verwenden.
Begrüßung während der Geschäftszeit	Die Begrüßung während der Geschäftszeit ist standardmäßig aktiviert, und es wird eine Systemansage wiedergegeben. Sie können jedoch eine von Ihnen erstellte benutzerdefinierte Begrüßungsdatei verwenden. Diese wird auch als Willkommensansage bezeichnet.
Begrüßung außerhalb der Geschäftszeit	Die Begrüßung außerhalb der Geschäftszeit ist standardmäßig aktiviert, und es wird eine Systemansage wiedergegeben. Sie können jedoch eine von Ihnen erstellte benutzerdefinierte Begrüßungsdatei verwenden. Diese wird auch als Willkommensansage bezeichnet.
Informationsansage	Informationsansagen sind standardmäßig deaktiviert. Wenn Sie eine Informationsansage aktivieren, müssen Sie eine benutzerdefinierte Begrüßungsdatei angeben.

## Systemansagen

Unified Messaging nutzt eine Sammlung von Standardtelefonansagen für die Verwendung mit Outlook Voice Access, Wähleinstellungen und automatischen Telefonzentralen. Es sind Hunderte von Systemansagen für jede Sprache verfügbar. Unified Messaging gibt die Audiodateien für diese Systemansagen für Anrufer wieder, wenn diese auf das Voicemailsystem zugreifen. Im Folgenden sind Beispiele für diese Systemansagen aufgeführt:

- "Geben Sie Ihre PIN ein".
- "Wenn Sie auf Ihr Postfach zugreifen möchten, geben Sie Ihre Durchwahl ein".
- "Zum Kontaktieren einer Person drücken Sie die Raute-Taste".
- "Buchstabieren Sie den Namen der Person, mit der eine Verbindung hergestellt werden soll. Beginnen Sie dabei mit dem Nachnamen".
- "Wenn Sie mit einer bestimmten Person sprechen möchten, nennen Sie den Namen".

**Caution**

Das Ändern der UM-Systemansagen wird nicht unterstützt.

## Begrüßungen und Informationsansagen für UM-Wählpläne

Wenn Sie einen UM-Wählplan erstellt haben, können Sie die Audiodateien für standardmäßige Systemansagen verwenden oder um benutzerdefinierte Audiodateien zu erstellen, die zusammen mit UM-Wählplänen eingesetzt werden können.

Um-Wählpläne haben eine Begrüßung und eine optionale Informationsansage, den, die Sie ändern können. Die Begrüßung wird verwendet, wenn ein Benutzer Outlook Voice Access oder einer anderen Anrufer eine Outlook Voice Access-Nummer anrufen. Die Anrufer hören, eine standardmäßige Willkommensseite Ansage, die besagt, "Willkommen, Sie mit Microsoft Exchange verbunden sind." Möglicherweise möchten Sie diese Standard-Begrüßung ändern, und geben Sie eine alternative Willkommen Begrüßung speziell für Ihr Unternehmen, z. B. "Willkommen, Outlook Voice Access für Woodgrove Bank." Wenn Sie diese Begrüßung anpassen, können Sie aufzeichnen die benutzerdefinierte Ansage und speichern sie als eine WAV-Datei, und konfigurieren Sie anschließend die Wähleinstellungen an diese benutzerdefinierte Begrüßung verwenden.

Bei Unified Messaging kann im Anschluss an die Begrüßung eine Informationsansage wiedergegeben werden. Standardmäßig ist keine Informationsansage konfiguriert. Sie können jedoch eine Informationsansage für Anrufer zur Verfügung stellen. Sie können die Informationsansage für allgemeine Ankündigungen verwenden, die sich häufiger ändern als die Begrüßung, oder für Ankündigungen, die zur Einhaltung von Unternehmensrichtlinien erforderlich sind. Wenn Anrufer unbedingt die gesamte Informationsansage abhören sollen, kann diese als nicht unterbrechbar konfiguriert werden. In diesem Fall kann ein Anrufer die Informationsansage nicht durch Drücken einer Taste oder Sprechen eines Befehls abbrechen.

In der folgenden Tabelle werden die Begrüßungen und Informationsansagen für UM-Wähleinstellungen beschrieben.

#### **Begrüßungen und Informationsansagen für UM-Wählpläne**

BEGRÜSSUNG	STANDARDBEISPIEL	ANGEPASSTES BEISPIEL
Begrüßung	"Willkommen, Sie mit Microsoft Exchange verbunden sind."	"Willkommen bei Outlook Voice Access der Woodgrove Bank".
Informationsansage	Standardmäßig ist keine Informationsansage konfiguriert.	"Durch das Verwenden dieses Systems erklären Sie sich einverstanden, alle Unternehmensrichtlinien zu befolgen, wenn Sie auf dieses System zugreifen".

Wenn Sie Begrüßungen und Ansagen anpassen und konfigurieren, stellen Sie sicher, dass die Spracheinstellung, die für die UM-Wähleinstellungen konfiguriert ist, der Spracheinstellung der von Ihnen erstellten benutzerdefinierten Telefonansagen entspricht. Wenn dies nicht der Fall ist, hört ein Anrufer ggf. eine Nachricht oder Begrüßung in einer Sprache und eine andere Nachricht oder Begrüßung in einer anderen Sprache.

## **Begrüßungen, Ansagen und Menüansagen für automatische UM-Telefonzentralen**

Ebenso wie UM-Wähleinstellungen verfügen auch automatische UM-Telefonzentralen über eine Begrüßung, eine optionale Informationsansage und eine optionale benutzerdefinierte Menüansage. Sie können verschiedene Versionen der Begrüßung und Menüansage für Zeitspannen innerhalb bzw. außerhalb der Geschäftszeiten konfigurieren. Alle diese Ansagen können geändert werden.

Die Begrüßung handelt es sich um ein Anrufer als erstes hört bei einer automatischen UM-Telefonzentrale den Anruf annimmt. In der Standardeinstellung bedeutet, "Willkommen Sie bei der Microsoft Exchange-Telefonzentrale." Die Audiodatei, die wiedergegeben wird für den Anruf ist der Standard-System-Eingabeaufforderung für die automatische Telefonzentrale. Allerdings sollten Sie als alternative Grußformel speziell für Ihr Unternehmen, z. B. "Vielen Dank für Woodgrove Bank aufrufen." Zum Anpassen dieser Begrüßung Aufzeichnen der benutzerdefinierten Ansage und als eine WAV-Datei zu speichern, und konfigurieren Sie die automatische Telefonzentrale verwenden Sie diese benutzerdefinierte Begrüßung. Mit der Willkommensseite Ansage auch anpassen können aufgefordert, klicken Sie im Menü.

Bei Unified Messaging kann zudem im Anschluss an die Begrüßung innerhalb oder außerhalb der Geschäftszeit eine Informationsansage wiedergegeben werden. Standardmäßig ist keine Informationsansage konfiguriert. Sie können Anrufern jedoch eine solche zur Verfügung stellen. Die Informationsansage kann die Geschäftszeiten der Organisation wiedergeben. Beispiel "Unsere Geschäftszeiten sind Montag bis Freitag von 08:00 Uhr bis 17:30 Uhr und Samstag von 8:30 Uhr bis 13:00 Uhr". Die Informationsansage kann ebenfalls Informationen enthalten, die für die Einhaltung von Organisationsrichtlinien erforderlich sind, wie zum Beispiel "Anrufe können zu Schulungszwecken überwacht werden". Wenn Anrufer unbedingt die gesamte Informationsansage abhören sollen, kann diese als nicht unterbrechbar konfiguriert werden. In diesem Fall kann der Anrufer die Informationsansage nicht durch Drücken einer Taste oder Sprechen eines Befehls abbrechen.

In der folgenden Tabelle werden die Begrüßungen und Informationsansagen für automatische UM-Telefonzentralen beschrieben.

### Begrüßungen, Informationsansagen und Menüansagen für automatische UM-Telefonzentralen

BEGRÜSSUNG	STANDARDBEISPIEL	ANGEPASSTES BEISPIEL
Begrüßung während der Geschäftszeit	"Willkommen bei der automatischen Telefonzentrale von Microsoft Exchange".	"Danke für Ihren Anruf bei der Woodgrove Bank".
Begrüßung außerhalb der Geschäftszeit	Es wird keine Begrüßung außerhalb der Geschäftszeit wiedergegeben, bevor Sie Geschäftszeiten für die automatische Telefonzentrale konfigurieren. Die Begrüßung innerhalb der Geschäftszeit wird jedoch jederzeit für Anrufer wiedergegeben.	"Sie rufen die Woodgrove Bank außerhalb der Geschäftszeit an. Unsere Geschäftszeiten sind Montag und Freitag zwischen 8:00 Uhr und 17:00 Uhr."
Informationsansage	Standardmäßig sind keine Informationsansagen konfiguriert.	"Anrufe können zu Schulungszwecken überwacht werden".
Hauptmenüansage während der Geschäftszeit	Es wird keine Standardmenüansage während der Geschäftszeit wiedergegeben, bevor Sie Tastenzuordnungen für die automatische Telefonzentrale konfigurieren.	"Wenn Sie technischen Support benötigen, drücken oder sagen Sie 1. Wenn Sie mit Unternehmensstandorten oder der Unternehmensverwaltung verbunden werden möchten, drücken oder sagen Sie 2. Wenn Sie mit dem Vertrieb verbunden werden möchten, drücken oder sagen Sie 3".
Hauptmenüansage außerhalb der Geschäftszeit	Es wird keine Standardmenüansage außerhalb der Geschäftszeit wiedergegeben, bevor Sie Tastenzuordnungen und die Geschäftszeiten für die automatische Telefonzentrale konfigurieren.	"Wir freuen uns sehr über Ihren Anruf. Sie rufen die Woodgrove Bank jedoch außerhalb der Geschäftszeit an. Wenn Sie eine Nachricht hinterlassen möchten, drücken oder sagen Sie 1. Wir rufen Sie so schnell wie möglich zurück".

Stellen Sie ebenso wie bei UM-Wähleinstellungen sicher, dass die für die automatische UM-Telefonzentrale konfigurierte Spracheinstellung der Sprache der von Ihnen erstellten benutzerdefinierten Begrüßungen entspricht und auf die gleiche Sprache wie die UM-Wähleinstellungen festgelegt ist. Wenn dies nicht der Fall ist, hört ein Anrufer ggf. eine Nachricht oder Begrüßung in einer Sprache und eine andere Nachricht oder Begrüßung in einer anderen Sprache.

## Anpassen von Begrüßungen, Informationsansagen und Menüansagen sowie Navigationsmenüs

Wenn Sie eine automatische UM-Telefonzentrale erstellen, sind die Begrüßungen und Ansagen innerhalb und außerhalb der Geschäftszeiten nicht konfiguriert, und es sind keine Tastenzuordnungen für Ansagen für das Hauptmenü innerhalb und außerhalb der Geschäftszeiten definiert. Gehen Sie wie folgt vor, um benutzerdefinierte Begrüßungen und Ansagen für eine automatische Telefonzentrale zu konfigurieren:

- Konfigurieren der Zeiten während und außerhalb der Geschäftszeiten auf der Seite **Geschäftszeiten**.
- Erstellen der Begrüßungsaudiodateien (WAV oder WMA), die für die Begrüßungsansagen während der Geschäftszeiten bzw. außerhalb der Geschäftszeiten verwendet werden.
- Konfigurieren der Begrüßungsansagen während und außerhalb der Geschäftszeiten auf der Seite

## **Begrüßungen.**

- Erstellen der Begrüßungsdateien, die für die Begrüßungsansagen für das Hauptmenü während und außerhalb der Geschäftszeiten verwendet werden.
- Konfigurieren der Begrüßungsansagen für das Hauptmenü während und außerhalb der Geschäftszeiten auf der Seite **Begrüßungen**.
- Aktivieren und Konfigurieren der Menünavigation während und außerhalb der Geschäftszeiten auf der Seite **Menünavigation**.

# Festlegen der Standardsprache für einen Wählplan

18.12.2018 • 2 minutes to read

## Verwenden der Exchange-Verwaltungskonsole zum Konfigurieren der Standardsprache für einen UM-Wählplan

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. Wählen Sie in der Listenansicht den UM-Wählplan aus, den Sie ändern möchten, und klicken Sie dann auf der Symbolleiste auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Wählen Sie auf der Seite **Einstellungen** unter **Audiosprache** in der Dropdownliste die gewünschte Sprache aus.
5. Klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.

## Verwenden der Shell zum Konfigurieren der Standardsprache für einen UM-Wählplan

In diesem Beispiel wird Deutsch als Standardsprache für den Satz UM-Wähleinstellungen " `MyUMDialPlan`" festgelegt.

```
Set-UMDialPlan -Identity MyUMDialPlan -DefaultLanguage de-DE
```

In diesem Beispiel wird Japanisch als Standardsprache für den Satz UM-Wähleinstellungen " `MyUMDialPlan`" festgelegt.

```
Set-UMDialPlan -Identity MyUMDialPlan -DefaultLanguage ja-JP
```

In diesem Beispiel wird australisches Englisch als Standardsprache für den Satz UM-Wähleinstellungen " `MyUMDialPlan`" festgelegt.

```
Set-UMDialPlan -Identity MyUMDialPlan -DefaultLanguage en-AU
```

# Auswählen der Sprache für eine automatische Telefonzentrale

18.12.2018 • 2 minutes to read

Sie können die Einstellung für eine automatische Telefonzentrale von Unified Messaging (UM) Prompt Standardsprache konfigurieren. Die Sprache einer automatischen UM-Telefonzentrale verfügbare Einstellung können Sie die Prompt Standardsprache für die automatische Telefonzentrale zu konfigurieren. Wenn Sie für die automatische Telefonzentrale fordert das Standard-System verwenden, ist dies die Sprache aus, die der Anrufer hört, wenn die automatische Telefonzentrale den eingehenden Anruf beantwortet. Diese Einstellung wirkt sich nicht benutzerdefinierten Ansagen aus, die auf eine automatische Telefonzentrale konfiguriert sind.

## Konfigurieren der Standardspracheinstellung mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf der Symbolleiste auf **Bearbeiten**.
3. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
4. Wählen Sie auf der Seite **Allgemein** unter **Sprache für automatisierte Sprachschnittstelle** aus der Dropdownliste die erforderliche Sprache aus.
5. Klicken Sie auf **Speichern**, um Ihre Änderungen zu übernehmen.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie die Einstellung für die Standardsprache

In diesem Beispiel wird die Standardsprache für die automatische Telefonzentrale `MyUMAutoAttendant` in Englisch (Großbritannien).

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -Language en-GB
```

In diesem Beispiel wird die Standardsprache für die automatische Telefonzentrale `MyUMAutoAttendant` Deutsch.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -Language de-DE
```

# Aktivieren der Aufzeichnung benutzerdefinierter Ansagen über die Benutzerschnittstelle für Telefoneingaben

18.12.2018 • 7 minutes to read

Sie können Exchange Online PowerShell verwenden, um die Aufzeichnung von benutzerdefinierten Ansagen aktivieren und Grußformeln für Unified Messaging (UM) einwählen, Wähleinstellungen und automatischen Telefonzentralen mithilfe der Benutzeroberfläche Telefon (TUI). Dies kann hilfreich sein, wenn Sie eine benutzerdefinierte Begrüßung oder Ankündigung mithilfe der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell ändern möchten, oder wenn Notfall wie eine Organisation Schließung aufgrund erheblich Wetter. Wenn Sie eine benutzerdefinierte Begrüßung oder Ankündigung auf einer automatischen UM-Telefonzentrale ändern, müssen Sie TUI Prompt Aufzeichnung für den Wählplan aktivieren, denen die automatische Telefonzentrale mit verknüpft ist.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter der "Um-Wählpläne" und "Automatische um-Telefonzentralen" Einträge im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie zum Aktivieren einer benutzerdefinierten Ansage oder die Ansage Aufzeichnung der TUI mit Exchange Online PowerShell

Befolgen Sie diese Schritte, um angepasste Ansagen und Begrüßungen über die TUI aufzuzeichnen:

1. Erstellen Sie ein Domänenbenutzerkonto, für das keine interaktive Anmeldung möglich ist.
2. Weisen Sie dem Domänenbenutzerkonto die Exchange-Organisationsadministrator-Rolle zu.
3. Erstellen Sie ein Postfach für den Domänenbenutzer.

4. Aktivieren Sie das Postfach des Domänenbenutzers für Unified Messaging.

**IMPORTANT**

Gewähren Sie nur den Administratoren, die Ansagen und Begrüßungen verwalten sollen, den Zugriff auf die Durchwahl und die PIN für das Benutzerkonto. Verwenden Sie dieses Benutzerkonto ausschließlich für die Verwaltung von Ansagen über das Telefon.

5. Erstellen und speichern Sie eine WAV- oder WMA-Datei, die für eine benutzerdefinierte Begrüßung für die UM-Wählpläne oder die automatische UM-Telefonzentrale verwendet werden soll.

**NOTE**

MP3-Dateien können für benutzerdefinierte Ansagen nicht verwendet werden.

6. Verwenden Sie die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell zum Konfigurieren der Wähleinstellungen verwenden Sie die benutzerdefinierte Begrüßung oder Konfigurieren der automatischen Telefonzentrale, um das Business oder nicht - Begrüßung während der Geschäftszeiten verwendet wird. Ausführliche Informationen zu einen Wählplan konfigurieren finden Sie [eine benutzerdefinierte Begrüßung für Outlook Voice Access-Benutzer zu aktivieren](#). Ausführliche Informationen zum Konfigurieren einer automatischen Telefonzentrale finden Sie unter [aktivieren eine benutzerdefinierte Begrüßung während der Geschäftszeit](#) oder [eine benutzerdefinierte Geschäftszeiten Begrüßung aktivieren](#).

7. Führen Sie das folgende Cmdlet aus:

```
Set-UMDialPlan -identity MyUMDialPlan -TUIPromptEditingEnabled $true
```

**NOTE**

Bevor Sie die Aufzeichnung einer benutzerdefinierten Ansage oder Begrüßung aktivieren können, müssen Sie sich bei dem Postfach anmelden, das für Ansagenaufzeichnung eingerichtet ist. Nachdem Sie die neue Ansage oder Begrüßung aufgezeichnet haben, müssen Sie sich abmelden und dann erneut anmelden, bevor Sie die neue Ansage oder Begrüßung hören können, wenn Sie die TUI verwenden.

## Aufzeichnen von TUI-Ansagen für eine automatische UM-Telefonzentrale

1. Vergewissern Sie sich, dass die automatische Telefonzentrale mit dem Wählplan verknüpft ist, den Sie für die Aufzeichnung von TUI-Ansagen aktiviert haben.
2. Rufen Sie eine Telefonnummer an, die für die automatische UM-Telefonzentrale konfiguriert wurde.
3. Drücken Sie während der Wiedergabe der Begrüßung während oder außerhalb der Geschäftszeiten durch die automatische Telefonzentrale die Taste mit dem Nummernzeichen (#) und dann die Sterntaste (\*).
4. Sie werden aufgefordert, die Durchwahlnummer des Benutzers einzugeben. Geben Sie die Durchwahlnummer des UM-aktivierten Benutzers ein, der die Berechtigung zum Aufzeichnen von TUI-Ansagen hat.
5. Sie werden zur Eingabe einer PIN aufgefordert. Geben Sie die PIN des Benutzers ein.
6. Befolgen Sie die Systemansagen, um die Begrüßung oder die Informationsansage für die automatische Telefonzentrale zu bearbeiten oder zu aktualisieren.

## Aufzeichnen von TUI-Ansagen für einen UM-Wählplan

1. Rufen Sie eine Outlook Voice Access-Nummer an, mit der Sie sich bei Outlook Voice Access anmelden.
2. Drücken Sie während der Wiedergabe der Begrüßung durch den UM-Wählplan die Taste mit dem Nummernzeichen (#) und dann die Sterntaste (\*).
3. Wenn Sie mit einem Telefon anrufen, das von einem UM-aktivierten Benutzer verwendet wird, werden Sie zur Eingabe einer PIN aufgefordert. Anstatt die PIN einzugeben, drücken Sie die Sterntaste (\*). Sie werden aufgefordert, eine Durchwahl einzugeben. Geben Sie die Durchwahlnummer des UM-aktivierten Benutzers ein, der die Berechtigung zum Aufzeichnen von TUI-Ansagen hat.
4. Wenn Sie mit einem Telefon anrufen, das nicht von einem UM-aktivierten Benutzer verwendet wird, werden Sie automatisch zur Eingabe einer Durchwahl aufgefordert. Geben Sie die Durchwahlnummer des UM-aktivierten Benutzers ein, der die Berechtigung zum Aufzeichnen von TUI-Ansagen hat.
5. Sie werden zur Eingabe einer PIN aufgefordert. Geben Sie die PIN des Benutzers ein.
6. Befolgen Sie die Systemansagen, um die Begrüßung oder die Informationsansage für den Wähler zu bearbeiten oder zu aktualisieren.

# Telefonsystemintegration mit UM

18.12.2018 • 9 minutes to read

Für die Bereitstellung eines Unified Messaging-Servers (UM) benötigen Sie ein solides Verständnis grundlegender Telefoniekonzepte und -komponenten. Nachdem Sie sich mit den Grundlagen der Telefonie vertraut gemacht haben, können Sie UM in eine Exchange-Organisation integrieren. Die grundlegenden Konzepte und Komponenten umfassen Folgendes:

- Leitungsvermittelte und paketvermittelte Netzwerke
- PBX-Anlagen (Private Branch eXchange)
- IP-PBX-Anlagen
- VoIP (Voice over Internet Protocol)
- VoIP-Gateways

In einer lokalen, Hybrid- oder Office 365-Umgebung ist das Verbinden und Konfigurieren der benötigten Telefoniekomponenten der komplexeste und wichtigste Schritt für eine erfolgreiche Bereitstellung von UM, ob mit oder ohne Lync Server Enterprise-VoIP. Für ein herkömmliches Telefonienetzwerk müssen Sie VoIP-Gateways, erweiterte VoIP-Gateways, Nebenstellenanlagen, IP-Nebenstellenanlagen und Session Border Controllers (SBCs) verbinden und konfigurieren und bei Verwenden von Microsoft Lync Server und UM mit einem Telefonienetzwerk verbinden.

Die Planung und Bereitstellung einer Neubereitstellung von UM oder ein Upgrade eines älteren Voicemailsystems kann für Organisationen mit Herausforderungen verbunden sein. Spezifische Kenntnisse zu VoIP-Gateways, Nebenstellenanlagen, IP-Nebenstellenanlagen, Microsoft Lync Server und Unified Messaging sind erforderlich. Abhängig von Ihrer technischen Erfahrung mit Exchange- und Voicemailsystmen sollten Sie möglicherweise einen Unified Messaging-Spezialisten hinzuziehen. Ein Exchange Unified Messaging-Spezialist kann einen reibungslosen Übergang von einem Legacy- oder Drittanbieter-Voicemailsystem zu Exchange Unified Messaging sicherstellen. Weitere Informationen zur Kontaktaufnahme mit einem Unified Messaging-Spezialisten finden Sie unter [Microsoft Exchange Server 2013 Unified Messaging \(UM\) Specialists](#).

```
> [!NOTE]
> Exchange Online UM support for third-party PBX systems via direct connections from customer operated SBCs
will end in July 2018. Please see the Exchange team blog [Discontinuation of support for Session Border
Controllers in Exchange Online Unified Messaging]
(https://blogs.technet.microsoft.com/exchange/2017/07/18/discontinuation-of-support-for-session-border-controllers-in-exchange-online-unified-messaging/) for more information.
```

## Integrieren Ihres Telefonienetzwerks

Unified Messaging erfordert die Integration Ihrer Exchange Server-Bereitstellung in das vorhandene Telefoniesystem oder eine Integration in Microsoft Lync Server für Ihre Organisation. Für eine erfolgreiche Bereitstellung und Verwaltung von UM-Voicemail müssen Sie die vorhandene Telefonie-Infrastruktur bzw. Microsoft Lync Server Enterprise Voice-Bereitstellung sorgfältig analysieren und die entsprechenden Planungsschritte ausführen.

### VoIP-Gateways

Wenn Sie UM in einer Exchange-Organisation bereitstellen, müssen Sie mindestens ein VoIP-Gateway installieren, bereitstellen und konfigurieren, um eine Verbindung mit den Nebenstellenanlagen in Ihrem Telefonienetzwerk

herzustellen, oder SIP-fähige (Session Initiation Protocol) Nebenstellenanlagen oder IP-Nebenstellenanlagen installieren, bereitstellen und konfigurieren.

Ein VoIP-Gateway ist ein Hardwaregerät eines Drittanbieters, das eine ältere Nebenstellenanlage mit Ihrem LAN verbindet. Das VoIP-Gateway ermöglicht der Nebenstellenanlage die Kommunikation mit den Exchange-Servern in Ihrer Organisation.

Unified Messaging basiert auf der Fähigkeit des VoIP-Gateways, TDM-Protokolle (Time Division Multiplexing) oder leitungsvermittelte Telefonieprotokolle wie ISDN oder QSIG von einer Nebenstellenanlage in IP- oder VoIP-basierte Protokolle wie SIP (Session Initiation Protocol), RTP (Realtime Transport Protocol) oder T.38 für die Faxübermittlung in Echtzeit zu übersetzen bzw. umzuwandeln. Das VoIP-Gateway ist ein integraler Bestandteil und Voraussetzung für die Funktionalität und den Betrieb von Unified Messaging. Der VoIP-Gateway kann ebenfalls an Nebenstellenanlagensysteme angeschlossen werden, die VoIP anstelle leitungsvermittelter Festnetzprotokolle verwenden.

Die Auswahl des geeigneten VoIP-Gateways, einer IP-Nebenstellenanlage, einer SIP-fähigen Nebenstellenanlage oder eines SBC ist nur der erste Schritt zur Integration der UM-Funktion in Ihr Telefoniesystem. Sie müssen diese Geräte für die Zusammenarbeit mit UM konfigurieren. Bei lokalen und Hybridbereitstellungen müssen Sie die benötigen Clientzugriffs- und Postfachserver bereitstellen sowie alle erforderlichen UM-Komponenten erstellen und konfigurieren. Für Office 365 mit gehosteter Voicemail müssen keine Server installiert und konfiguriert werden. Die Komponenten erlauben eine Verbindung zwischen Ihrem leitungsbasierten Telefonienetzwerk und Ihrem IP-Datennetzwerk, wodurch Voicemail für die Benutzer in Ihrer Organisation ermöglicht wird. Einzelheiten und unterstützte Telefoniegeräte finden Sie in den folgenden Ressourcen:

- [Telefonieratgeber für Exchange 2013](#)
- [Konfigurationshinweise zu unterstützten VoIP-Gateways, IP-Nebenstellenanlagen und Nebenstellenanlagen](#)
- [Konfigurationshinweise für unterstützte Session Border Controller](#)

## **Microsoft Lync Server**

Unified Messaging kann Microsoft Lync Server nutzen, um Sprachnachrichten, Chat, erweiterte Anwesenheitsinformationen, Audio-/Videokonferenzen und E-Mail in einer vertrauten, integrierten Kommunikationsumgebung zu kombinieren. Das Bereitstellen von Enterprise Voice-Funktionen für die Benutzer in Ihrer Organisation durch Integration von UM und Microsoft Lync Server hat die folgenden Vorteile:

- Benachrichtigungen zur erweiterten Anwesenheitskontrolle für eine Vielzahl von Anwendungen, die Benutzer über die Verfügbarkeit von Kontakten informieren.
- Integration von Chat, Sprachnachrichten, Konferenzfunktionen, E-Mail und anderen Kommunikationsmodi, mit deren Hilfe die Benutzer den für die jeweilige Aufgabe optimal geeigneten Modus auswählen können. Die Benutzer können bei Bedarf auch von einem Modus in einen anderen wechseln.
- Die Verfügbarkeit von Kommunikationsalternativen an beliebigen Standorten mit verfügbarer Internetverbindung.
- Ein intelligenter Client (Microsoft Lync) für Telefonie, Chat und Konferenzen.
- Einheitliche Benutzerfreundlichkeit über verschiedene Geräte hinweg.

Die Exchange UM-Routingkomponente übernimmt das Routing von Voicemail zwischen Lync Server und Exchange-Servern, um Lync Server mit Unified Messaging-Funktionen zu integrieren. Die Exchange UM-Routingkomponente in Lync Server übernimmt auch das erneute Routing von Voicemail über das Festnetz, wenn keine Exchange-Server verfügbar sind. Wenn Enterprise Voice an Zweigstellenstandorten bereitgestellt sind und diese Standorte keine ausfallsichere WAN-Verbindung zu einem zentralen Standort haben, stellt eine Survivable Branch Appliance, die Sie am Zweigstellenstandort bereitstellen, Voicemail für die Benutzer der Zweigstelle bereit, sollte eine WAN-Verbindung ausfallen. Wenn die WAN-Verbindung nicht verfügbar ist, führt die Survivable

Branch Appliance folgende Aufgaben aus:

- Erneutes Routing nicht beantworteter Anrufe über das Festnetz zu einem Exchange-Server am zentralen Standort.
- Bereitstellen der Fähigkeit, dass Benutzer Sprachnachrichten über das Festnetz abrufen können.
- Einreihen von Benachrichtigungen über verpasste Anrufe in eine Warteschlange und deren anschließendes Hochladen auf den Exchange-Server, wenn die WAN-Verbindung wieder besteht.

Weitere Informationen zu Microsoft Lync Server finden Sie unter [Microsoft Lync Server](#).

**Caution**

Wenn Sie Unified Messaging und Lync Server in einer lokalen oder Hybridbereitstellung integrieren, stehen Benachrichtigungen über verpasste Anrufe Benutzern nicht zur Verfügung, die über ein Postfach auf einem Exchange 2007- oder Exchange 2010-Postfachserver verfügen. Es wird eine Benachrichtigung über einen verpassten Anruf generiert, wenn ein Benutzer sich abmeldet, bevor der Anruf an einen Postfachserver gesendet wurde.

# Telefonieratgeber für Exchange 2013

18.12.2018 • 19 minutes to read

Unified Messaging (UM) erfordert die Integration von Microsoft Exchange mit dem vorhandenen Telefoniesystem Ihrer Organisation. Für eine erfolgreiche Bereitstellung und die Durchführung der richtigen Planungsschritte für die Bereitstellung von Unified Messaging ist eine sorgfältige Analyse Ihrer vorhandenen Telefonieinfrastruktur erforderlich.

Die Planungsphase möglicherweise eine erhebliche Herausforderung für Exchange Administratoren mit geringer oder ohne mit einem Telefonienetzwerk auftreten. Dieses Problem bereits lösen, finden Sie im folgenden Abschnitt **Ressourcen, die mit der UM-Bereitstellung unterstützen**.

In den anderen Abschnitten in diesem Thema werden die unterstützten VoIP-Gateways für Unified Messaging behandelt, wie Sie bestimmen, ob der Nebenstellenanlage unterstützt wird mit einem bestimmten VoIP-Gateway-Modell oder Hersteller, ob der IP-Nebenstellenanlage unterstützt wird mit einer direkten SIP-Verbindung und unterstützt Session Border Controller (SBCs) für Exchange Online UM.

## Hilferessourcen für die UM-Bereitstellung

Das Erstellen von Richtlinien für die Bereitstellung von Telefonienetzwerken stellt eine Herausforderung dar. Da diese Netzwerke VoIP-Gateways, IP-Nebenstellenanlagen und Nebenstellenanlagen mit unterschiedlichen Konfigurationseinstellungen und Anforderungen oder unterschiedlicher Firmware umfassen können, sind große Unterschiede möglich. Es sind jedoch zahlreiche Ressourcen verfügbar, die Ihnen bei einer erfolgreichen Bereitstellung von Unified Messaging behilflich sein können:

- **Unified Messaging-Experten:** UM Spezialisten sind Systemintegratoren, die technischen Schulungen zu Exchange Unified Messaging von Exchange-Entwicklungsteams durchgeführt erhalten haben. Um einen reibungslosen Übergang zu Unified Messaging aus älteren Voicemail-Systemen zu gewährleisten, empfiehlt es sich, dass alle Kunden ausschließlich für einen UM-Spezialisten zu Kontaktinformationen finden Sie auf [Microsoft Exchange Server 2013 Unified Messaging \(UM\)-Experten](#) oder [Microsoft Hindernissen bei für Unified Messaging](#).
- **Konfigurationshinweise für unterstützte VoIP-Gateways, IP-PBX-Anlagen und PBX-Anlagen:** Diese Konfigurationshinweise enthalten, Einstellungen und andere Informationen, die sehr nützlich ist, wenn Sie VoIP-Gateways, IP-PBX-Anlagen und PBX-Anlagen zum Kommunizieren mit Unified Messaging konfigurieren Server, die in Ihrem Netzwerk sind. Weitere Informationen finden Sie unter [Konfigurationshinweise für unterstützte VoIP-Gateways, IP-Nebenstellenanlagen und PBX-Anlagen](#).
- **Konfigurationshinweise für unterstützte Session Border Controller:** Diese Konfigurationshinweise enthalten, Einstellungen und andere Informationen, die sehr nützlich ist, wenn Sie Session Border Controller (SBCs) kommunizieren mit Unified Messaging konfigurieren Server in Hybrid und Exchange Online UM-Bereitstellungen. Weitere Informationen finden Sie unter [Konfigurationshinweise für unterstützte Session Border Controller](#).

### NOTE

Exchange Online UM Unterstützung für Drittanbieter-Nebenstellenanlage Systeme über direkte Verbindungen von Kunden betrieben SBCs werden im Juli 2018 beendet. Weitere Informationen finden Sie im Exchange-Teamblog [die Einstellung der Unterstützung für Session Border Controller in Exchange Online unified messaging](#) für Weitere Informationen.

Bevor Sie einen Unified Messaging-Spezialisten engagieren, sollten Sie in der Lage sein, die wichtigsten Fragen zu beantworten, die dieser Ihnen stellen wird. Wenn Sie die Antworten auf die folgenden Fragen kennen, wird dies die Produktivität Ihrer Unterhaltung mit dem UM-Spezialisten steigern.

- Wie viele Telefon- bzw. Voicemailbenutzer befinden sich bereits in Ihrer Organisation?
- Für wie viele Benutzer möchten Sie Unified Messaging bereitstellen?
- Welche Nebenstellenanlagen (PBX) sollen für die Integration mit Unified Messaging verwendet werden?
- Über wie viele PBX-Anlagen verfügt Ihre Organisation? Geben Sie hierbei auch die Anbieter, Typenbezeichnungen (leitungsvermittelt oder IP-basiert), Modellbezeichnungen und Firmwareversionen an.
- Sind die PBX-Anlagen vernetzt, und sind sie zentralisiert, oder befinden sie sich an mehreren Orten?
- Welche Voicemailsysteme werden zurzeit in Ihrer Organisation verwendet? Geben Sie hierbei auch die Anbieter, Typenbezeichnungen, Modellbezeichnungen und Firmwareversionen an.
- Wie sind die Voicemailsysteme in Ihre PBX-Anlagen integriert (Analog, T1/E1, PRI, Digital Set Emulation, VoIP oder anders)?
- Verwenden Sie zurzeit Sprachnetzwerke?
- Welche Typen von Faxsystemen werden in Ihrer Organisation verwendet, und unterstützen die Faxsysteme eingehendes Faxrouting an Exchange?
- Verwendet Ihre Organisation automatische Telefonzentralen?
- Benötigen Sie Unterstützung für reine Telefonbenutzer, d. h. Benutzer die keinen E-Mail-Zugriff haben?

## Unterstützte VoIP-Gateways

Für die Integration von Unified Messaging mit Nebenstellenanlagen ist der Einsatz von mindestens einem VoIP-Gateway erforderlich, um die von TDM-basierten Nebenstellenanlagen verwendeten leitungsvermittelten Protokolle in IP-basierte, paketvermittelte Protokolle zu übersetzen, die von Unified Messaging verwendet werden. Es wurden Anbieter mit mehreren Modellen von VoIP-Gateways getestet, die für Unified Messaging unterstützt werden.

Das Testen der Interoperabilität von Unified Messaging mit VoIP-Gateways, IP-Nebenstellenanlagen und SBCs wurde in das Microsoft Unified Communications Open Interoperability Program integriert. Weitere Informationen hierzu finden Sie unter [Microsoft Unified Communications Open Interoperability Program](#).

Das Qualifizierungsprogramm für IP-Gateways, IP-Nebenstellenanlagen und erweiterte VoIP-Gateways gemäß dem [Microsoft Unified Communications Open Interoperability Program](#) gewährleistet Kunden eine nahtlose Setup- und Unterstützungserfahrung, wenn sie qualifizierte VoIP-Telefoniegateways und IP-Nebenstellenanlagen mit Microsoft Unified Communications-Software verwenden. Nur Produkte, die strenge und umfassende Testanforderungen erfüllen und die Spezifikationen und Testpläne einhalten, erhalten die Qualifizierung.

Einzelheiten zum Konfigurieren von unterstützten VoIP-Gateways, IP-Nebenstellenanlagen, Nebenstellenanlagen und SBCs finden Sie in den folgenden Ressourcen:

- [Konfigurationshinweise zu unterstützten VoIP-Gateways, IP-Nebenstellenanlagen und Nebenstellenanlagen](#)
- [Konfigurationshinweise für unterstützte Session Border Controller](#)

Interoperabilität wurde für die folgenden Anbieter von VoIP-Gateways bestätigt:

- AudioCodes

- Dialogic
- In der folgenden Tabelle sind der VoIP-Gatewayanbieter, das IP-Gatewaymodell und die von jedem Modell unterstützten Protokolle aufgeführt.

### **Unterstützte VoIP-Gateways für Unified Messaging**

ANBIETER	MODELL	UNTERSTÜTZTE PROTOKOLLE
AudioCodes	MediaPack 114/8 FXO	Analog mit In-Band oder DTMF Analog mit SMDI
AudioCodes	Mediant 1000	Analog mit In-Band oder DTMF Analog mit SMDI BRI Q.SIG T1/E1 Q.SIG IP-zu-IP
AudioCodes	Mediant 2000	T1/E1 CAS T1/E1 Q.SIG IP-zu-IP
Dialogic	DMG1000PBXDNIW	Digital Set Emulation
Dialogic	DMG1000LSW	Analog mit In-Band oder DTMF Analog mit SMDI
Dialogic	DMG2000	T1 CAS T1/E1 Q.SIG
Dialogic	DMG3000	BRI Q.SIG
NET	VX1200	T1 Q.SIG
Sonus	SBC 1000/2000 2.2.1 oder höher	TDM-Signal (ISDN): AT&T 4ESS/5ESS, Nortel DMS- 100, Euro ISDN (ETSI 300-102), QSIG, NTT InsNet (Japan), ANSI National ISDN-2 (NI-2) TDM-Signalisierung (CAS): T1-CAS (E & M, Schleife Start) E1-CAS (R2)
Quintum	Tenor DX-Reihe	T1 Q.SIG

### **Unterstützte Nebenstellenanlagen bei Verwendung eines VoIP-Gateways von AudioCodes**

In der folgenden Tabelle sind die Nebenstellenanlagen aufgeführt, die für die Verwendung mit VoIP-Gateways von AudioCodes unterstützt werden, einschließlich der Modelle MediaPack-114 FXO, MediaPack-118 FXO und Mediant 2000.

#### **Mit einem VoIP-Gateway von AudioCodes unterstützte Nebenstellenanlagen**

PBX-HERSTELLER	PBX-MODELL/-TYP	AUDIOCODES-MODELL "X" - NACH BEDARF DURCH 4 ODER 8 ERSETZEN "Y"- NACH BEDARF DURCH 1, 2, 4, 8 ODER 16 ERSETZEN
Alcatel	OmniPCX 4400	MediaPack 11x/FXO/AC/SIP-0 Mediant2000/ySpans/SIP
Aastra	M1000, M2000	Mediant2000/ySpans/SIP
Avaya	Definity G3	MediaPack 11x/FXO/AC/SIP-0 Mediant1000/ySpans/SIP Mediant2000/ySpans/SIP
Avaya	Magix/Merlin	MediaPack 11x/FXO/AC/SIP-0
Avaya	S8300	MediaPack 11x/FXO/AC/SIP-0 Mediant1000/ySpans/SIP Mediant2000/ySpans/SIP
Avaya	S8700	MediaPack 11x/FXO/AC/SIP-0 Mediant1000/ySpans/SIP Mediant2000/ySpans/SIP
Avaya	IP Office	MediaPack 11x/FXO/AC/SIP-0 Mediant2000/ySpans/SIP
Cisco	CallManager 4.x	Mediant1000/IP-zu-IP Mediant2000/IP-zu-IP
NEC	Electra Elite	MediaPack 11x/FXO/AC/SIP-0
NEC	NEAX2400	MediaPack 11x/FXO/AC/SIP-0 Mediant2000/ySpans/SIP/RS232
NeXspan	S	MediaPack 11x/FXO/AC/SIP-0
Nortel	Communication Server-1000M, 1000S, 1000E	Mediant1000/ySpans/SIP Mediant2000/ySpans/SIP
Nortel	Meridian 11c, 51c, 61c, 81c	Mediant1000/ySpans/SIP Mediant2000/ySpans/SIP
Panasonic	KX-TES824, KX-TEA308	MediaPack 11x/FXO/AC/SIP-0
Panasonic	KX-TDA30, KX-TDA100, KX-TDA200, KX-TDA600	MediaPack 11x/FXO/AC/SIP-0
Shortel	IP-Telefoniesystem	MediaPack 11x/FXO/AC/SIP-0
Siemens	HiCom 150E	MediaPack 11x/FXO/AC/SIP-0
Siemens	HiPath 3550	MediaPack 11x/FXO/AC/SIP-0

PBX-HERSTELLER	PBX-MODELL/-TYP	AUDIOCODES-MODELL "X" - NACH BEDARF DURCH 4 ODER 8 ERSETZEN "Y"- NACH BEDARF DURCH 1, 2, 4, 8 ODER 16 ERSETZEN
Siemens	HiPath 4000	MediaPack 11x/FXO/AC/SIP-0 Mediant1000/ySpans/SIP Mediant2000/ySpans/SIP
Tadiran Telecom	Coral Flexicom, Coral IPX	MediaPack 11x/FXO/AC/SIP-0 Mediant1000/ySpans/SIP Mediant2000/ySpans/SIP

## Unterstützte Nebenstellenanlagen bei Verwendung eines VoIP-Gateways von Dialogic

Jedes VoIP-Gatewaymodell von Dialogic unterstützt verschiedene Nebenstellenanlagen. In den folgenden Tabellen sind die Hersteller und das Modell von Nebenstellenanlagen sowie das jeweils verwendbare VoIP-Gateway von Dialogic aufgeführt. Jedes VoIP-Gateway verwendet unterschiedliche Signalmethoden, -dichten und -protokolle.

### Unterstützte Nebenstellenanlagen bei Verwendung eines Mediengateways der DMG1000-Serie

In der folgenden Tabelle werden die PBX-Anlagen aufgeführt, die mit dem Mediengateway mit niedriger Dichte von Dialogic (DMG1000) unterstützt werden. Wenn aber ein analoger DMG1000 verwendet wird, ist ergänzende Signalgebung (RS232 SMDI, MD110, MCI-Protokolle oder In-Band-DTMF-Signalgebung) erforderlich.

### Für die Verwendung mit VoIP-Gateways der Dialogic DMG1000-Serie mit niedriger Dichte unterstützte Nebenstellenanlagen

PBX-HERSTELLER	PBX-MODELL/-TYP	DMG-MODELL UND ZUSÄTZLICHE SIGNALGEBUNG
Aastra	Aastra MD110 (früher Ericsson MD110)	DMG1008LSW Analogverbindung unter Verwendung des MD110 RS232-Protokolls
Alcatel	Omni PCX 4400	DMG1008LSW
Avaya	Definity G3 S8100, S8300, S8700 und S8710 (Communications Mgr SW V2.0 oder höher)	DMG1008DNIW
Intercom		DMG1008LSW Analogverbindung unter Verwendung des seriellen SMDI-Protokolls
Mitel	SX-200D, SX-200 Light, SX-2000 Light, SX-2000 S, SX-2000 VS, SX-200 ICP	DMG1008MTLDNIW
NEC	2000, 2400, 2400 IPX	DMG1008DNIW

PBX-HERSTELLER	PBX-MODELL/-TYP	DMG-MODELL UND ZUSÄTZLICHE SIGNALGEBUNG
Nortel	Meridian 1 - Option 11, 21, 21A, 51, 61, 71 und 81 Meridian SL1 - Generic X11, Version 15 oder höher Nortel Communication Server - 1000M, 1000S, 1000E mit V3.0 oder höher	DMG1008DNIW
Nortel	SL 100	DMG1008LSW Analogverbindung unter Verwendung des seriellen SMDI-Protokolls
Siemens	HiCom 300E CS	DMG1008DNIW
Siemens	HiCom 300E (Europa)	DMG1008LSW Analogverbindung unter Verwendung der In-Band-DTMF-Signalgebung
Siemens/ROLM	8000 (SW-Version 80003 oder höher) 9000 (alle Versionen) 9751 (alle Versionen von SW-Version 9005) 9751 (SW-Version 9006.4 oder höher)	DMG1008RLMDNIW
Siemens	HiPath 4000	DMG1008LSW
Toshiba	CTX (SW-Version AR1ME021.00)	DMG1008LSW
Sonstige	Verschiedene	DMG1008LSW Analogverbindung unter Verwendung von entweder In-Band-DTMF oder SMDI

#### Unterstützte Nebenstellenanlagen bei Verwendung eines Mediengateways der DMG2000-Serie

In der folgenden Tabelle werden die PBX-Anlagen aufgeführt, die mit dem T1/E1-Mediengateway von Dialogic (DMG2000) unterstützt werden. Das DMG2000-Gateway, das es in den Dichteausführungen Single-Span (DMG2030DTIQ), Dual-Span (DMG2060DTIQ) und Quad-Span (DMG2120DTIQ) gibt, unterstützt folgende Protokolle:

- T1 CAS
- T1 Q.SIG
- E1 Q.SIG
- T1 NI-2
- T1 5ESS
- T1 DMS100

Wenn CAS-Signalgebung (Channel Associated Signaling) verwendet wird, ist ergänzende Signalgebung (RS232 SMDI, MD110, MCI-Protokolle oder In-Band-DTMF-Signalgebung) erforderlich. Wenn Q.SIG-Signalgebung verwendet wird, muss die Nebenstellenanlage die Ergänzungsdienste unterstützen, die mit Informationen über den anrufenden und angerufenen Teilnehmer in Verbindung stehen, sowie die Anrufvermittlungsfunktionen, die für Unified Messaging erforderlich sind.

## Mit dem DMG2000-Mediengateway unterstützte PBX-Anlagen

PBX-HERSTELLER	PBX-MODELL/-TYP	ERFORDERLICHE SOFTWAREVERSION	PROTOKOLL UND ZUSÄTZLICHE SIGNALGEBUNG
Alcatel	Omni PCX 4400	Version 3.2.712.5	T1 Q.SIG E1 Q.SIG
Avaya	Definity G3	Version 3 oder höher	T1 CAS
Avaya	S8500	Manager SW V2.0 oder höher	T1 CAS T1 Q.SIG E1 Q.SIG
Ericsson	MD110	Version MX1 TSW R2A (BC13)	E1 Q.SIG
Intercom			CAS (mit seriellem SMDI-Protokoll)
NEC	2400 IMX	Release 5200 Dez. 92 1b oder nachfolgende Versionen	CAS (mit seriellem MCI-Protokoll)
NEC	2400 IPX	R17 Version 03.46.001	T1 Q.SIG
Nortel	Meridian 1 - Option 11	Release 15 oder nachfolgende Versionen und Optionen 19 und 46 sind erforderlich	T1 Q.SIG E1 Q.SIG
Nortel	Communication Server 1000	Version 2121, Release 4	T1 Q.SIG E1 Q.SIG
Siemens	HiCom 300E CS	Version 9006.4 oder höher (Hinweis: Nur nordamerikanische Software)	T1 CAS
Siemens	HiPath 4000	V2 SMR 9 SMPO	T1 Q.SIG E1 Q.SIG
Mitel	SX-2000 S, SX-2000 VS	LW 34	T1 Q.SIG E1 Q.SIG
Mitel	3300	Version 5.1.4.8	T1 Q.SIG E1 Q.SIG

## Unterstützte Nebenstellenanlagen bei Verwendung eines Mediengateways der DMG4008BRI-Serie

Die Mediengateways der DMG4000-Serie bieten mehrere TDM-Schnittstellenoptionen. DMG4008BRI unterstützt 4-Port/8-Kanal dichten und unterstützt die folgenden Protokolle:

- ISDN BRI Q.SIG
- ETSI-DSS1 (Euro ISDN)
- NET 3 (Belgien)

- VN3 (Frankreich)
- 1TR6 (Deutschland)
- INS-64 (Japan)
- 5ESS Custom (Nordamerika - AT&T)
- National ISDN (NI1 - Nordamerika)

In der folgenden Tabelle werden die PBX-Anlagen aufgeführt, die für die Verwendung mit einem Mediengateway der Dialogic 4000-Serie (DMG4008) unterstützt werden.

#### **Unterstützte PBX-Anlagen bei Verwendung eines Mediengateways der DMG4008BR-Serie**

PBX-HERSTELLER	PBX-MODELL/-TYP	ERFORDERLICHE SOFTWAREVERSION	PROTOKOLL UND ZUSÄTZLICHE SIGNALGEBUNG
Siemens	HiCom 300	SA300 V3.05	BRI-Q.SIG (ECMAV2)
Siemens	HiPath 4000	S.0 B4400	BRI-Q.SIG (ECMAV2)

## Unterstützte IP-PBX-Anlagen

IP-Nebenstellenanlagen werden ebenfalls von Unified Messaging unterstützt. In der folgenden Tabelle werden die IP-Nebenstellenanlagen aufgeführt, die für die Verwendung einer direkten SIP-Verbindung mit Unified Messaging unterstützt werden.

#### **Für die Verwendung einer direkten SIP-Verbindung unterstützte IP-Nebenstellenanlagen**

PBX-HERSTELLER	PBX-MODELL/-TYP	ERFORDERLICHE SOFTWAREVERSION
Aastra	MX-ONE	4.0
Avaya	Aura	5.2.1 mit Servicepack 5 (SP5)
Avaya	Communication Server 2100	CS2100 SE13
Cisco	Call Manager, Unified Communications Manager	5.1, 6.x, 7.0 and8.0

## Für die Verwendung von SIP-Mediengateways unterstützte IP-Nebenstellenanlagen

IP-Nebenstellenanlagen, die SIP-Mediengateways verwenden, werden ebenfalls von Unified Messaging unterstützt. In der folgenden Tabelle sind die IP-Nebenstellenanlagen aufgeführt, die für die Verwendung von IP-zu-IP-Funktionen von SIP-Mediengateways zum Herstellen einer Verbindung mit Unified Messaging unterstützt werden.

#### **Für die Verwendung von SIP-Mediengateways unterstützte IP-Nebenstellenanlagen**

PBX-HERSTELLER	PBX-MODELL/-TYP	SIP-GATEWAYMODELL
Cisco	Call Manager 4.x	AudioCodes Mediant 1000/2000 (IP-zu-IP-fähig)

## Exchange Unified Messaging, Office Communications Server 2007 R2 und Microsoft Lync Server

Bei lokalen und Hybridbereitstellungen kann Exchange Unified Messaging zusammen mit Microsoft Office Communications Server 2007 R2, Microsoft Lync Server 2010 oder Lync Server 2013 bereitgestellt werden, um Benutzern in Ihrer Organisation Sprachnachrichten, Chatfunktionen, erweiterte Anwesenheitsinformationen, Audio-/Videokonferenzen sowie integrierte E-Mail- und Messagingfunktionen zur Verfügung zu stellen. Weitere Informationen finden Sie unter:

- [Integrieren von Exchange 2013 UM with Lync Server](#)
- [Microsoft Lync Server 2013](#)

Weitere Informationen zum Microsoft Unified Communications Open Interoperability Program für Unternehmenstelefonieinfrastrukturen, einschließlich einer Auflistung der qualifizierten SIP-Festnetzgateways und IP-Nebenstellenanlagen sowie einer Beschreibung des Prozesses zur Teilnahme an diesem Programm für Telefonieinfrastrukturanbieter finden Sie unter [Microsoft Unified Communications Open Interoperability Program](#).

# Konfigurationshinweise zu unterstützten VoIP-Gateways, IP-Nebenstellenanlagen und Nebenstellenanlagen

18.12.2018 • 13 minutes to read

Auf dieser Seite finden Sie Links zu Konfigurationshinweisen, die von Microsoft oder einem Partner für VoIP-Gateways erstellt und getestet wurden. Wenn Microsoft oder ein Partner Unified Messaging mit einem neuen VoIP-Gateway und einer Konfiguration aus Nebenstellenanlage oder IP-Nebenstellenanlage bereitstellt, werden die Voraussetzungen und Konfigurationseinstellungen dokumentiert. Diese Informationen werden zum Erstellen von Konfigurationshinweisen verwendet.

Jeder Konfigurationshinweis für Nebenstellenanlagen enthält Informationen darüber, wie Unified Messaging mit einer bestimmten Telefoniekonfiguration bereitgestellt wird, einschließlich Hersteller, Modell und Firmwareversion für die VoIP-Gateways, IP-Nebenstellenanlagen oder Nebenstellenanlagen. Darüber hinaus enthält jeder Konfigurationshinweis für PBX-Anlagen weitere Informationen, z. B.:

- Beteiligte Autoren des Konfigurationshinweises.
- Detaillierte Voraussetzungen, einschließlich der folgenden:
  - Funktionen, die in der PBX-Anlage aktiviert bzw. deaktiviert werden müssen.
  - Spezielle Hardware, die installiert werden muss.
  - Ob ein VoIP-Gateway erforderlich ist.
  - Funktionen, über die das VoIP-Gateway verfügen muss, falls eines erforderlich ist.
  - Spezielle Verkabelungs-/Anschlussanforderungen zwischen IP-Gateway und PBX-Anlage.
  - Eine Liste der Unified Messaging-Funktionen, die mit einer vorgegebenen Telefoniekonfiguration möglicherweise nicht verfügbar sind.

Weitere Informationen zum Microsoft Unified Communications Open Interoperability Program für Telefonieinfrastrukturen in Unternehmen, einschließlich einer Liste qualifizierter SIP-PSTN-Gateways und IP-Nebenstellenanlagen, sowie zum Registrierungsprozess für Telefonieinfrastrukturanbieter, die an diesem Programm teilnehmen möchten, finden Sie unter [Microsoft Unified Communications Open Interoperability Program](#).

## Konfigurationshinweise für VoIP-Gateways, IP-PBX- und PBX-Anlagen

Microsoft arbeitet mit den Partnern für VoIP-Gateways AudioCodes und Dialogic zusammen, um die Liste von getesteten Nebenstellenanlagen zu erweitern. Da zurzeit zahlreiche Kombinationen von Telefoniekomponenten getestet werden, wird dieses Thema regelmäßig aktualisiert. Überprüfen Sie wiederholt diese Seite, wenn Sie den erforderlichen Konfigurationshinweis für Ihre Bereitstellung nicht finden können.

**Aastra**

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEI DOWNLOAD
Aastra MD110 (früher Ericsson MD110)	MX1 TSW R2A (alternative Bezeichnung: BC13)	Analog - Seriell MD110	Dialogic	DMG1008LSW	Dialogic	<a href="#">Herunterladen</a>
Aastra MD110 (früher Ericsson MD110)	MX1 TSW R2A (alternative Bezeichnung: BC13)	E1 Q.SIG	Dialogic	DMG2030DTIQ	Dialogic	<a href="#">Herunterladen</a>
Aastra MX-ONE	4.0	Direkte SIP-Verbindung	ENTFÄLLT	ENTFÄLLT	Aastra	<a href="#">Download</a>

## Alcatel

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEI DOWNLOAD
OmniPCX 4400	R4.2-D2.304-4-h-IL-c6s2	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>

## Avaya

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEI DOWNLOAD
Aura	Communication Manager 5.2.1 mit SP 5 Session Manager 5.2.	Direkte SIP-Verbindung	ENTFÄLLT	ENTFÄLLT	Avaya	<a href="#">Download</a>
CS 2100	CS 2100 SE13	Direkte SIP-Verbindung	ENTFÄLLT	ENTFÄLLT	Avaya	<a href="#">Herunterladen</a>
Definity G3	R009i.05.122.4	Digital Set Emulation (DNI7434)	Dialogic	DMG1008DN IW	Dialogic	<a href="#">Herunterladen</a>
Definity G3	R013i.01.1.62 8.7	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
Definity G3	R013i.01.1.62 8.7	T1 CAS - In-Band-DTMF	AudioCodes	Mediant 2000	AudioCodes	<a href="#">Herunterladen</a>
Definity G3	R013i.01.1.62 8.7	T1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	<a href="#">Herunterladen</a>
Definity G3	R013i.01.1.62 8.7	E1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	<a href="#">Herunterladen</a>

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
Merlin Magix	Version 1.5 v.6.0	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
S8300	G3xV11 Communication Manager 1.3	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
S8300	R013x.01.2.63 2.1	T1 CAS - In-Band-DTMF	AudioCodes	Mediant 2000	AudioCodes	<a href="#">Herunterladen</a>
S8300	R013x.01.2.63 2.1	E1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	<a href="#">Herunterladen</a>
S8500	Communication Manager 3.0 (R013x00.1.34 6.0)	E1 Q.SIG	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>
S8500	Communication Manager 3.0 (R013x00.1.34 6.0)	T1 CAS - In-Band-DTMF	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>
S8500	Communication Manager 3.0 (R013x00.1.34 6.0)	T1 Q.SIG	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>
S8700	R011x.02.0.11 0.4	E1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	<a href="#">Herunterladen</a>

## Cisco

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
Cisco Call Manager 4.x	4.x	IP-zu-IP	AudioCodes	AudioCodes	AudioCodes	<a href="#">Herunterladen</a>
Cisco Call Manager 5.1	5.1.0.9921-12	Direkte SIP-Verbindung	ENTFÄLLT	ENTFÄLLT	Microsoft	<a href="#">Herunterladen</a>
Cisco Unified Communications Manager 6.0 und 6.1	6.x	Direkte SIP-Verbindung	ENTFÄLLT	ENTFÄLLT	Microsoft	<a href="#">Herunterladen</a>

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
Cisco Unified Communications Manager 7.0	7.0.2.20000-5	Direkte SIP-Verbindung	ENTFÄLLT	ENTFÄLLT	Microsoft	<a href="#">Herunterladen</a>
Cisco Unified Communications Manager 8.0	8.0.3.20000-5	Direkte SIP-Verbindung	ENTFÄLLT	ENTFÄLLT	Microsoft	<a href="#">Herunterladen</a>

### Inter-Tel

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
5000	Inter-Tel 5000 v2.1	T1 CAS - In-Band-DTMF	AudioCodes	Mediant 2000	AudioCodes	<a href="#">Herunterladen</a>
Axxess	Axxess V9.0	T1 CAS - In-Band-DTMF	AudioCodes	Mediant 2000	AudioCodes	<a href="#">Herunterladen</a>

### Intecom

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
PointSpan M6880	40PS3.5.K.2	T1 CAS - SMDI	AudioCodes	Mediant 2000	AudioCodes	<a href="#">Herunterladen</a>

### Mitel

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
3300	5.1.4.8	E1 Q.SIG	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>
3300	5.1.4.8	T1 Q.SIG	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>
SX2000	5.0.24	Digital Set Emulation (DNISS430)	Dialogic	DMG1008MT LDNIW	Dialogic	<a href="#">Herunterladen</a>
3300	7	T1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	<a href="#">Herunterladen</a>

### NEC

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
Electra Elite 192	SP034V4.5	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
NEAX2400IM X	Version 7400	T1 CAS - Seriell MCI	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>
NEAX2400IM X & IPX	Version 7400	Digital Set Emulation (DNIDtermIII)	Dialogic	DMG1008DN IW	Dialogic	<a href="#">Herunterladen</a>
NEAX2400IPX	Ver. R18.06.24.00 0	T1 CAS - Seriell MCI	AudioCodes	Mediant 2000	AudioCodes	<a href="#">Herunterladen</a>
NEAX2400IPX	Ver. R18.06.24.00 0	Analog - Seriell MCI	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
NEAX2400IPX	Ver.17 Rel.03.46.001	T1 Q.SIG - Seriell MCI	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>

### NeXspan

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
L	RMS1 Version R1.3 E1TA	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>

### Nortel

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
CS1000	3.0 & 4.5	E1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	<a href="#">Herunterladen</a>
Meridian 81C	4.5	E1 Q.SIG	AudioCodes	Mediant 2000	AudioCodes	<a href="#">Herunterladen</a>
Meridian 81C	4.5	T1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	<a href="#">Herunterladen</a>
Option11c	Version 25	Digital Set Emulation (DNI2616)	Dialogic	DMG1008DN IW	Dialogic	<a href="#">Herunterladen</a>
Option11c	Version 25	T1 Q.SIG	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>
Option11c	Version 25	E1 Q.SIG	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
CS-1000M (Nachfolger)	Version 25.40	E1 Q.SIG	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>

### Panasonic

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
KX-TDA200	001-001	Analog - In-Band-DTMF	AudioCodes	Mediant 1000	AudioCodes	<a href="#">Herunterladen</a>
KX-TDA200	3	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
KX-TES824	2.0.2	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>

### Rolm

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
9751	9005	Digital Set Emulation (DNIRP400)	Dialogic	DMG1008RL MDNIW	Dialogic	<a href="#">Herunterladen</a>

### ShoreTel

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
IP-Telefonesystem	6.1	Analog - SMDI	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
IP-Telefonesystem	7.5	Analog - SMDI	AudioCodes	Mediant 1000	AudioCodes	<a href="#">Herunterladen</a>

### Siemens

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
HiCom 150E	Vers. 2.2	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
HiCom 300	SA300 V3.05	BRI QSIG	Dialogic	DMG3000	Dialogic	<a href="#">Herunterladen</a>

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
HiCom 300	9006.4SMR3	Digital Set Emulation (DNIOptiset)	Dialogic	DMG1008DN IW	Dialogic	<a href="#">Herunterladen</a>
HiCom 300	9006.4SMR3	T1 CAS - In-Band-DTMF	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>
HiPath 3550	Vers. 3	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
HiPath 4000	Ver 3.0 SMR5 SMP4	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
HiPath 4000	SA300 V3.05	BRI QSIG	Dialogic	DMG3000	Dialogic	<a href="#">Herunterladen</a>
HiPath 4000	Ver 3.0 SMR5 SMP4	T1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	<a href="#">Herunterladen</a>
HiPath 4000	Version 2.0 SMR9 SMP0	Analog - In-Band-DTMF	Dialogic	DMG1008LS W	Dialogic	<a href="#">Herunterladen</a>
HiPath 4000	Version 2.0 SMR9 SMP0	T1 Q.SIG	Dialogic	DMG2030DTI Q	Dialogic	<a href="#">Herunterladen</a>

## Sonus

VOIP-GATEWAYMODELL	VOIP-GATEWAYSOFTWAREVERSION	UNTERSTÜTZTE PROTOKOLLE	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDownload
SBC 1000/2000	2.2.1 oder höher	TDM-Signal (ISDN): AT&T 4ESS/5ESS, Nortel DMS- 100, Euro ISDN (ETSI 300-102), QSIG, NTT InsNet (Japan), ANSI National ISDN-2 (NI-2) TDM-Signalisierung (CAS): T1-CAS (E & M, Schleife Start) E1-CAS (R2)	Sonus	<a href="#">Download</a>

## Tadiran

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
Coral Flexicom	14.67.49	Analog - In-Band-DTMF	AudioCodes	MP 11x FXO	AudioCodes	<a href="#">Herunterladen</a>
Coral Flexicom	14.67.49	BRI QSIG	AudioCodes	Mediant 1000	AudioCodes	<a href="#">Herunterladen</a>

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
Coral Flexicom	14.67.49	E1 CAS - In-Band-DTMF	AudioCodes	Mediant 2000	AudioCodes	<a href="#">Herunterladen</a>
Coral Flexicom	14.67.49	E1 Q.SIG	AudioCodes	Mediant 1000/2000	AudioCodes	<a href="#">Herunterladen</a>
Coral IPX	14.67.49	Analog - In-Band-DTMF	AudioCodes	MP-11x FXO	AudioCodes	<a href="#">Herunterladen</a>
Coral IPX	14.67.49	BRI QSIG	AudioCodes	Mediant 1000	AudioCodes	<a href="#">Herunterladen</a>
Coral IPX	14.67.49	E1 CAS - In-Band-DTMF	AudioCodes	Mediant 2000	AudioCodes	<a href="#">Herunterladen</a>
Coral IPX	14.67.49	E1 QSIG	AudioCodes	Mediant 1000/2000	AudioCodes	<a href="#">Herunterladen</a>

### Toshiba

PBX-MODELL	PBX-SOFTWAREVERSION	PROTOKOLL	GATEWAYANBIETER	GATEWAYMODELL	KONFIGURATIONSAUTOR	KONFIGURATIONSDATEIDOWNLOAD
CTX	AR1ME021.00	Analog - SMDI	Dialogic	DMG1008LSW	Dialogic	<a href="#">Herunterladen</a>
CTX	AR1ME021.00	Analog - In-Band-DTMF	Dialogic	DMG1008LSW	Dialogic	<a href="#">Herunterladen</a>

# Konfigurationshinweise für unterstützte Session Border Controller

18.12.2018 • 5 minutes to read

Session Border Controller (SBCs) ermöglichen das Verbinden Ihres lokalen Telefonienetzwerks mit einem Microsoft-Datencenter über eine dedizierte öffentliche WAN-Verbindung. Ein SBC befindet sich am Rand Ihres lokalen IP-Netzwerks und verbindet sich mit einem zweiten SBC in einem Microsoft-Datencenter.

Für SBCs müssen digitale Zertifikate verwendet werden, um den gesamten Datenverkehr zwischen der lokalen Organisation und dem Microsoft-Datencenter zu verschlüsseln. Sie müssen ein digitales Zertifikat für das Netzwerkrandelement (z. B. Session Border Controller) beziehen, das Sie für die Kommunikation mit Hybrid- und Onlinebereitstellungen von Exchange verwenden. Digitale Zertifikate stellen eine Vertrauensstellung zwischen der lokalen Organisation und dem Microsoft-Datencenter her und ermöglichen gegenseitige Transport Layer Security (Mutual TLS oder MTLS). Nachdem diese Vertrauensstellung hergestellt wurde, tauschen die Netzwerkrandelemente in der lokalen Organisation und im Microsoft-Datencenter Sitzungsschlüssel aus, die dann zum Verschlüsseln des nachfolgenden Datenverkehrs verwendet werden.

Bei Hybrid- oder Onlinebereitstellungen stellt das UM-IP-Gateway einen SBC dar. Der allgemeine Antragstellername im Zertifikat muss mit dem FQDN-Wert im Adressfeld des UM-IP-Gateways übereinstimmen, das Sie erstellen. Wenn Sie beispielsweise die FQDN-Adresse "sbexternal.contoso.com" für Ihr UM-IP-Gateway angeben, stellen Sie sicher, dass der Antragstellername und der alternative Antragstellername im Zertifikat denselben Wert enthalten: sbexternal.contoso.com. Beim verwendeten Namen wird Groß-/Kleinschreibung unterschieden, sodass Sie sich vergewissern müssen, dass die Schreibung von Zertifikat und UM-IP-Gateway identisch ist. Wenn Sie einen Acme Packet SBC verwenden und der allgemeine Name nicht mit dem FQDN des UM-IP-Gateways übereinstimmt, wird der Aufruf mit dem Fehler 403 zurückgewiesen.

## NOTE

Da SBCs sich am Rand des Netzwerks befinden, fungieren sie außerdem als Firewall. Wenn Sie einen SBC hinter der Firewall Ihrer Organisation einrichten, kann er Konfigurationsprobleme verursachen. Zudem wird er für die Verbindung zu Office 365 nicht unterstützt.

## Unterstützte Session Border Controller

Die folgenden SBCs wurden erfolgreich auf Interoperabilität mit Hybrid- und Onlinebereitstellungen von Exchange getestet. Beachten Sie, dass die Funktionen und Kompatibilitäten von SBCs variieren können. Auch deren Einrichtung kann abhängig von anderen Geräten in Ihrem Netzwerk anders sein. Wenden Sie sich an den SBC-Hersteller, um herauszufinden, ob es spezielle Konfigurationshinweise für Unified Messaging in einer Hybrid- und Onlinebereitstellung gibt.

## NOTE

Exchange Online UM Unterstützung für Drittanbieter-Nebenstellenanlage Systeme über direkte Verbindungen von Kunden betriebene SBCs werden im Juli 2018 beendet. Weitere Informationen finden Sie im Exchange-Teamblog [die Einstellung der Unterstützung für Session Border Controller in Exchange Online unified messaging](#) für Weitere Informationen.

ANBIETER	MODELL	KONFIGURATIONSHINWEISE	ANMERKUNGEN
Acme Packet	Net-Net 3820 oder 4500	Wenden Sie sich an den Hersteller der Hardware, auf dem aktuellen Stand Anweisungen zum Einrichten ihres Geräts.	Dedizierter SBC
AudioCodes	Mediant 1000 MSBG	Wenden Sie sich an den Hersteller der Hardware, auf dem aktuellen Stand Anweisungen zum Einrichten ihres Geräts.	Dedizierter SBC
AudioCodes	Mediant 1000 MSBG	Wenden Sie sich an den Hersteller der Hardware, auf dem aktuellen Stand Anweisungen zum Einrichten ihres Geräts.	SBC und IP-Gateway
Cisco	ASR 1000 <b>Hinweis:</b> müssen S3 IOS 15,4 (3) oder höher installiert sein.	Wenden Sie sich an den Hersteller der Hardware, auf dem aktuellen Stand Anweisungen zum Einrichten ihres Geräts.	Dedizierter SBC
Ingate	SIParator	Wenden Sie sich an den Hersteller der Hardware, auf dem aktuellen Stand Anweisungen zum Einrichten ihres Geräts.	Dedizierter SBC
NET	VX1200 & VX1800	Wenden Sie sich an den Hersteller der Hardware, auf dem aktuellen Stand Anweisungen zum Einrichten ihres Geräts.	SBC-Option für ein VoIP-Gatewayprodukt
Sonus	SBC 1000/2000 2.2.1 oder höher	Wenden Sie sich an den Hersteller der Hardware, auf dem aktuellen Stand Anweisungen zum Einrichten ihres Geräts.	Dedizierter SBC

# Verbinden Ihres Voicemailsystems mit Ihrem Telefonnetz

18.12.2018 • 2 minutes to read

Nachdem Sie die gesamte Telefonieausrüstung für Ihre Organisation bereitgestellt haben (einschließlich VoIP-Gateways, IP-Nebenstellenanlagen und SIP-aktivierten PBX-Anlagen oder Microsoft Lync Server), müssen Sie alle UM-Komponenten (Unified Messaging) erstellen, über die die Telefoniegeräte mit Servern in Ihrer Organisation kommunizieren können.

## UM-Komponenten

Die UM-Komponenten ermöglichen die Integration von Unified Messaging in die Verzeichnisstruktur und die vorhandene Telefonieinfrastruktur. In Ihrem Verzeichnis werden alle Komponenten und Einstellungen für UM gespeichert. Jede UM-Komponente ist erforderlich, damit Unified Messaging unterstützt wird. Einige UM-Komponenten werden als Darstellungen für Telefoniehardwaregeräte erstellt. Andere werden erstellt, um Telefoniewählpläne für eine Organisation darzustellen oder bestimmte Features von Unified Messaging zu unterstützen.

Zwischen den UM-Komponenten und den in Unified Messaging verfügbaren Features besteht eine enge und wechselseitige Beziehung. Um Unified Messaging in Ihrer Organisation erfolgreich planen und bereitzustellen zu können, müssen Sie die Beziehungen zwischen jeder UM-Komponenten und den anderen Komponenten vollständig kennen.

Weitere Informationen zu den UM-Komponenten finden Sie unter:

- [UM-Wählpläne \[ONP\]](#)
- [UM-IP-Gateways](#)
- [UM-Sammelanschlüsse](#)
- [Automatisches Beantworten Sie und Weiterleiten Sie eingehender Anrufe](#)

Weitere Informationen zum Einrichten von Voicemail für Benutzer finden Sie unter:

- [UM-Postfachrichtlinien](#)
- [Voicemail für Benutzer](#)

# UM-Wählpläne [ONP]

18.12.2018 • 22 minutes to read

Unified Messaging-Wählpläne (UM) sind die wichtigste Komponente von Unified Messaging und für eine erfolgreiche Bereitstellung von Unified Messaging-Voicemail in Ihrem Netzwerk erforderlich. In den folgenden Abschnitten werden UM-Wählpläne und deren Verwendung in einer UM-Bereitstellung erläutert.

## UM-Wählpläne - Übersicht

Ein UM-Wählplan stellt eine Gruppe von Nebenstellenanlagen (Private Branch eXchange, PBX) oder IP-Nebenstellenanlagen dar, die bestimmte Benutzerdurchwahlnummern gemeinsam nutzen. Alle Benutzer-Durchwahlnummern, die auf Nebenstellenanlagen oder IP-Nebenstellenanlagen in einem Wählplan gehostet werden, müssen die gleich Anzahl von Stellen umfassen. Die Benutzer können die Durchwahlen der anderen Benutzer wählen, ohne eine Sondernummer an die Durchwahl anfügen oder eine vollständige Telefonnummer wählen zu müssen.

UM-Wählpläne entsprechen den Telefoniewählplänen. Telefoniewählpläne werden für PBX- oder -IP-PBX-Anlagen konfiguriert.

In Unified Messaging können die folgenden Topologien für UM-Wählpläne vorhanden sein:

- Ein einzelner Wählplan, der eine Untermenge von Durchwahlen bzw. alle Durchwahlen einer Organisation mit einer PBX- oder IP-PBX-Anlage abbildet.
- Ein einzelner Wählplan, der eine Untermenge von Durchwahlen bzw. alle Durchwahlen einer Organisation mit mehreren PBX- oder IP-PBX-Anlagen in einem Netzwerk abbildet.
- Mehrere Wählpläne, die eine Untermenge von Durchwahlen bzw. alle Durchwahlen einer Organisation mit einer PBX- oder IP-PBX-Anlage abbilden.
- Mehrere Wählpläne, die eine Untermenge von Durchwahlen bzw. alle Durchwahlen einer Organisation mit mehreren PBX- oder IP-PBX-Anlagen abbilden.

Benutzer, die demselben Wählplan angehören, besitzen folgende Merkmale:

- Eine Durchwahlnummer, die das Benutzerpostfach in dem Wählplan eindeutig identifiziert.
- Die Möglichkeit zum Anrufen oder zum Senden von Sprachmitteilungen an andere Mitglieder des Wählplans nur unter Verwendung der Durchwahlnummer.

Weitere Informationen zum Aktivieren eines Benutzers für Unified Messaging finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).

UM-Wählpläne werden in Unified Messaging verwendet, um sicherzustellen, dass die Telefondurchwahlen der Benutzer eindeutig sind. In einigen Telefonnetzen sind mehrere Nebenstellenanlagen oder IP-Nebenstellenanlagen vorhanden. In solchen Telefonnetzen können theoretisch zwei Benutzer mit identischer Telefondurchwahlnummer vorhanden sein. Mithilfe von UM-Wählplänen kann dies vermieden werden. Indem Sie die beiden Benutzer zwei getrennten UM-Wählplänen zuordnen, werden ihre Durchwahlen eindeutig.

## Funktionsweise von Wählplänen

Wenn ein Telefonnetz in Unified Messaging integriert wird, muss mindestens ein VoIP-Gateway (Voice over IP) genanntes Hardwaregerät oder eine IP-Nebenstellenanlage vorhanden sein, das bzw. die Ihr Telefonnetz mit dem

IP-basierten, paketvermittelten Netzwerk verbindet. VoIP-Gateways wandeln leitungsvermittelte Protokolle von einer Nebenstellenanlage in einem Telefonnetz in datenvermittelte Protokolle wie IP um. IP-Nebenstellenanlagen wandeln ebenfalls leitungsvermittelte Protokolle in ein datenvermitteltes Protokoll um. Mithilfe von Session Border Controllern (SBCs), die sich in UM-Hybrid- oder -Onlinebereitstellungen befinden, können Sie zwei IP-basierte Netzwerke über ein öffentliches oder privates WAN verbinden. Jedes VoIP-Gateway, jede IP-Nebenstellenanlage oder jeder Session Border Controller (SBC) in Ihrer Organisation wird durch ein UM-IP-Gateway dargestellt. Weitere Informationen zu UM-IP-Gateways finden Sie unter [UM-IP-Gateways](#).

Unified Messaging macht es erforderlich, mindestens einen UM-Wählplan zu erstellen. Es spielt keine Rolle, ob Sie einen oder mehrere Wählpäne erstellen - eingehende Anrufe werden von allen Exchange-Servern in Ihrer Organisation entgegengenommen. Außerdem muss mindestens ein UM-IP-Gateway dem Wählpfen zugeordnet sein. In lokalen oder Hybridbereitstellungen werden eingehende Anrufe nach Installation der Exchange-Server und Zuordnung eines UM-IP-Gateways für alle Wählpäne von allen Exchange-Servern entgegengenommen. Allerdings müssen Sie in lokalen oder Hybridbereitstellungen bei der Integration von Exchange und Lync Server SIP-UIR-Wählpäne erstellen.

#### IMPORTANT

Bei jedem einen UM-Wählplan erstellen ist auch eine Standard-Postfachrichtlinie erstellt. Die um-Postfachrichtlinie heißt < *Dial Plan Name* > Default Policy. Diese UM-Postfachrichtlinie kann gelöscht oder unterschiedlich konfiguriert werden.

Wenn Sie bei der Erstellung des ersten UM-IP-Gateways einen UM-Wählplan angeben, wird zudem ein UM-Standardsammelanschluss erstellt. Nach dem Erstellen dieser Komponenten können von den Exchange-Servern Anrufe von einem VoIP-Gateway, einer IP-Nebenstellenanlage oder einem SBC entgegengenommen und für die Benutzer verarbeitet werden, die dem UM-Wählplan zugeordnet sind. In lokalen oder Hybridbereitstellungen werden Anrufe, die beim VoIP-Gateway, der IP-Nebenstellenanlage oder dem SBC eingehen, an einen Clientzugriffsserver weitergeleitet. Der Clientzugriffsserver leitet den Anruf dann an einen Postfachserver weiter, der nach einer Übereinstimmung zwischen Durchwahl des Benutzers und zugeordnetem UM-Wählplan sucht.

## Typen von Wählpänen

Ein URI (Uniform Resource Identifier) ist eine Zeichenfolge (Zahlen oder Buchstaben) zur Identifizierung oder Benennung einer Ressource. Beim Unified Messaging besteht der Hauptzweck eines URIs darin, VoIP-Geräte mithilfe bestimmter Protokolle für die Kommunikation mit anderen Geräten zu aktivieren. Ein URI definiert das Namens- und das Zahlenformat oder -schema, das für die Informationen zum anrufenden und zum angerufenen Teilnehmer verwendet wird, die in einem SIP-Header (Session Initiation Protocol) für einen eingehenden oder ausgehenden Anruf enthalten sind.

Welche Arten von UM-Wählpänen Sie in Unified Messaging erstellen, hängt davon ab, welche URI-Typen von den VoIP-Gateways oder IP-Nebenstellenanlagen in Ihrer Organisation unterstützt werden. Der URI-Typ ist die Art von Zeichenfolge, die von der Nebenstellenanlage oder IP-Nebenstellenanlage gesendet wird. Für das Erstellen eines Wählpfanes sollten Ihnen die URI-Typen bekannt sein, die jeweils von Ihren PBX- oder IP-PBX-Anlagen unterstützt werden. Es gibt drei Formate oder URI-Typen, die für Unified Messaging-Wählpäne konfiguriert werden können:

- Telefondurchwahl (TelExtn)
- SIP-URI
- E. 164

Immer, wenn Sie in Unified Messaging einen Wählpfen erstellen, wird der Wählpfen standardmäßig für die Verwendung des URI-Typs "Telefondurchwahl" erstellt. Wenn Sie einen Wählpfen erstellt haben, können Sie den URI-Typ nicht mehr ändern. Sie müssen den vorhandenen Wählpfen löschen und einen anderen mit dem richtigen URI-Typ erstellen.

## **URI-Typ "Telefondurchwahl"**

Der URI-Typ "Telefondurchwahl" ist der gängigste UM-Wählplantyp, der für IP-Nebenstellenanlagen und Nebenstellenanlagen verwendet wird. Wenn Sie einen Telefondurchwahl-Wählplan (TelExtn) konfigurieren, müssen die VoIP-Gateways, Nebenstellenanlagen und IP-Nebenstellenanlagen den URI-Typ "TelExtn" unterstützen. Dieser URI-Typ wird heute von den meisten Nebenstellenanlagen und IP-Nebenstellenanlagen unterstützt.

Wenn ein Anruf an der Nebenstellenanlage eingeht und der UM-aktivierte Benutzer den Anruf nicht entgegennehmen kann, wird der Anruf von der Nebenstellenanlage an das VoIP-Gateway weitergeleitet. Das VoIP-Gateway (oder die IP-Nebenstellenanlage, falls verfügbar) wandelt den Anruf von einem leitungsvermittelten Protokoll in ein IP-basiertes Protokoll um. Im Header für das SIP-Paket (Session Initiation Protocol), das von dem VoIP-Gateway oder der IP-Nebenstellenanlage empfangen wird, werden die Informationen zum anrufenden und zum angerufenen Teilnehmer in einem der folgenden Formate aufgeführt:

- Tel:512345
- 512345 @<IP-Adresse>

Das Format "Telefondurchwahl" (TelExtn) wird basierend auf der Konfiguration des VoIP-Gateways oder der IP-Nebenstellenanlage verwendet.

## **SIP-URI-Typ**

SIP (Session Initiation Protocol) ist ein Standardprotokoll zum Initiieren interaktiver Benutzersitzungen, die Multimediaelemente wie Video, Sprache, Chat und Spiele umfassen. SIP ist ein auf Anforderungen und Antworten basierendes Protokoll, das Anforderungen von Clients und Antworten von Servern beantwortet. Clients werden durch SIP-URIs identifiziert. Anforderungen können über ein beliebiges Transportprotokoll, z. B. UDP oder TCP, gesendet werden. SIP bestimmt den für die Sitzung zu verwendenden Endpunkt durch Auswahl des Kommunikationsmediums und der Medienparameter.

Wenn Sie einen neuen Wählplan erstellen, haben Sie die Möglichkeit, einen SIP-URI-Wählplan zu erstellen, wenn in Ihrer Umgebung Microsoft Office Communications Server 2007 R2 oder Microsoft Lync Server implementiert ist. Sie können einen SIP-URI-Wählplan auch erstellen, wenn in Ihrer Organisation IP-Nebenstellenanlagen oder SIP-aktivierte Nebenstellenanlagen verfügbar sind. In letzterem Fall muss Ihre Organisation auch SIP-URIs und das SIP-Routing unterstützen.

Einen SIP-URI ist SIP-Telefonnummer des Benutzers. Der SIP-URI ähnelt einer e-Mail-Adresse und wird im folgenden Format geschrieben: `sip- :<Username>@<Domäne oder IP-Adresse>:Port`. Wenn eine SIP-aktivierte IP-Nebenstellenanlage oder der Nebenstellenanlage verwendet wird, um einen Anruf an die Exchange-Server zu senden, wird das Gerät sendet den SIP-URI für die aufrufenden und aufgerufenen Partei in der SIP-Header und Durchwahlnummern nicht einschließen.

## **URI-Typ E.164**

E.164 ist ein Standardformat für Telefonnummern, das den Nummerierungsplan für internationale öffentliche Fernmeldedienste (International Public Telecommunication Numbering Plan) definiert, der im PSTN (Public Switched Telephone Network) und einigen Datennetzwerken verwendet wird. E.164 definiert das Format von Telefonnummern. E.164-Nummern können bis zu 15 Ziffern enthalten und weisen in der Regel ein Pluszeichen (+) vor den Ziffern der Telefonnummer auf. Wenn Sie eine gemäß E.164 formatierte Telefonnummer von einem Telefon aus wählen möchten, muss die internationale Vorwahl in die gewählte Nummer einbezogen werden. In einem Nummerierungsplan für öffentliche Telefonsysteme nach E.164 enthält jede zugeordnete Nummer einen Ländercode, eine Bereichskennzahl und eine Teilnehmernummer.

Wenn Sie einen neuen Wählplan erstellen, können Sie einen E.164-Wählplan erstellen. Wenn Sie jedoch einen E.164-Wählplan erstellen und konfigurieren, müssen die PBX- und IP-PBX-Anlagen das E.164-Routing unterstützen. Der SIP-Header, der von einem E.164-Wählplan zugeordneten VoIP-Gateway empfangen wird, enthält die Telefonnummer im E.164-Format sowie Informationen zum anrufenden und zum angerufenen

Teilnehmer. Das Format sieht wie folgt aus: Tel:+14255550123. Bei Exchange Online-Bereitstellungen mit Exchange Unified Messaging und Lync Server müssen Sie für Outlook Voice Access und die automatische Telefonzentrale richtig formatierte E.164-Nummern verwenden.

## VoIP-Sicherheit

Exchange-Server können je nach Konfiguration des UM-Wählplans mit VoIP-Gateways, IP-Nebenstellenanlagen und anderen Exchange-Computern im ungesicherten, SIP-gesicherten oder gesicherten Modus kommunizieren. In lokalen und Hybridbereitstellungen können Clientzugriffs- und Postfachserver in jedem für einen Wähleplan konfigurierten Modus ausgeführt werden, da TCP-Port 5060 und TCP-Port 5061 von den Servern gleichzeitig auf ungesicherte bzw. gesicherte Anforderungen überwacht werden, sofern sie zum Starten im Dualmodus konfiguriert sind. Clientzugriffs- und Postfachserver beantworten alle eingehenden Anrufe für alle UM-Wählpläne, aber diese Wählepläne können unterschiedliche VoIP-Sicherheitseinstellungen aufweisen.

In der lokale und hybride Bereitstellungen, standardmäßig beim Erstellen eines UM-Wählplan, wird er in nicht abgesicherten Modus kommunizieren und die Clientzugriffs- und Postfachservern Servern sendet und empfängt Daten von VoIP-Gateways, IP-Nebenstellenanlagen und SBCs ohne Verschlüsselung. Im nicht abgesicherten Modus werden weder der Echtzeit Transport Protocol (RTP) Media Kanal noch SIP-signaldatenverkehr über Informationen verschlüsselt. Sie können das Cmdlet **Get-UMDialPlan** im Exchange Online PowerShell Sie um die sicherheitseinstellung für einen bestimmten UM-Wählplan zu bestimmen.

In lokalen und Hybridbereitstellungen können Sie einen Clientzugriffs- und Postfachserver für die Verwendung von MTLS (Mutual TLS) zur Verschlüsselung des SIP- und RTP-Datenverkehrs konfigurieren, der von anderen Geräten und Servern gesendet und empfangen wird. Wenn Sie den Wähleplan für den Modus "SIP-gesichert" konfigurieren, wird nur der SIP-Signalverkehr verschlüsselt, und die RTP-Medienkanäle verwenden weiterhin das unverschlüsselte TCP. Wenn Sie den Wähleplan jedoch für den Modus "Gesichert" konfigurieren, werden sowohl der SIP-Signalverkehr als auch die RTP-Medienkanäle verschlüsselt. Ein verschlüsselter Signalmedienkanal, der SRTP (Secure Realtime Transport Protocol) einsetzt, verwendet außerdem MTLS (Mutual TLS) zum Verschlüsseln der VoIP-Daten.

Beim Erstellen eines neuen Wähleplans oder nachdem Sie einen Wähleplan mithilfe der Exchange-Verwaltungskonsole oder über das Cmdlet **Set-UMDialPlan** im Exchange Online PowerShell erstellt haben, können Sie den VoIP-Sicherheitsmodus konfigurieren. Beim Konfigurieren der um-Wähleplan zu mit SIP-gesicherte oder gesicherte Modus, Clientzugriffs- und Postfachserver verschlüsselt das SIP-Datenverkehr, der RTP-medienkanäle oder beides Signale. Allerdings um verschlüsselte Daten zu und von Exchange-Server senden können, müssen Sie ordnungsgemäß die UM-Wähleinstellungen und VoIP-Geräten wie VoIP-Gateways, IP-PBX-Anlagen, konfigurieren und SBCs müssen mutual TLS unterstützen.

## Outlook Voice Access

Zwei Arten von Anrufern greifen mithilfe der Outlook Voice Access-Nummer, die für einen UM-Wählplan konfiguriert ist, auf das Voicemailsystem zu: nicht authentifizierte Anrufer und authentifizierte Anrufer. Wenn Anrufer die im Wähleplan konfigurierte Outlook Voice Access-Nummer anrufen, gelten sie als anonym oder nicht authentifiziert, bis sie ihre Voicemaildurchwahl und PIN eingegeben haben. Die einzige Option, die anonymen oder nicht authentifizierten Anrufern zur Verfügung steht, ist das Verzeichnissuchfeature. Nachdem die Anrufer ihre Voicemaildurchwahl und PIN eingegeben haben, werden sie authentifiziert und erhalten Zugriff auf ihr Postfach. Nachdem der Zugang zum Voicemailsystem gewährt wurde, verwenden sie das Outlook Voice Access-Feature.

Outlook Voice Access besteht aus einer Reihe von Sprachansagen, mit denen der Anrufer auf E-Mail, Voicemail, Kalender und andere Informationen zugreifen kann. Outlook Voice Access ermöglicht authentifizierten Anrufern mithilfe von MFV-Tasten- oder Spracheingaben (auch als Tonwahl bezeichnet) die Navigation durch ihre persönlichen Informationen, das Tätigen von Anrufen oder Auffinden von Benutzern.

### Outlook Voice Access-Nummern

Nachdem Sie einen UM-Wählplan erstellt haben, müssen Sie mindestens eine Outlook Voice Access-Nummer hinzufügen. Outlook Voice Access-Nummern werden auch als Pilotnummern für Wählpässe bezeichnet. Diese Nummer wird von Outlook Voice Access-Benutzern für den Zugriff auf ihre Postfächer verwendet und ermöglichen ihnen die Verzeichnissuche.

Beim Erstellen eines UM-Wählplans werden standardmäßig keine Outlook Voice Access-Nummern konfiguriert. Sie müssen mindestens eine Telefon- oder Durchwahlnummer konfigurieren, damit die Benutzer das Outlook Voice Access-Feature verwenden können. Die Anzahl alphanumerischer Zeichen in der Outlook Voice Access-Nummer darf 20 nicht überschreiten. Nachdem Sie diese Nummer für den Wählpas konfiguriert haben, wird sie in den Voicemailoptionen in Microsoft Outlook sowie in Outlook Web App angezeigt.

Sie können eine Telefonnummer oder Durchwahl über das Feld **Outlook Voice Access-Nummern** zum UM-Wählplan hinzufügen, die ein Benutzer anrufen kann, um auf das Voicemailsystem mithilfe von Outlook Voice Access zuzugreifen. In den meisten Fällen wird eine Durchwahl oder eine externe Telefonnummer eingegeben. Da in diesem Feld jedoch alphanumerische Zeichen zulässig sind, kann ein SIP-URI angegeben werden, wenn eine IP-Nebenstellenanlage, Office Communications Server 2007 R2 oder Microsoft Lync Server verwendet wird.

In Abhängigkeit von den Anforderungen in Ihrer Organisation können Sie eine oder mehrere Outlook Voice Access-Nummern konfigurieren. Sie können eine einzige oder mehrere Outlook Voice Access-Nummern für einen einzelnen UM-Wählplan verwenden. Sie können jedoch keine einzelne Outlook Voice Access-Nummer verwenden, die mehrere UM-Wählpläne umfasst.

# UM-Wählpläne Plan Verfahren [EXO]

18.12.2018 • 2 minutes to read

[Erstellen eines UM-Wählplans](#)

[Verwalten eines UM-Wählplans](#)

[Ändern des Audiocodecs](#)

[Konfigurieren der maximalen Anrufdauer](#)

[Konfigurieren Sie die maximale Aufzeichnung Dauer](#)

[Konfigurieren Sie den Wert der Aufzeichnung Leerlauftimeout](#)

[Konfigurieren der VoIP-Sicherheitseinstellung](#)

[Konfigurieren eines Wählplans für Benutzer mit ähnliche Namen](#)

[Löschen von einem um-Wählplan](#)

# Erstellen eines UM-Wählplans

18.12.2018 • 14 minutes to read

In einem Unified Messaging (UM)-Wählplan sind die Konfigurationsinformationen enthalten, die Ihr Telefonienetzwerk betreffen. UM-Wähleinstellungen richten eine Verknüpfung zwischen der Telefon-Durchwahlnummer eines Voicemail-aktivierten Benutzers und seinem Postfach ein. Wenn Sie UM-Wähleinstellungen erstellen, können Sie die Anzahl der Ziffern in den Durchwahlnummern, den URI-Typ (Uniform Resource Identifier) und die VoIP-Sicherheitseinstellung (Voice over IP) für die Wähleinstellungen konfigurieren.

Bei jedem einen UM-Wählplan erstellen ist auch eine UM-Postfachrichtlinie erstellt. Die um-Postfachrichtlinie heißt < *Wählplannamens* > Default Policy.

Weitere Verwaltungsaufgaben im Zusammenhang mit um-Wählpläne finden Sie unter [Planen von Verfahren UM einwählen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#) .
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen von UM-Wähleinstellungen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**, und klicken Sie dann auf **New**  


2. Füllen Sie auf der Seite **neue UM-Wählplan** folgende Felder aus:

- **Name:** Geben Sie den Namen des Wählplans. Ein UM-Wählplanname ist erforderlich und muss eindeutig sein. Es wird jedoch nur für die Anzeige in der Exchange-Verwaltungskonsole und Exchange Online PowerShell verwendet. Wenn Sie den Anzeigenamen des Wählplans ändern haben, nachdem es erstellt wurde, müssen Sie zunächst Löschen

der vorhandenen um-Wählplan und erstellen Sie eine andere Wählp plan mit dem entsprechenden Namen. Wenn Ihre Organisation mehrere um-Wählpläne verwendet, wird empfohlen, für die Verwendung von aussagekräftigen Names für die um-Wählpläne. Die maximale Länge einer UM-Wählplannname beträgt 64 Zeichen und Leerzeichen enthalten. Es kann jedoch keine der folgenden Zeichen: "/ \ []: | = , + \* ? < >.

Wenn gleich der Name eines UM-Wählplans Leerzeichen enthalten darf, ist bei der Integration von Unified Messaging in Office Communications Server 2007 R2 oder Microsoft Lync Server die Verwendung von Leerzeichen im Namen von Wählp län en nicht zulässig. Wenn Sie daher einen Wählp län mit Leerzeichen im Anzeigenamen erstellt haben und Sie eine Integration in Office Communications Server 2007 R2 oder Lync Server durchführen, müssen Sie diesen Wählp län zunächst löschen und einen anderen Wählp län erstellen, der keine Leerzeichen im Anzeigenamen aufweist.

#### IMPORTANT

Obwohl das Feld für den Namen des Wählp län 64 Zeichen akzeptieren kann, kann nicht der Name des Wählp län länger als 49 Zeichen sein. Wenn Sie versuchen, ein Wählp län mit mehr als 49 Zeichen zu erstellen, erhalten Sie eine Fehlermeldung angezeigt. Die Nachricht wird angenommen, dass die um-Postfachrichtlinie konnte nicht generiert werden, da der UM-Wählplannname zu lang ist. In diesem Fall daran, wie bereits erwähnt, wenn Sie einen Wählp län eine Standard-Postfachrichtlinie mit dem Namen erstellen \_ <Wählplannamens> \_ Standardrichtlinie wird ebenfalls erstellt. Wenn der Name des Wählp län 15 Zeichen in Standardrichtlinie hinzugefügt werden, überschreitet die Gesamtzahl der Zeichen den Grenzwert. Der Parameter *Name* für beide dem UM-Wählplan planen, und UM-Postfachrichtlinie kann 64 Zeichen sein. Wenn der Name des Wählp län länger als 49 Zeichen ist, jedoch wird der Name des standardmäßigen UM-Postfachrichtlinie länger als 64 Zeichen sein, und dies ist nicht zulässig, vom System.

- **Erweiterungslänge (Ziffern):** Geben Sie die Anzahl der Nachkommastellen für den Wählp län . Die Anzahl der Nachkommastellen für Durchwahlnummern basiert auf der Telefonie Wählp län auf eine Private Branch eXchange, (Nebenstellenanlage PBX) oder IP-PBX-Ressource erstellt. Beispielsweise wenn ein Benutzer zugeordnet ein Wählp län Telefonie wählt eine vierstellige Erweiterung zum Aufrufen eines anderen Benutzers in der gleichen Telefonie-Wählplan, wählen Sie 4 als die Anzahl der Nachkommastellen in der Erweiterung.

Dies ist ein erforderliches Feld mit Werten im Bereich von 1 bis 20. Die typische Durchwahllänge liegt zwischen 3 und 7. Wenn die vorhandene Telefoniumgebung Durchwahlnummern umfasst, dann müssen Sie eine Anzahl für die Stellen festlegen, die mit der Anzahl der Stellen in diesen Durchwahlnummern übereinstimmt.

Beim Erstellen einer Session Initiation Protocol (SIP) oder einer e. 164-Wählplan und ordnen Sie den Wählp län einen UM-aktivierten Benutzer, müssen Sie dennoch eine Durchwahlnummer ein, die vom Benutzer

verwendet werden eingeben. Diese Nummer wird von Outlook Voice Access-Benutzer verwendet, beim Zugriff auf ihr Postfach.

- **Dial PlanTyp:** eine Uniform Resource Identifier (URI) ist eine Zeichenfolge, die identifiziert oder den Namen einer Ressource. Die Hauptaufgabe der diese Identifikation ist mit VoIP-Geräte zur Kommunikation mit anderen Geräten über ein Netzwerk mit bestimmten Protokollen aktiviert. URIs in Schemas, die eine bestimmte Syntax und Format und die Protokolle für den Anruf definieren definiert sind. Einfach ausgedrückt wird dieses Format aus die IP-Nebenstellenanlage oder der Nebenstellenanlage übergeben. Nach dem Erstellen ein UM-Wähleinstellungen, nicht möglich, den URI-Typ zu ändern, ohne die Wähleinstellungen löschen und Neuerstellen der Wähleinstellungen der richtigen URI-Typ enthalten. Sie können eine der folgenden URI-Typen für den Wählplan auswählen:
  - **Durchwahl:** Dies ist die am häufigsten verwendeten URI-Typ. Die aufrufenden und aufgerufenen von Informationen aus der VoIP-Gateway oder IP Private Branch eXchange, (Nebenstellenanlage PBX) in einem der folgenden Formate aufgeführt ist: Tel:512345 oder 512345 @</IP-Adresse>. Dies ist der Standard-URI-Typ für Wählpläne.
  - **SIP-URI:** Verwenden Sie diesen URI-Typ aus, wenn Sie einen Session Initiation Protocol (SIP) URI-Wählplan wie etwa eine IP-Nebenstellenanlage verfügen müssen, die SIP-routing unterstützt oder Integration von Microsoft Office Communications Server 2007 R2 oder Microsoft Lync Server und Unified Messaging. Die aufrufenden und aufgerufenen Parteiinformationen aus der VoIP-Gateway. IP-Nebenstellenanlage oder Communications Server 2007 R2 oder Lync Server ist eine SIP-Adresse im folgenden Format aufgelistet: sip: <Username>@<Domäne oder \_IP Adresse \_>: Port.
  - **E. 164:** e. 164 ist ein internationaler Nummerierung Plan für Öffentliche Telefonsystemen in der enthält jede Nummer eine Landesvorwahl, einen Code national Ziel und die Rufnummer. Die aufrufenden und aufgerufenen von Informationen aus der VoIP-Gateway oder IP-PBX gesendet wird im folgenden Format aufgelistet: Tel: + 14255550123.

**Caution**

Wenn Sie einen Wählplan erstellt haben, können Sie den URI nur ändern, wenn Sie den Wählplan löschen und anschließend mit dem richtigen URI-Typ neu erstellen.

- **VoIP-Sicherheitsmodus:** Verwenden Sie diese Dropdown-Liste die VoIP-sicherheitseinstellung für den Wählplan auswählen. Sie können eine der folgenden Sicherheitseinstellungen für den Wählplan auswählen:
  - **Unsecured:** beim Erstellen eines UM-Wählplans, es wird standardmäßig auf nicht verschlüsselt die SIP-Signale oder RTP-Datenverkehr. Im nicht abgesicherten Modus die Clientzugriffs- und Postfachservern Server zugeordnete UM Dial Plan senden und Empfangen von Daten von VoIP-Gateways, IP-Nebenstellenanlagen, SBCs und anderen Servern Clientzugriffs- und Postfachservern, die keine Verschlüsselung. Im nicht abgesicherten Modus werden weder der

Echtzeit Transport Protocol (RTP) Media Kanal noch SIP-signaldatenverkehr über Informationen verschlüsselt.

- **SIP-gesichert:** Wenn Sie **SIP-gesichert** auswählen, nur das SIP-signaldatenverkehr verschlüsselt werden und der RTP-medienkanäle weiterhin verwenden TCP, das ist nicht verschlüsselt. Mit SIP-gesicherte wird Mutual Transport Layer Security (TLS) zum Verschlüsseln von SIP-signaldatenverkehr über Datenverkehr und VoIP-Daten verwendet.
- **Secured:** Wenn Sie **Secured** auswählen, werden beide SIP-Datenverkehr und der RTP-medienkanäle Signale verschlüsselt. Sowohl der sicheren Media signalkanal, der sichere Echtzeit SRTP (Transport Protocol) und der SIP-signaldatenverkehr verwendet mutual TLS verwenden Sie zum Verschlüsseln der VoIP-Daten.
- **Sprache:** mit dieser Liste können Sie die Standardsprache von Outlook Voice Access-Benutzer verwendet werden. Diese Einstellung wird nicht auf die Einstellung für die Sprache auf einer automatischen UM-Telefonzentrale angewendet. Sie können festlegen, dass die Sprache für Outlook Voice Access oder mit diesem identisch unterschiedliche von der Sprache sein, die auf eine automatische um-Telefonzentrale verwendet wurde. Wenn ein Benutzer einen Anruf an einen Benutzer, die zu einem Wählplan verknüpft ist tätigt, ist die audio Sprache als Standardsprache, die den VoIP-aufgezeichnet-Operator verwendet. Fordert das System, die Anrufer hören sind in der gleichen Sprache wiedergegeben. Die Sprache, die dem um-Wählplan ausgewählt sind wird zum Lesen von e-Mail, Voicemail und Kalenderelemente verwendet. um den Namen des Benutzers angenommen, wenn eine persönliche noch nicht Ansage aufgezeichnet wurde. Um eine Sprachnachricht mit dem Feature Voicemailvorschau aufzuzeichnen; und so aktivieren Sie die automatische Spracherkennung Spracherkennung (ASR) ordnungsgemäß funktioniert.
- **Länder-/Regionscode:** in diesem Feld Geben Sie die Anzahl der Land/Region Code für ausgehende Anrufe verwendet werden können. Diese Nummer wird die Telefonnummer vorangestellt, die gewählt wird. In diesem Feld akzeptiert von 1 bis 4 Ziffern. In den USA ist beispielsweise Länder-/Regionscode 1 an. Im Vereinigten Königreich's es 44.

3. Klicken Sie auf **Speichern**.

## Mit Exchange Online PowerShell erstellen Sie eine automatische UM-Wählplan

Dieses Beispiel erstellt einen neuen UM-Wählplan mit dem Namen `MyUMDialPlan`, die vierstellige Durchwahlnummern verwendet.

```
New-UMDialplan -Name MyUMDialPlan -NumberofDigits 4
```

Dieses Beispiel erstellt einen neuen UM-Wählplan mit dem Namen `MyUMDialPlan`, die fünfstellige Durchwahlnummern verwendet und SIP-URIs unterstützt.

```
New-UMDialplan -Name MyUMDialPlan -UriType SIPName -NumberofDigits 5
```

# Verwalten eines UM-Wählplans

18.12.2018 • 65 minutes to read

Nach Erstellen von Unified Messaging-Wähleinstellungen (UM) können Sie verschiedene Einstellungen anzeigen und konfigurieren. Sie können beispielsweise den Grad der VoIP-Sicherheit (Unified Messaging), den Audiocodec und Wähleinschränkungen konfigurieren. Die von Ihnen konfigurierten UM-Wählplaneinstellungen wirken sich auf alle Benutzer aus, die diesen Einstellungen über eine UM-Postfachrichtlinie zugeordnet sind.

Zusätzliche Verwaltungsaufgaben im Zusammenhang mit UM-Wählplänen finden Sie unter [UM Dial Plan Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Anzeigen oder Konfigurieren von UM-Wählplaneinstellungen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie anzeigen oder ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**. Über die Konfigurationsoptionen können Sie so, wie dies in den folgenden Schritten beschrieben ist, bestimmte Wähleinstellungen anzeigen sowie Features aktivieren oder deaktivieren.
4. **Allgemein:** Verwenden Sie diese Seite anzeigen bestimmter Wähleinstellungen zu aktivieren oder Deaktivieren von Features für UM-aktivierte Benutzer:
  - **Name:** Dies ist der Name des Wählplans, der erstellt wurde. Die maximale Länge einer UM-Wählplanname beträgt 64 Zeichen und Leerzeichen enthalten. Es kann jedoch enthalten die folgenden Zeichen: "/\[]:|=, + \* ? < >.
  - Wenngleich der Name eines UM-Wählplans Leerzeichen enthalten darf, ist bei der Integration von Unified Messaging in Office Communications Server 2007 R2 oder Microsoft Lync Server die Verwendung von Leerzeichen im Namen von Wählplänen nicht zulässig. Wenn Sie daher einen Wählplan mit Leerzeichen im

Anzeigennamen erstellt haben und Sie eine Integration in Office Communications Server 2007 R2 oder Lync Server durchführen, müssen Sie diesen Wählplan zunächst löschen und einen anderen Wählplan erstellen, der keine Leerzeichen im Anzeigennamen aufweist.

#### IMPORTANT

Obwohl das Feld für den Namen des Wählplans 64 Zeichen akzeptieren kann, kann nicht der Name des Wählplans länger als 49 Zeichen sein. Wenn Sie versuchen, ein Wählplanname erstellen, die mehr als 49 Zeichen enthält, erhalten Sie eine Fehlermeldung angezeigt. Die Nachricht wird angenommen, dass die um-Postfachrichtlinie konnte nicht generiert werden, da der UM-Wählplanname zu lang ist. In diesem Fall daran, wie bereits erwähnt, wenn Sie einen Wählplan eine Standard-Postfachrichtlinie mit dem Namen erstellen \_ <Wählplannamens> \_ Standardrichtlinie wird ebenfalls erstellt. Wenn der Name des Wählplans 15 Zeichen in Standardrichtlinie hinzugefügt werden, überschreitet die Gesamtzahl der Zeichen den Grenzwert. Der Parameter *Name* für beide dem UM-Wählplan planen, und UM-Postfachrichtlinie kann 64 Zeichen sein. Wenn der Name des Wählplans länger als 49 Zeichen ist, jedoch wird der Name des standardmäßigen UM-Postfachrichtlinie länger als 64 Zeichen sein, und dies ist nicht zulässig.

- **Erweiterungslänge (Ziffern):** Dies ist die Anzahl der Stellen in den Durchwahlnummern für Benutzer, die diesen Wähleinstellungen zugeordnet sind. Wenn ein Benutzer einen Wählplan zugeordnet einer 4-Digit Extension lautet zum Aufrufen eines anderen Benutzers in der gleichen Wählplan anwählt, wählen Sie 4 als die Anzahl der Nachkommastellen in die Erweiterung fest.

Die Anzahl von Ziffern für Durchwahlnummern basiert auf dem Telefoniewählplan, der auf einer IP-Nebenstellenanlage oder Nebenstellenanlage eingerichtet wurde. Dies ist ein erforderliches Feld mit Werten von 1 bis 20. Die typische Durchwahllänge ist 3 bis 7 Stellen. Wenn in der vorhandenen Telefoniumgebung Durchwahlnummern verwendet werden, müssen Sie beim Erstellen der UM-Wähleinstellungen eine Anzahl für die Stellen festlegen, die mit der Anzahl der Stellen in diesen Durchwahlen übereinstimmt.

- **Dial Plantyp:** eine Uniform Resource Identifier (URI) ist eine Zeichenfolge, die identifiziert oder den Namen einer Ressource. Die Hauptaufgabe der diese Identifikation wird zum Aktivieren von VoIP-Geräte und PBX-Anlagen für die Kommunikation mit anderen Geräten über ein Netzwerk mit bestimmten Protokollen. URIs in Schemas, die eine bestimmte Syntax und Format und die Protokolle für den Anruf definieren definiert sind. Einfach ausgedrückt dieses Format wird von der IP-PBX oder PBX übergeben, und der Typ des Wählplans, die Sie erstellen, muss dieses Format übereinstimmen. Nachdem Sie einen um-Wählplan erstellt haben, wird nicht Sie den Typ der Dial Plan ändern, ohne die Wähleinstellungen löschen und Neuerstellen des Wählplans des korrekten Typs sein. Sie können die folgenden Arten von Dial Plan auswählen:
  - **Durchwahl:** Dies ist der am häufigsten verwendeten Dial Plan. Die aufrufenden und aufgerufenen von Informationen aus der VoIP-Gateway oder IP Private Branch eXchange, (Nebenstellenanlage PBX) in einem der folgenden Formate aufgeführt ist: Tel:512345 oder 512345 @<IP-Adresse>. Dies ist der Standardtyp für Wählpläne.
  - **SIP-URI:** Verwenden Sie diesen Wähleinstellungen Typ, wenn Sie einen Session Initiation Protocol (SIP) URI-Wählplan wie etwa eine IP-Nebenstellenanlage, die SIP-routing, unterstützt eine SIP-aktivierte PBX benötigen, oder wenn die Integration von Microsoft Office Communications Server 2007 R2 oder Microsoft Lync Server und Unified Messaging. Die aufrufenden und aufgerufenen Parteiinformationen aus der VoIP-Gateway. IP-Nebenstellenanlage, SIP-aktivierte PBX oder Communications Server 2007 R2 oder Lync Server ist eine SIP-Adresse im folgenden Format aufgelistet: sip:<Username>@<Domäne oder IP-Adresse>: Port.
  - **E. 164:** e. 164 ist ein internationaler Nummerierung Plan für Öffentliche Telefonsystemen in der enthält jede Nummer eine Landesvorwahl, einen Code national Ziel und die Rufnummer. Die aufrufenden und aufgerufenen von Informationen aus der VoIP-Gateways und PBX oder IP-PBX gesendet wird im folgenden Format aufgelistet: Tel: + 14255550123.

#### NOTE

Wenn Sie einen Wählplan erstellt haben, können Sie den Typ des Wählplans nur ändern, wenn Sie den Wählplan löschen und anschließend mit dem richtigen Wählplantyp neu erstellen.

- **VoIP-Sicherheitsmodus:** Verwenden Sie diese Dropdown-Liste die VoIP-sicherheitseinstellung für den Wählplan auswählen. Sie können eine der folgenden Sicherheitseinstellungen für den Wählplan auswählen:
- **Unsecured:** in der Standardeinstellung beim Erstellen eines UM-Wählplans festgelegt SIP-Signale oder RTP-Datenverkehr nicht verschlüsselt. Im nicht abgesicherten Modus die Exchange-Server zugeordnete UM einwählen Plan senden und Empfangen von Daten von VoIP-Gateways, IP-Nebenstellenanlagen, SBCs und anderen Exchange-Servern keine Verschlüsselung. Im nicht abgesicherten Modus werden weder der Echtzeit Transport Protocol (RTP) Media Kanal noch SIP-signaldatenverkehr über Informationen verschlüsselt.
- **SIP-gesichert:** Wenn Sie **SIP-gesichert** auswählen, nur das SIP-signaldatenverkehr verschlüsselt werden und der RTP-medienkanäle weiterhin verwenden TCP, das ist nicht verschlüsselt. Mit SIP-gesicherte wird mutual Transport Layer Security (TLS) zum Verschlüsseln von SIP-signaldatenverkehr über Datenverkehr und VoIP-Daten verwendet.
- **Secured:** Wenn Sie **Secured** auswählen, werden beide SIP-Datenverkehr und der RTP-medienkanäle Signale verschlüsselt. Sowohl der sicheren Media signalkanal, der sichere Echtzeit SRTP (Transport Protocol) und der SIP-signaldatenverkehr verwendet mutual TLS verwenden Sie zum Verschlüsseln der VoIP-Daten.

5. **Wählen Sie eine Codes:** Verwenden Sie diese Seite zum Konfigurieren der Kurzwahlnummern für UM-Wähleinstellungen. Für den Wählplan können mehrere Dial Code Einstellungen festgelegt werden. Eingehende und ausgehende Anrufoptionen beinhalten. Sie können die folgenden konfigurieren:

- **Kurzwahlnummern für ausgehende Anrufe:** Verwenden Sie diese Einstellungen an die Einwahl-Codes für ausgehende Anrufe, die von UM-aktivierten Benutzern hergestellt werden kann. Diese ausgehende Anrufe werden Anrufe, die mithilfe von Outlook Voice Access befinden oder aus einem Voicemailnachricht.
- **Amtskennziffer:** Verwenden Sie dieses Feld die Nummer oder Zahlen verwendet, um eine externe Telefonnummer für ausgehende Anrufe mit externen Zugriff eingeben. Diese Nummer wird die Telefonnummer gewählt vorangestellt. Dies ist auch einen Trunk Zugriffscode bezeichnet. Dieses Feld akzeptiert von 1 bis 16 Ziffern. Für viele Organisationen ist diese Nummer 9. Dieses Feld ist nicht standardmäßig aufgefüllt.

Diese Einstellung wird häufig in Telefoniumgebungen verwendet, in denen eine Nebenstellenanlage oder IP-Nebenstellenanlage am Standort genutzt wird (am Standort oder durch eine Organisation gewartet). Eine Konfiguration ist möglicherweise nicht erforderlich, wenn die Telefoniumgebung der Organisation von einem externen Unternehmen oder Dienstleister verwaltet wird.

- **Internationale VAZ:** Verwenden Sie dieses Feld, geben Sie den Code für den Zugriff von internationalen Rufnummern für ausgehende Anrufe auf. Diese Nummer wird die Telefonnummer gewählt vorangestellt. Dieses Feld ist nicht standardmäßig aufgefüllt. Dieses Feld akzeptiert von 1 bis 4 Ziffern. Internationale VAZ für die USA ist beispielsweise 011. Für Europa's es 00.
- **Nationales Rufnummernpräfix:** Verwenden Sie dieses Feld, geben Sie den Code, mit dem Telefonnummern gewählt, die aus einer Ortskennzahl, aber innerhalb des Landes/der Region sind. Diese Nummer wird die Telefonnummer gewählt vorangestellt. Dieses Feld ist nicht standardmäßig aufgefüllt. Dieses Feld akzeptiert von 1 bis 4 Ziffern. Beispielsweise 0 in Europa verwendet wird und 1 wird in Nordamerika verwendet.
- **Länder-/Regionscode:** mit diesem Feld können Sie die Eingabe der Land/Region Code Anzahl für

ausgehende Anrufe verwendet. Diese Nummer wird die Telefonnummer gewählt vorangestellt. Dieses Feld ist nicht standardmäßig aufgefüllt. Dieses Feld akzeptiert von 1 bis 4 Ziffern. In den USA ist beispielsweise Länder-/Regionscode 1 an. Im Vereinigten Königreich's es 44.

- **Zahlenformate für den Wählvorgang zwischen um-Wählplänen:** Verwenden Sie diese Einstellungen, um Anrufe zwischen Benutzern in getrennte Wählpläne, wenn sie Anrufe zwischen Wählpläne platzieren zu konfigurieren.

- **Land/Region Zahlenformat:** Verwenden Sie dieses Feld, um festzulegen, wie Telefonnummer des Benutzers von den Exchange-Servern gewählt werden sollte, wenn Benutzer in einem anderen Wählplan sind, die den gleichen Ländercode hat. Hiermit wird von automatischen Telefonzentralen und wenn ein Benutzer Outlook Voice Access durchsucht und versucht, den Benutzer im Verzeichnis aufzurufen.

Bei diesem Eintrag besteht aus einem Rufnummernpräfix und einer Variablen Anzahl von Zeichen (beispielsweise 020 XXXXXX). Um die Telefonnummer zu bestimmen, wird die Unified Messaging die letzten X Ziffern aus die Telefonnummer in das Verzeichnis, in dem angegebenen Präfix angegebenen angefügt.

- **Internationale Zahlenformat:** Verwenden Sie dieses Feld, um anzugeben, wie Telefonnummer des Benutzers mit Unified Messaging gewählt werden soll, wenn die Benutzer in verschiedene Wählpläne, die verschiedene Ländercodes aufweisen. Dies wird durch eine automatische Telefonzentrale und verwendet, wenn ein Benutzer Outlook Voice Access sucht und versucht, den Benutzer im Verzeichnis aufzurufen.

Bei diesem Eintrag besteht aus einem Rufnummernpräfix und einer Variablen Anzahl von Zeichen (beispielsweise 4420 XXXXXX). Um die Telefonnummer zu bestimmen, wird die Unified Messaging die letzten X Ziffern aus die Telefonnummer in das Verzeichnis, in dem angegebenen Präfix angegebenen angefügt.

- **Zahlenformate für eingehende Anrufe innerhalb desselben Wählplans:** Verwenden Sie dieses Feld zum Hinzufügen oder Entfernen einer Zahlenformat für eingehende Anrufe, die zwischen Benutzern in den gleichen Wähleinstellungen platziert werden. Dieses Feld akzeptiert Zahlen und den Buchstaben "X" als einen Platzhalter. In diesem Feld können keine anderen Buchstaben verwendet werden.

Fügen Sie ein Format für eingehende Anrufe innerhalb desselben Wählplans hinzu. Beispielsweise um ein Zahlenformat für 5-stellige Durchwahlnummern hinzuzufügen, geben, 142570XXXX, und klicken Sie auf **Hinzufügen** . Wenn ein Zahlenformat entfernen möchten, klicken Sie auf **Entfernen** .

6. **Outlook Voice Access:** Verwenden Sie diese Seite zum Konfigurieren von Outlook Voice Access-Einstellungen für den UM-Wählplan. Outlook Voice Access ermöglicht Benutzern Zugriff auf ihre einzelne Postfächer zum Abrufen von e-Mail, Sprachnachrichten, Kontakte und Kalenderinformationen über ein Telefon. Sie können anzeigen oder konfigurieren Sie Folgendes:

- **Begrüßung:** dieses reine Anzeigefeld zeigt den Namen der Audiodatei, die für die Begrüßung verwendet werden.
- **Standard-Ansage:** die Begrüßung wird verwendet, wenn ein Benutzer Outlook Voice Access oder einer anderen Anrufer die Outlook Voice Access-Nummer ruft und sucht nach ein Verzeichnis. Diese Audiodatei ist die standardmäßige Begrüßung für UM-Wähleinstellungen. Allerdings sollten Sie diese Begrüßung ändern, und geben Sie einen anderen bestimmte Begrüßung für Ihr Unternehmen, wie beispielsweise "Willkommen, Outlook Voice Access für Contoso, Ltd."

Wenn Sie diese Begrüßung anpassen möchten, müssen Sie zuerst eine entsprechende Ansage aufzeichnen, diese als WAV-Datei speichern und dann den Wählplan so konfigurieren, dass diese Begrüßung verwendet wird. Die Länge des Dateinamens und Pfads darf 255 Zeichen nicht überschreiten.

Sie können eine angepasste Begrüßung hinzufügen, indem Sie auf **Ändern** und dann auf **Durchsuchen** klicken, um eine zuvor aufgezeichnete angepasste Ansage auszuwählen und die Audiodatei (WAV)

anzugeben, die für den Willkommensgruß verwendet werden soll. Wenn Sie keine Audiodatei angeben, wird für Outlook Voice Access-Anrufer eine Standardbegrüßung mit folgendem Text abgespielt: "Willkommen. Sie sind mit Microsoft Exchange verbunden."

- **Informationsansage:** Bei Aktivierung dieses optionale Aufzeichnung wiedergegeben wird, unmittelbar nach der Business oder Begrüßung während der Geschäftszeiten. Eine Informationsansage möglicherweise angegeben, dass der Organisation Sicherheitsrichtlinien für den Zugriff auf das System, z. B. "beim Zugriff auf unser System mithilfe von Outlook Voice Access, Sie haben die Begriffe der unsere Business Vereinbarung und alle Sicherheitsrichtlinien für zugestimmt unserer Organisation gelten. Zugriff auf unser System wird überwacht und unzulässige Zugriff verfolgt werden." Eine Informationsansage kann auch Informationen bereitzustellen, die für die Einhaltung von Unternehmensrichtlinien, beispielsweise erforderlich "Anrufe für Schulungszwecke überwacht werden können." Wenn sie so wichtig ist, dass die gesamte Informationsansage Anrufer hören, können sie wie unterbrechungsfreie markiert.

Standardmäßig ist für UM-Wählpläne keine Informationsansage konfiguriert. Wenn Sie eine Informationsansage aktivieren und eine auf Ihre Organisation abgestimmte benutzerdefinierte Audiodatei verwenden möchten, klicken Sie auf **Ändern** und dann auf **Durchsuchen**.

- **Ankündigung zu einer Unterbrechung zulassen:** Aktivieren Sie dieses Kontrollkästchen, damit der Benutzer Outlook Voice Access die Informationsansage unterbrechen kann. Sie sollten dies tun, wenn Sie lange Informationszwecken Ankündigungen verfügen. Outlook Voice Access-Benutzer sind möglicherweise enttäuscht, wenn die Informationsansage lang ist und sie können nicht unterbrechen, um Optionen für die von dem um-Wählplan bereitgestellten aufrufen.
- **Outlook Voice Access-Nummern:** Verwenden Sie dieses Feld Hinzufügen einer Telefon- oder Durchwahlnummer Nummer oder einen SIP-URI, mit denen ein Outlook Voice Access-Benutzer Zugriff auf das Voice Mail-System mithilfe von Outlook Voice Access aufgerufen wird. Geben Sie in den meisten Fällen einer Durchwahlnummer oder eine externe Telefonnummer. Jedoch, da dieses Feld alle alphanumerische Zeichen zulässt, können einen SIP-URI verwendet werden, wenn Sie eine IP-Nebenstellenanlage, Office Communications Server 2007 R2 oder Microsoft Lync Server verwenden.

Beim Erstellen eines Wählplans werden standardmäßig keine Outlook Voice Access-Nummern definiert. Sollen Outlook Voice Access-Benutzer in der Lage sein, sich in Outlook Voice Access einzuhören, müssen Sie mindestens eine Telefonnummer konfigurieren. Die Nummer darf nicht mehr als 20 alphanumerische Zeichen enthalten.

Wenn Sie diese Nummer für den Wählplan konfigurieren, wird diese Nummer in Microsoft Office Outlook 2007 oder höher und Outlook Web App für Voice Mail-Optionen angezeigt.

Um eine neue Outlook Voice Access-Nummer hinzuzufügen, geben Sie die Nummer in das Feld, und klicken Sie auf **Hinzufügen**  Klicken Sie auf **Entfernen**, um eine Outlook Voice Access-Nummer zu entfernen, .

7. **Einstellungen:** Verwenden Sie diese Seite, um Wähleinstellungen für Unified Messaging konfiguriert. Beim Konfigurieren von Einstellungen auf dieser Seite können Sie steuern, wie Outlook Voice Access-Benutzer und externe Anrufer, die bei einer automatischen Telefonzentrale mit dem Wählplan verknüpft aufrufen Benutzer in Ihrer Organisation, die Audiocodec zu finden, die für Voicemail-Nachrichten, die Anzahl der verwendet wird Anmeldung mit Fehlern und Timeoutwerte. Sie können die folgenden konfigurieren:

- **Bevorzugte Methode, um nach Namen zu suchen:** mit dieser Liste können Sie die primäre Methode wählen, Anrufer einen Benutzer finden können, wenn sie in das System einwählen.

Standardmäßig ist **Nachname Vorname** ausgewählt. Bei dieser Einstellung geben Benutzer bei der Suche nach Benutzern im Verzeichnis zuerst den Nachnamen und dann den Vornamen ein.

Wenn ein Outlook Voice Access-Benutzer eine Outlook Voice Access-Nummer für den Zugriff auf sein Postfach anruft, ein Anrufer eine Outlook Voice Access-Nummer zum Durchführen einer Verzeichnissuche

anruft oder ein Anrufer eine mit einem UM-Wählplan verknüpfte automatische Telefonzentrale anruft, können diese Benutzer nach einem Benutzer im Verzeichnis suchen, indem sie den Namen oder den Alias dieses Benutzers buchstabieren.

Sie müssen eine der unterstützten Methoden auswählen, um die primäre Methode für Wahl nach Namen verwenden zu können. Die folgenden Methoden werden unterstützt:

- **Nachn., Vorn. (Standardeinstellung)**
- **Vorname Nachname**
- **SMTP-Adresse**
- **Sekundäre Weise zu suchenden Namen:** mit dieser Liste können Sie die sekundäre Methode wählen, Anrufer einen Benutzer finden können, wenn sie in das System einwählen.

Standardmäßig ist **SMTP-Adresse** ausgewählt. Wenn ein Benutzer nach einem Benutzer im Verzeichnis sucht, gibt er bei dieser Einstellung den E-Mail-Alias oder die SMTP-Adresse des Benutzers ein.

Wenn ein Outlook Voice Access-Benutzer eine Outlook Voice Access-Nummer für den Zugriff auf sein Postfach anruft, ein Anrufer eine Outlook Voice Access-Nummer zum Durchführen einer Verzeichnissuche anruft oder ein Anrufer eine mit einem UM-Wählplan verknüpfte automatische Telefonzentrale anruft, können diese Benutzer nach einem Benutzer im Verzeichnis suchen, indem sie den Namen oder den Alias dieses Benutzers buchstabieren. Wenn Sie eine dieser Optionen auswählen, können Anrufer die primäre oder die sekundäre Methode für die Namenssuche verwenden, um nach Benutzern im Verzeichnis zu suchen.

Sie müssen keine der vier unterstützten Methoden auswählen. Wenn Sie keine sekundäre Methode für die Suche nach Benutzern auswählen, können Anrufer nur eine Methode für diese Suche nutzen. Die folgenden Optionen sind verfügbar:

- **Nachname Vorname**
- **Vorname Nachname**
- **SMTP-Adresse (Standard)**
- **Keine**
- **Audiocodec:** mit dieser Liste können Sie den AudioCodec auszuwählen, die von den Wählplan verwendet werden soll. Wenn ein Anrufer einen Anruf an einen Benutzer platziert, die den Wählplan zugeordnet ist und bewirkt, dass eine Sprachnachricht Unified Messaging verwendet den AudioCodec, den Sie aus dieser Liste aufzeichnen Sprachnachrichten auswählen, die an e-Mail-aktivierte Benutzer gesendet wird. Die folgenden AudioCodecs werden unterstützt:
  - **MP3 (Standardeinstellung)**
  - **WMA (Windows Media Audio)**
  - **G711 (Pulse Code Modulation (PCM) Linear)**
  - **GSM (Group System Mobile 06.10)**

Standardmäßig ist das MP3-Format ausgewählt. Das MP3-Format ist ein gängiges Audiodateiformat, das zum weitreichenden Verkleinern der Audiodatei dient und auf MP3-Playern und anderen Audiogeräten weite Verbreitung gefunden hat. MP3 ist ein plattformübergreifender AudioCodecTyp, der mit vielen Mobiltelefonen und -geräten sowie verschiedenen Computerbetriebssystemen kompatibel ist.

WMA wird wegen seiner besonders starken Komprimierung verwendet und hat qualitativ hochwertige Formateigenschaften. G.711 PCM Linear ist ein AudioCodecformat mit Telefonqualität, das den niedrigsten

Komprimierungsgrad und die geringste Formatqualität hat. GSM 06.10 ist ein AudioCodecformat, das von Mobiltelefonherstellern verwendet wird. Dieses Format wird als Standard bei digitalen Mobilfondiensten benutzt.

Wenn Sie Bedenken bezüglich der Datenträgerkapazität von Benutzern haben, wählen Sie WMA als AudioCodec aus. Die Größe von Sprachnachrichten reduziert sich auf ungefähr die Hälfte, wenn diese im WMA-Format statt mit einem der anderen AudioCodecs gespeichert werden.

- **Operator-Erweiterung:** Verwenden Sie dieses Textfeld, um die Telefonnummer oder einer Durchwahlnummer für den Wählplan Operator einzugeben. Dies ist anders als Erweiterung Operator, die für eine automatische um-Telefonzentrale konfiguriert ist. Jedoch können Sie in die gleiche Anzahl von Telefon oder Erweiterung für beide Arten von Operatoren einfügen.

Sie können diese Einstellung so konfigurieren, dass die Anrufe ggf. an eine automatische Telefonzentrale, eine Vermittlungskraft, externe Rufnummern oder Durchwahlnummern umgeleitet werden.

Wenn ein Anrufer bei Verwendung der Telefontastatur die Null (0) drückt oder "Empfang" oder "Vermittlungsstelle" sagt, oder wenn der Schwellenwert **Anzahl der Eingabefehler vor dem Trennen der Verbindung** überschritten wird, wird der Anrufer an die in diesem Textfeld angegebene Telefon- oder Durchwahlnummer weitergeleitet.

Bei der Telefonnummer kann es sich um eine externe Telefonnummer oder eine interne Durchwahl handeln. Wenn die Durchwahl zum Empfang oder zur Vermittlungsstelle 81964 lautet und Ihre Organisation nur einen Satz mit Wähleinstellungen verwendet, geben Sie 81964 ein.

Diese Einstellung enthält standardmäßig keinen Wert. Wenn Sie in dieses Feld keine Nummer eingeben, können keine Anrufe an die Vermittlungsstelle umgeleitet werden, und der Anruf wird auf höfliche Weise beendet, da niemand den Anruf entgegennehmen kann.

Es wird empfohlen, in diesem Feld eine Telefonnummer einzugeben, die Anrufer an eine Vermittlung weiterleitet, wenn der entsprechende Benutzer im Verzeichnis nicht erreichbar ist.

- **Anzahl der Anmeldung Fehler vor dem Trennen:** Verwenden Sie dieses Textfeld, um die Nummer des aufeinander folgender fehlgeschlagener Anmeldeversuche zulässig sind, bevor ein Anrufer getrennt wird.

Der Wertbereich dieser Einstellung ist 1 bis 20. Bei einem zu niedrigen Wert reagieren Benutzer unter Umständen verärgert. Für die meisten Organisationen sollte dieser Wert auf die Standardeinstellung von drei Versuchen festgelegt werden.

- **Timeouts und Wiederholungsversuche:** Diese Einstellungen gelten für Outlook Voice Access-Benutzer und externe Anrufer, die in einer automatischen UM-Telefonzentrale anrufen.
- **Maximale Dauer (in Minuten) des Anrufs:** Verwenden Sie dieses Textfeld, um die maximale Anzahl von Minuten einzugeben, das ein eingehender Anruf verbunden werden kann, das System ohne um eine gültige Durchwahlnummer übertragen wird, bevor der Anruf beendet wird. In den meisten Unternehmen sollte dieser Wert auf den Standardwert von 30 Minuten festgelegt werden.

Diese Einstellung gilt für alle Arten von Anrufen. Dazu zählen eingehende Outlook Voice Access-Anrufe, interne Sprachanrufe innerhalb der Organisation sowie Sprachanrufe und eingehende Faxanrufe von außerhalb der Organisation.

Der Wertebereich dieser Einstellung ist 10 bis 120. Wenn Sie diesen Wert zu niedrig ansetzen, werden eingehende Anrufe möglicherweise vor ihrem Abschluss unterbrochen. Wenn Ihre Organisation beispielsweise lange Faxnachrichten erhält, sollten Sie diesen Wert höher als den Standardwert festlegen, damit alle Seiten der Faxnachricht empfangen werden.

- **Maximale Dauer (in Minuten) aufzeichnen:** Verwenden Sie dieses Textfeld, geben die maximale zulässige Anzahl von Minuten für jede Stimme aufzeichnen, wenn ein Anrufer eine Voicemailnachricht

verlässt. In den meisten Unternehmen sollte dieser Wert auf den Standardwert von 20 Minuten festgelegt werden.

Der Wertebereich dieser Einstellung ist 1 bis 100. Wenn Sie diesen Wert zu niedrig ansetzen, werden lange Sprachnachrichten möglicherweise vor ihrem Abschluss unterbrochen. Wird dieser Wert zu hoch eingestellt, können Benutzer übermäßig lange Sprachnachrichten im Posteingang speichern.

Diese Einstellung ist wichtig, wenn Sie strikte Datenträgerkontingente für Benutzer eingerichtet haben. Dieser Wert muss unter dem der Einstellung **Maximale Anrufdauer (Minuten)** liegen.

- **Aufzeichnung im Leerlauf Timeout (Sekunden):** Verwenden Sie dieses Textfeld, um die Anzahl der Sekunden Pause einzugeben, die das System ermöglicht, wenn eine Sprachnachricht aufgezeichnet wird, bevor der Anruf beendet wird. In den meisten Unternehmen sollte dieser Wert auf den Standardwert von 5 Sekunden festgelegt werden.

Der Wertebereich dieser Einstellung ist 2 bis 10. Wenn Sie diesen Wert zu niedrig ansetzen, trennt das System möglicherweise die Verbindung, bevor die Sprachnachricht vollständig ist. Bei einer zu hohen Einstellung dieses Werts können Sprachnachrichten zu lange Pausen enthalten.

- **Anzahl der Eingabefehler vor dem Trennen:** Verwenden Sie dieses Textfeld, wie oft so konfiguriert, dass Anrufer falsche Menüoptionen eingeben können, bevor sie getrennt sind. In den meisten Unternehmen sollte dieser Wert auf den Standardwert von drei Versuche festgelegt werden. Dies ist eine wichtige Einstellung für um-Wählpläne sprachaktivierte.

Ein Eingabefehler entsteht beispielsweise, wenn ein Anrufer eine nicht im System gefundenen Durchwahl anfordert, das System die Durchwahl des Benutzers zum Weiterleiten des Anrufs nicht erreichen kann oder der Anrufer eine nicht zulässige Menüoption drückt.

Der Wertebereich dieser Einstellung ist 1 bis 20. Bei einem zu niedrigen Wert wird die Verbindung des Anrufers möglicherweise vorzeitig getrennt.

- **Sprache:** mit dieser Liste können Sie die Standardsprache von Outlook Voice Access-Benutzer verwendet werden. Diese Einstellung wird nicht auf die Einstellung für die Sprache auf einer automatischen UM-Telefonzentrale angewendet. Sie können festlegen, dass die Sprache für Outlook Voice Access oder mit diesem identisch unterschiedliche von der Sprache sein, die auf eine automatische um-Telefonzentrale verwendet wurde. Wenn ein Benutzer einen Anruf an einen Benutzer, die zu einem Wählplan verknüpft ist tätigt, ist die audio Sprache als Standardsprache, die den VoIP-aufgezeichnet-Operator verwendet. Fordert das System, die Anrufer hören sind in der gleichen Sprache wiedergegeben. Die Sprache, die dem um-Wählplan ausgewählt sind wird zum Lesen von e-Mail, Voicemail und Kalenderelemente verwendet. um den Namen des Benutzers angenommen, wenn eine persönliche noch nicht Ansage aufgezeichnet wurde. Um eine Sprachnachricht mit dem Feature Voicemailvorschau aufzuzeichnen; und so aktivieren Sie die automatische Spracherkennung Spracherkennung (ASR) ordnungsgemäß funktioniert.

Wenn bei lokalen Bereitstellungen weitere Sprachen hinzugefügt werden, kann Outlook Voice Access eine andere Sprache anstelle von Englisch (USA) verwenden. Wenn ein Outlook Voice Access-Benutzer beispielsweise über eine Outlook Voice Access-Nummer von einem Tischtelefon aus anruft, wird eine vorab aufgezeichnete Ansage der Vermittlungsstelle in englischer Sprache abgespielt. Selbst wenn derselbe Benutzer eine andere Sprache (z. B. Französisch) in Outlook Web App auswählt, erfolgen die Menüansagen weiterhin auf Englisch (USA). Damit der Benutzer die aufgezeichneten Menüs in französischer Sprache abrufen kann, müssen Sie das entsprechende Sprachpaket installieren.

#### NOTE

Für Exchange Online sind alle Sprachen verfügbar.

8. **Wählregeln:** Verwenden Sie diese Seite Wählregeln für nationale/regionale und internationale von UM-

aktivierte Benutzer getätigten Anrufe an. Jeder Eintrag für die Einwahl Regel definiert bestimmt die Arten von Anrufen, die Benutzer in einer bestimmten Wählvorgang Regelgruppe vornehmen können. Nachdem Sie die Seite **Wählregeln** Wählregeln konfigurieren mithilfe, müssen Sie den UM-Wählplan, einer um-Postfachrichtlinie oder einer automatischen UM-Telefonzentrale, um die entsprechende Wählvorgang Regel verwenden konfigurieren. Nach dem Konfigurieren der UM-Postfachrichtlinie, um eine Wählvorgang Regelgruppe verwenden, gelten der Wählvorgang Einschränkungen konfiguriert für alle UM-aktivierten Benutzer, die die um-Postfachrichtlinie zugeordnet sind. Beispielsweise können Sie eine Gruppe der Wählvorgang Regel konfigurieren, die Benutzer nicht, die der Wähleinstellungen eine Amtskennziffer einwählen benötigen, wenn sie einen an eine Telefonnummer für Land/Region Anruf zugeordnet sind. Sie können die folgenden konfigurieren:

- **Nationale/regionale Wählregeln:** Verwenden Sie dieses Feld hinzufügen, entfernen oder Bearbeiten von UM-Postfachrichtlinien verwendete nationale/regionale Wählregelgruppen. Klicken Sie auf **Hinzufügen**, um eine Regel Wählvorgang zu erstellen, [ ]. Klicken Sie auf **Bearbeiten**, um eine vorhandene Regel Wählvorgang zu bearbeiten, [ ]. Wenn eine Regel Wählvorgang entfernen möchten, klicken Sie auf **Entfernen** [ ]. Beim Erstellen einer Wählregel, fügen Sie die folgenden Informationen auf der Seite **neue Wählvorgang Regel** hinzu:
  - **Wählen Sie Regelname:** Verwenden Sie dieses Textfeld zur Eingabe des Namens für die Wählregel Sie erstellen. Sie können den gleichen Namen sammeln mehrere Regeln in einer Gruppe, und klicken Sie dann aktivieren oder deaktivieren sie unter **wählberechtigungen**. Der Name kann bis zu 32 Zeichen lang sein.
  - **Nummernmuster zur Transformation von (Zahl Maske):** Verwenden Sie dieses Textfeld, um das Nummernmuster vor dem wählen, beispielsweise 91425xxxxxx umgewandelt einzugeben. Wenn ein Benutzer eine Zahl, die diesem Muster entspricht eingibt, wird UM die Rufnummer in einer gewählten Rufnummer angerufene den Anruf entgegennehmen umgewandelt. Sie können nur eingeben, Zahlen und dem Platzhalterzeichen, "x".
  - **Anzahl der Dialed:** Verwenden Sie dieses Textfeld eingeben die Nummer, die Sie anwählen möchten, der das Nummernmuster Sie, in dem **Muster entspricht (Zahl Maske) umgewandelt festlegen**. Die gewählte Nummer wird verwendet, um die tatsächliche Dial Zeichenfolge gesendet, um die VoIP-Gateway oder IP-PBX zu bestimmen. Diese Nummer kann von der Anzahl von Unified Messaging für den ausgehenden Anruf abgerufen abweichen. Allerdings Ihre PBX- oder IP-PBX kann auch die Vorwahl für Ortsgespräche ausgelassen werden, konfiguriert werden und für die private VoIP Nummerierung Pläne konfiguriert werden kann. Keine Platzhalterzeichen ( X) in der Zeichenfolge für die Einwahl werden durch die Ziffern, aus der ursprünglichen Zahl ersetzt, die von der Anzahl Maske für die Einwahl Regel gefunden wurden. Ein Beispiel für eine gültige gewählte Nummer ist 9 Xxxxxx. In diesem Feld kann nur Zahlen und das Zeichen \_X\_ enthalten.
  - **Kommentar:** Verwenden Sie dieses Textfeld um in einen Kommentar oder eine Beschreibung für die Einwahl-Regel, die Sie hinzufügen oder ändern zu platzieren. In der Standardeinstellung ist dieses Feld leer.

#### NOTE

Wenn Sie eine Integration mit Office Communications Server 2007 R2 oder Microsoft Lync Server durchführen, ist es möglicherweise nicht notwendig, Wählregeln oder Wählregelgruppen in Unified Messaging zu konfigurieren. Office Communications Server 2007 R2 und Lync Server sind so konzipiert, dass sie Anrufl Weiterleitung und Nummernübersetzung für Benutzer in Ihrer Organisation ausführen, und übernehmen diese Aufgaben auch, wenn Anrufe im Namen von Benutzern getätigten werden.

- **Internationale Regeln:** Verwenden Sie dieses Textfeld, um hinzufügen, entfernen oder Bearbeiten von UM-Postfachrichtlinien verwendete internationale Wählregelgruppen.
- **Wählen Sie Regelname:** Verwenden Sie dieses Textfeld zur Eingabe des Namens für die Wählregel Sie

erstellen. Sie können den gleichen Namen sammeln mehrere Regeln in einer Gruppe, und klicken Sie dann aktivieren oder deaktivieren sie unter **wählberechtigungen**. Der Name kann bis zu 32 Zeichen lang sein.

- **Nummernmuster zur Transformation von (Zahl Maske):** Verwenden Sie dieses Textfeld, um das Nummernmuster vor dem wählen, beispielsweise 91425xxxxxx umgewandelt einzugeben. Wenn ein Benutzer eine Zahl, die diesem Muster entspricht eingibt, wird UM die Rufnummer in einer gewählten Rufnummer angerufene den Anruf entgegennehmen umgewandelt. Sie können nur eingeben, Zahlen und dem Platzhalterzeichen, "x".
- **Anzahl der Dialed:** Verwenden Sie dieses Textfeld eingeben die Nummer, die Sie anwählen möchten, der das Nummernmuster in **Nummernmuster zur Transformation von (Zahl Maske)** festgelegt entspricht. Die gewählte Nummer wird verwendet, um die tatsächliche Dial Zeichenfolge gesendet, um die VoIP-Gateway oder IP-PBX zu bestimmen. Diese Nummer kann von der Anzahl von Unified Messaging für den ausgehenden Anruf abgerufen abweichen. Allerdings Ihre PBX- oder IP-PBX kann auch die Vorwahl für Ortsgespräche ausgelassen werden, konfiguriert werden und für die private VoIP Nummerierung Pläne konfiguriert werden kann. Keine Platzhalterzeichen ( X) in der Zeichenfolge für die Einwahl werden durch die Ziffern, aus der ursprünglichen Zahl ersetzt, die von der Anzahl Maske für die Einwahl Regel gefunden wurden. Ein Beispiel für eine gültige gewählte Nummer ist 9 Xxxxxx. In diesem Feld kann nur Zahlen und das Zeichen \_X\_ enthalten.
- **Kommentar:** Verwenden Sie dieses Textfeld um in einen Kommentar oder eine Beschreibung für die Einwahl-Regel, die Sie hinzufügen oder ändern zu platzieren. In der Standardeinstellung ist dieses Feld leer.

#### NOTE

Wenn Sie bei lokalen Bereitstellungen eine Integration mit Office Communications Server 2007 R2 oder Microsoft Lync Server durchführen, ist es möglicherweise nicht notwendig, Wählregeln oder Wählregelgruppen in Unified Messaging zu konfigurieren. Office Communications Server 2007 R2 und Lync Server sind so konzipiert, dass sie Anruferleiterung und Nummernübersetzung für Benutzer in Ihrer Organisation ausführen, und übernehmen diese Aufgaben auch, wenn Anrufe im Namen von Benutzern getätigt werden.

9. **Wählen Sie die Autorisierung:** Verwenden Sie diese Seite Auswahl Wählregeln für Anrufer, die auf einem um-Wählplan konfiguriert eine Outlook Voice Access-Nummer anrufen. Sie können den Typ der Anrufe von Anrufer, wenn ein nicht authentifizierter Benutzer oder eine Outlook Voice Access-Benutzer an eine Outlook Voice Access-Nummer auf einem Wählplan konfiguriert ist, Konfigurieren von Wählregelgruppen und Wählvorgang Einschränkungen aufruft, einschränken. Sie können die folgenden konfigurieren:

- **Anrufe in die gleiche UM-Wählplan:** Aktivieren Sie dieses Kontrollkästchen, um Benutzern zu ermöglichen, die auf einem Wählplan konfiguriert eine Outlook Voice Access-Nummer anrufen tätigen oder durchstellen von Anrufen an eine Durchwahlnummer ein UM-aktivierten Benutzer innerhalb desselben Wählplans zugeordnet. Diese Einstellung ist standardmäßig aktiviert.

Wenn Sie diese Einstellung deaktivieren, sind Benutzer, die über die Outlook Voice Access-Nummer anrufen, nicht in der Lage, Anrufe an Benutzer ohne UM-Aktivierung, an andere Durchwahlnummern oder an UM-aktivierte Benutzer zu senden oder weiterzuleiten, die demselben Wählplan zugeordnet sind. Der Grund dafür ist, dass die Einstellung **Anrufe an jede Durchwahl zulassen** standardmäßig deaktiviert ist.

- **Zulassen von Anrufen an eine beliebige Erweiterung:** Wenn diese Einstellung deaktiviert ist, können nicht Benutzer, die eine Outlook Voice Access-Nummer des Wählplans anrufen Anrufe werden nicht UM-aktivierten Benutzern oder andere keinem UM-aktivierten Benutzer zugeordneten Durchwahlnummern platzieren. Sie können jedoch einen Anruf tätigen oder Weiterleiten eines Anrufs an Durchwahlnummern UM-aktivierten Benutzer zugeordnet. Dies ist, da die **Anrufe in demselben UM-Wählplans** Einstellung standardmäßig aktiviert ist. Die Einstellung für **jede Erweiterung aufrufen zulassen** ist standardmäßig deaktiviert.

#### **NOTE**

Um versuchte Betrug und andere potenziellen Bedrohungen für Unified Messaging-Umgebung zu vermeiden, befolgen Sie die Anweisungen in den Blogbeitrag [ist Ihre Exchange Unified Messaging vor Telekommunikation Betrug geschützt?](#)

Wenn diese Einstellung aktiviert ist, können Benutzer, die über eine im Wählplan konfigurierte Outlook Voice Access-Nummer anrufen, Anrufe mit Benutzern ohne UM-Aktivierung, mit anderen Durchwahlnummern, die keinem UM-aktivierten Benutzer zugeordnet sind, und mit UM-aktivierten Benutzern führen. Der Grund dafür ist, dass die Einstellung **Anrufe im gleichen UM-Wählplan** standardmäßig aktiviert ist.

Diese Einstellung kann in einer Umgebung aktiviert werden, in der nicht alle Benutzer UM-aktiviert sind. Sie ist außerdem nützlich, wenn Sie zulassen möchten, dass Benutzer, die über eine Outlook Voice Access-Nummer anrufen, die in einem Wählplan konfiguriert ist, Durchwahlnummern anrufen können, die nicht zugeordnet sind.

- **Autorisierte nationale/regionale Wählregelgruppen:** Verwenden Sie diesen Abschnitt zum Hinzufügen oder Entfernen von zulässigen nationale/regionale Wählregeln. Standardmäßig sind keine nationale/regionale Wählregeln auf um-Wählpläne konfiguriert.

Mithilfe von nationalen/regionsinternen Wählregelgruppen kann der Zugriff auf Telefonnummern in einem Land oder einer Region zugelassen oder eingeschränkt werden, die ein Benutzer, der die Teilnehmerzugriffsnummer gewählt hat, wählen kann. Diese Maßnahme hilft, unnötige bzw. nicht autorisierte Telefonate und Gebühren zu vermeiden.

Damit Sie nationale Wählregeln hinzufügen können, müssen Sie zuerst die entsprechende nationale Wählregel im Wählplan erstellen und dann der Wählregel die entsprechenden Wählregeleinträge hinzufügen. Nachdem Sie die erforderlichen Wählregeln im Wählplan erstellt haben, müssen Sie die Wählregeln im Wählplan auf der Registerkarte **Wählautorisierungen** der Liste der Wählautorisierungen hinzufügen.

Nationale/regionsinterne Wählregelgruppen können verwendet werden, um den Zugriff auf Rufnummern in einem Land oder einer Region zuzulassen oder einzuschränken. Dies gilt für alle Benutzer, die bei einer Outlook Voice Access-Nummer angerufen haben.

- **Internationale Wählregelgruppen autorisiert:** Verwenden Sie diesen Abschnitt zum Hinzufügen oder Entfernen von internationalen Wählregeln zulässig. Standardmäßig sind keine internationale Wählregeln auf um-Wählpläne konfiguriert.

Mithilfe von internationalen Wählregeln können die internationalen Telefonnummern zugelassen oder eingeschränkt werden, die ein Benutzer wählen kann, der sich über die Outlook Voice Access-Nummer eingewählt hat. Diese Maßnahme hilft, unnötige bzw. nicht autorisierte Telefonate und Gebühren zu vermeiden.

Damit Sie internationale Wählregelgruppen hinzufügen können, müssen Sie zuerst die entsprechenden internationalen Wählregeln im Wählplan erstellen und dann die entsprechenden Wählregeleinträge hinzufügen. Nachdem Sie die erforderlichen Wählregeln im Wählplan erstellt haben, müssen Sie die Wählregeln im Wählplan auf der Registerkarte **Wählautorisierungen** der Liste der Wählautorisierungen hinzufügen.

Internationale Wählregelgruppen können verwendet werden, um den Zugriff auf Rufnummern außerhalb eines Landes oder einer Region zuzulassen oder einzuschränken. Dies gilt für alle Benutzer, die bei einer Outlook Voice Access-Nummer angerufen haben.

10. **Übertragung & Suche:** mit dieser Seite können Sie um die UM Dial Plan Funktionen zu konfigurieren.

Verschiedene Features können auf dem um-Wählplan konfiguriert werden. Weiterleiten von Anrufen, Sprachnachrichten senden und Suche nach Benutzern beinhalten. Sie können die folgenden konfigurieren:

- **Anrufer zulassen:** Verwenden Sie diese Einstellungen, um zu bestimmen, wie Benutzer, die eine Outlook Voice Access-Nummer anrufen Benutzer wenden können. Sie können die folgenden konfigurieren:
- **Weiterleitung an Benutzer:** Aktivieren Sie dieses Kontrollkästchen, damit Outlook Voice Access Benutzer Anrufe an Benutzer übertragen können. Diese Option ist standardmäßig aktiviert. Auf diese Weise können Benutzer, die der Dial Plan Übertragung Anrufe für Benutzer in der gleichen UM-Wähleinstellungen. Nachdem Sie dieses Kontrollkästchen aktivieren, können Sie die Gruppe von Benutzern festlegen, die Anrufer für durchsuchen können, indem Sie die entsprechende Option im Abschnitt **Zulassen Anrufer zu suchenden Benutzer nach Name oder Alias** auf dieser Seite auswählen.

Wenn Sie diese Option deaktivieren, lässt Outlook Voice Access für keinen Benutzer zu, dass er an einen anderen Benutzer im Wählplan weitergeleitet wird.

- **Sprachnachrichten ohne eines Benutzers Telefon klingeln lassen:** Aktivieren Sie dieses Kontrollkästchen, um Anrufer Sprachnachrichten an Benutzer senden aktivieren. Diese Option ist standardmäßig aktiviert. Auf diese Weise können Outlook Voice Access-Benutzer, die in der gleichen um-Wählplan Dial Plan senden Sprachnachrichten für Benutzer zugeordnet sind. Nachdem Sie dieses Kontrollkästchen aktivieren, können Sie die Gruppe von Benutzern festlegen, die Anrufer für durchsuchen können, indem Sie die entsprechende Option im Abschnitt **Zulassen Anrufer zu suchenden Benutzer nach Name oder Alias** auf dieser Seite auswählen.

Wenn Sie diese Option deaktivieren, gibt Outlook Voice Access Anrufern in einer Systemansage nicht die Möglichkeit, eine Sprachnachricht zu senden.

- **Anrufer zulassen nach Benutzern nach Name oder Alias zu suchen:** Verwenden Sie diese Optionen, um eine Gruppierung von Benutzern zu bestimmen, die durchsucht werden können. Standardmäßig ist die Option **In diesen Wähleinstellungen nur** ausgewählt. Sie können jedoch die Gruppierung von Benutzern ändern. Wählen Sie die folgenden Optionen aus:

- **In diesen Wähleinstellungen nur:** Verwenden Sie diese Option, um zuzulassen, Anrufer, die mit Outlook Voice Access zu suchen, und wenden Sie sich an Benutzer, die innerhalb der Wähleinstellungen sind planen, dass sie Mitglied sind.
- **In der gesamten Organisation:** Verwenden Sie diese Option, ob Anrufer können eine Verbindung zu Outlook Voice Access zu suchen, und wenden Sie sich an Personen in der gesamten Organisation aufgeführt ist. Dies umfasst alle Benutzer, die Postfach aktiviert sind, oder UM-aktivierten Benutzer in allen Wählplänen.
- **Nur für diese automatische Telefonzentrale:** mit dieser Liste können Benutzer eine Verbindung mit einer automatischen UM-Telefonzentrale und verbinden Sie dann potenziell an eine andere automatische Telefonzentrale Sie Outlook Voice Access konfiguriert haben. Sie müssen diese automatische Telefonzentrale damit Aufrufer an eine andere automatische Telefonzentrale übertragen werden, der angegeben wird, erstellen.
- **Nur für diese Erweiterung:** Verwenden Sie diese Option, damit Outlook Voice Access-Benutzer mit einer Durchwahlnummer verbinden, die Sie in das Feld für diese Option angeben. In diesem Feld kann nur numerische Ziffern. Die Anzahl der Ziffern, die in diesem Feld definiert, muss die Anzahl der Nachkommastellen für den Wählplan zugeordnet der automatischen Telefonzentrale konfiguriert übereinstimmen.
- **Für Benutzer mit dem gleichen Namen einzufügenden Informationen:** mit diesem Feld können Sie auswählen, wie die Wähleinstellungen zwischen Benutzern unterschieden wird, die die gleichen oder ähnlichen Namen haben. Wenn ein Anrufer aufgefordert wird, um Buchstaben einzugeben oder zu sagen Sie den Namen der Person um einen bestimmten Benutzer in der Organisation zu finden, entspricht

Eingabe, die in einigen Fällen mehr als einen Namen des Anrufers. Wenn zwei Benutzer mit dem gleichen Namen vorhanden sind, werden UM eine der folgenden Methoden zusätzliche Informationen zu den Namen des Benutzers hinzufügen verwenden. Beispielsweise bei Auswahl von **Abteilung**, wenn ein Outlook Voice Access-Benutzer Outlook Voice Access und sucht nach einem Benutzer ruft und doppelte oder ähnliche Namen in das Verzeichnis vorhanden sind, wird der Anrufer Name und Abteilung des Benutzers beispielsweise hören:

1. System: "Willkommen bei Outlook Web Access. Geben Sie bitte Ihre PIN ein, und drücken Sie die Rautetaste."
2. Der Anrufer gibt seine PIN ein, und drückt die Rautetaste (#).
3. System: "Bitte sagen Sie Sprachnachricht, E-Mail, Kalender, persönliche Kontakte, Verzeichnis oder persönliche Optionen."
4. Anrufer: "Verzeichnis"
5. System: "Verzeichnissuche. Für die folgenden Aufgaben müssen Sie die Tastatur Ihres Telefons benutzen, eine Spracheingabe ist nicht möglich. Buchstabieren Sie über die Tastatur entweder den Namen der Person, nach der Sie suchen möchten, dabei zuerst den Nachnamen, oder den ersten Teil der E-Mail-Adresse der Person, und drücken Sie zweimal die Rautetaste. Wenn Sie die Durchwahl kennen, drücken Sie die Rautetaste."
6. Der Aufrufer gibt über die Telefontastatur "smithtony" ein und drückt die #-Taste.
7. System: "Für Tony Smith, Forschung, drücken Sie die 1. Für Tony Smith, Verwaltung, drücken Sie die 2. Für Tony Smith, Technischer Support, drücken Sie die 3."
8. Der Anrufer drückt die entsprechende Taste auf der Tastatur, und der Anruf wird an den Benutzer weitergeleitet.

Standardmäßig übernehmen alle diesen UM-Wähleinstellungen zugeordneten automatischen UM-Telefonzentralen diese Einstellung. Sie können diese Einstellung für jede automatische UM-Telefonzentrale ändern, die Sie erstellen.

Wählen Sie eine der folgenden Methoden aus, mit deren Hilfe dem Anrufer weitere Informationen bereitgestellt werden, um ihm beim Auffinden des gewünschten Benutzers in der Organisation behilflich zu sein:

- **Keine:** keine weiteren Informationen erhält, wenn Übereinstimmungen aufgelistet werden. Diese Methode ist standardmäßig aktiviert.
  - **Titel:** das Voicemailsyste Titel des Benutzers gehört Übereinstimmungen aufgeführt sind.
  - **Abteilung:** das Voicemailsyste Abteilung des Benutzers gehört Übereinstimmungen aufgeführt sind.
  - **Speicherort:** das Voicemailsyste Standort des Benutzers gehört Übereinstimmungen aufgeführt sind.
  - **Prompt für Alias:** das Voicemailsyste fordert den Anrufer in der Aliasname des Benutzers.
11. Nachdem Sie die erforderlichen Einstellungen konfiguriert haben, klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

## Verwenden von Exchange Online PowerShell, UM-Wähleinstellungen konfiguriert

In diesem Beispiel wird einen um-Wählplan mit dem Namen konfiguriert `MyDialPlan` für die Amtskennziffer 9 verwenden.

```
Set-UMDialplan -Identity MyDialPlan -OutsideLineAccessCode 9
```

In diesem Beispiel wird einen um-Wählplan mit dem Namen konfiguriert `MyDialPlan` zu einer Begrüßung konfiguriert.

```
Set-UMDialplan -Identity MyDialPlan -WelcomeGreetingEnabled $true -WelcomeGreetingFilename welcome.wav
```

In diesem Beispiel wird einen um-Wählplan mit dem Namen konfiguriert `MyDialPlan` mit Wählregeln.

```
$csv=import-csv "C:\MyInCountryGroups.csv"  
Set-UMDialPlan -Identity MyDialPlan -ConfiguredInCountryGroups $csv  
Set-UMDialPlan -Identity MyDialPlan -AllowedInCountryGroups "local, long distance"
```

## Mithilfe von Exchange Online PowerShell Ansicht UM-Wähleinstellungen

In diesem Beispiel wird eine Liste aller UM-Wählpläne angezeigt.

```
Get-UMDialplan
```

In diesem Beispiel wird eine formatierte Liste aller Einstellungen auf einem um-Wählplan mit dem Namen `MyUMDialPlan`.

```
Get-UMDialplan -Identity MyUMDialPlan | Format-List
```

# Ändern des Audio codecs

18.12.2018 • 3 minutes to read

Unified Messaging kann einen von vier Codecs zum Erstellen von Voicemailnachrichten verwenden: MP3, Windows Media Audio (WMA), Group System Mobile (GSM) 06.10 und G.711 Pulse Code Modulation (PCM) Linear. Beim Erstellen eines Unified Messaging-Wählplans wird standardmäßig der MP3-Audiocodec verwendet, um Sprachnachrichten aufzuzeichnen. Das MP3-Audioformat ist ein beliebtes Format, das mit verschiedenen Betriebssystemen, E-Mail-Clients und MP3-Playern verwendet werden kann. Nachdem Sie den UM-Wählplan erstellt haben, können Sie ihn jedoch für die Verwendung eines anderen Audioformats (einschließlich WMA-, GSM 06.10- oder G.711 PCM Linear-Audiocodexs) konfigurieren. Zum Wiedergeben einer Sprachnachricht muss auf einem Mobiltelefon oder Computer eine kompatible Audiosoftware installiert sein.

Zusätzliche Aufgaben im Zusammenhang mit UM-Wählplänen finden Sie unter [UM Dial Plan Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern des Audio codec für Unified Messaging-Wählpläne mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Wählen Sie in **Einstellungen** unter **Audiocodec** eine der folgenden Optionen aus der Dropdownliste aus:
  - MP3
  - WMA
  - GSM
  - G711

5. Klicken Sie auf **Speichern**.

## Mit Exchange Online PowerShell so ändern Sie den Audiocodec für Unified Messaging-Wählplan

In diesem Beispiel wird den Audiocodec auf einem um-Wählplan mit dem Namen `MyUMDialPlan`, g. 711.

```
Set-UMDialPlan -Identity MyUMDialPlan -AudioCodec G711
```

In diesem Beispiel wird den Audiocodec auf einem um-Wählplan mit dem Namen `MyUMDialPlan` in WMA.

```
Set-UMDialPlan -Identity MyUMDialPlan -AudioCodec Wma
```

# Konfigurieren der maximalen Anrufdauer

18.12.2018 • 3 minutes to read

Sie können die maximale Anzahl der Minuten angeben, für die bei einem eingehenden Anruf die Verbindung mit dem System ohne Umleitung auf eine zulässige Durchwahl erhalten bleibt, bevor der Anruf abgebrochen wird. Für die meisten Organisationen sollte dieser Wert auf die Standardeinstellung festgelegt werden: 30 Minuten. Diese Einstellung gilt für alle Anrufe, u. a. eingehende Outlook Voice Access-Anrufe, interne Sprachanrufe innerhalb der Organisation, Sprachanrufe an automatische UM-Telefonzentralen (Unified Messaging) sowie Faxanrufe von außerhalb der Organisation.

Dieser Wert kann auf eine Zahl zwischen 10 und 120 festgelegt werden. Wenn Sie diesen Wert zu niedrig ansetzen, werden eingehende Anrufe möglicherweise vor ihrem Abschluss unterbrochen. Wenn Ihre Organisation beispielsweise lange Faxnachrichten erhält, sollten Sie diesen Wert höher als den Standardwert festlegen, damit alle Seiten der Faxnachricht empfangen werden.

Zusätzliche Aufgaben im Zusammenhang mit UM-Wählplänen finden Sie unter [UM Dial Plan Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der maximalen Anrufdauer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Geben Sie im Abschnitt **Einstellungen** unter **Maximale Anrufdauer (Minuten)** einen Wert in Minuten ein.
5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie die maximale Anrufdauer

In diesem Beispiel wird die maximale Anrufdauer auf 10 Minuten auf einem um-Wählplan mit dem Namen

`MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -MaxCallDuration 10
```

# Konfigurieren Sie die maximale Aufzeichnung Dauer

18.12.2018 • 3 minutes to read

Sie können die maximale Anzahl an Minuten festlegen, die pro Sprachaufzeichnung zulässig ist, wenn ein Anrufer eine Sprachnachricht hinterlässt. Dieser Wert kann auf eine Zahl von 1 bis 100 festgelegt werden. In den meisten Organisationen kann die Standardeinstellung von 20 Minuten verwendet werden. Wenn Sie diesen Wert zu niedrig ansetzen, werden lange Sprachnachrichten möglicherweise vor ihrem Abschluss unterbrochen. Wird dieser Wert zu hoch eingestellt, können Benutzer übermäßig lange Sprachnachrichten im Posteingang speichern.

Diese Einstellung ist wichtig, wenn Sie strikte Datenträgerkontingente für Benutzer eingerichtet haben. Der Wert muss unterhalb des Werts der Einstellung für **Maximale Anrufdauer (Minuten)** liegen.

Zusätzliche Aufgaben im Zusammenhang mit um-Wählpläne finden Sie unter [Planen von Verfahren UM einwählen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der maximalen Aufzeichnungsdauer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Geben Sie im Abschnitt **Einstellungen** unter **Maximale Aufzeichnungsdauer (Minuten)** einen Wert in Minuten ein.
5. Klicken Sie auf **Speichern**.

Verwenden von Exchange Online PowerShell so konfigurieren Sie die maximale Aufzeichnung Dauer

In diesem Beispiel wird die maximale Aufzeichnung Dauer auf 10 Minuten für einen UM-Wählplan mit dem Namen `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -MaxRecordingDuration 10
```

# Konfigurieren Sie den Wert der Aufzeichnung Leerlauftimeout

18.12.2018 • 2 minutes to read

Sie können die Anzahl von Sekunden festlegen, in denen beim Aufzeichnen einer Sprachnachricht geschwiegen werden darf, bevor das Telefonat beendet wird. Für die meisten Organisationen sollte dieser Wert auf die Standardeinstellung von 5 Sekunden festgelegt werden.

Sie können diesen Wert auf 2 bis 10 festlegen. Wenn Sie diesen Wert zu niedrig ansetzen, trennt das System möglicherweise die Verbindung, bevor die Sprachnachricht vollständig ist. Bei einer zu hohen Einstellung dieses Werts können Sprachnachrichten zu lange Pausen enthalten.

Zusätzliche Verwaltungsaufgaben im Zusammenhang mit UM-Wählplänen finden Sie unter [UM Dial Plan Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren des Werts "Aufzeichnungsleerlauf-Zeitüberschreitung" mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Geben Sie in **Einstellungen** unter **Aufzeichnungsleerlauf-Zeitüberschreitung (Sekunden)** den Wert in Sekunden ein.
5. Klicken Sie auf **Speichern**.

Verwenden von Exchange Online PowerShell so konfigurieren Sie den

## Timeoutwert der Aufzeichnung im Leerlauf

In diesem Beispiel wird den Wert der Aufzeichnung Leerlauftimeout bis 10 für einen UM-Wählplan mit dem Namen `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -RecordingIdleTimeout 10
```

# Konfigurieren der VoIP-Sicherheitseinstellung

18.12.2018 • 4 minutes to read

Sie können VoIP-Sicherheit (Voice over IP) für einen UM-Wählplan (Unified Messaging) aktivieren. Beim Erstellen von UM-Wählplänen verwenden diese standardmäßig den ungesicherten Modus und keine Verschlüsselung. Exchange-Server können Anrufe für einzelne oder mehrere UM-Wählpläne sowie für Wählerne annehmen, die andere VoIP-Sicherheitseinstellungen haben. In Office 365 und Exchange Online ist der abgesicherte Modus erforderlich und kann nicht deaktiviert werden.

Wenn Sie einen UM-Wählplan so konfigurieren, dass der SIP-gesicherte (Session Initiation Protocol) oder der sichere Modus verwendet wird, verschlüsseln die Exchange-Server, die Anrufe für den UM-Wählplan annehmen, den SIP-Signalverkehr (für den SIP-gesicherten Modus) oder sowohl die RTP-Medienkanäle (Realtime Transport Protocol) als auch den SIP-Signalverkehr (für den sicheren Modus).

## IMPORTANT

Wenn Sie bei lokalen und Hybridbereitstellungen den SipTCPListenPort, SipTLSListeningPort oder UMStartUpMode auf einem Clientzugriffsserver, auf dem der Microsoft Exchange Unified Messaging-Anrufrouterdienst ausgeführt wird, oder einem Postfachserver konfigurieren, auf dem der Microsoft Exchange Unified Messaging-Dienst ausgeführt wird, müssen Sie die Regeln der Windows-Firewall so konfigurieren, dass SIP- und RTP-Netzwerksdatenverkehr ordnungsgemäß zugelassen wird.

Weitere Verwaltungsaufgaben im Zusammenhang mit um-Wählpläne finden Sie unter [Planen von Verfahren UM einwählen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren von VoIP-Sicherheit für einen UM-Wählplan mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**, wählen Sie den UM-Wählplan auf dem Sie die VoIP-Sicherheit ändern möchten, und klicken Sie dann auf **Bearbeiten**.

2. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
3. Wählen Sie in **Allgemein** unter **VoIP-Sicherheitsmodus** eine der folgenden Optionen aus:
  - **SIP-gesichert**
  - **Ungesichert** (Standard)
  - **Gesichert**
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie VoIP-Sicherheit auf einem um-Wählplan

In diesem Beispiel wird einen um-Wählplan mit dem Namen konfiguriert `MySecureDialPlan` zum Verschlüsseln von SIP- und RTP-Datenverkehr.

```
Set-UMDialPlan -identity MySecureDialPlan -VoIPSecurity Secured
```

In diesem Beispiel wird einen um-Wählplan mit dem Namen konfiguriert `MySecureDialPlan` SIP verschlüsseln, aber nicht verschlüsselt RTP-Datenverkehr.

```
Set-UMDialPlan -identity MySecureDialPlan -VoIPSecurity SIPsecured
```

In diesem Beispiel wird einen um-Wählplan mit dem Namen konfiguriert `MySecureDialPlan` SIP- und RTP-Datenverkehr nicht verschlüsselt.

```
Set-UMDialPlan -identity MySecureDialPlan -VoIPSecurity Unsecured
```

# Konfigurieren eines Wählplans für Benutzer mit ähnlichen Namen

18.12.2018 • 5 minutes to read

Sie können einen UM-Wählplan (Unified Messaging) zum Angeben von Informationen konfigurieren, die für Anrufer bereitgestellt werden, wenn Benutzer denselben oder ähnliche Namen besitzen. Anhand dieser Einstellung unterscheidet UM zwischen Benutzern mit demselben oder ähnlichen Namen und stellt diese Information den Anrufern bereit. Wenn ein Anrufer oder ein Benutzer von Outlook Voice Access aufgefordert wird, Buchstaben einzugeben, um einen bestimmten Benutzer zu suchen, entsprechen manchmal mehrere Namen der Eingabe des Anrufers. Anhand einer der verfügbaren Optionen können Sie dem Anrufer weitere Informationen bereitstellen und ihm beim Auffinden des gewünschten Benutzers behilflich sein.

Diese Einstellung kann sowohl in UM-Wählplänen als auch in automatischen UM-Telefonzentralen festgelegt werden. Wenn eine automatische UM-Telefonzentrale erstellt wird, übernimmt diese die Einstellung von dem Wählplan der zugehörigen automatischen Telefonzentrale. Standardmäßig ist diese Einstellung nicht für Wählpläne konfiguriert, sodass Anrufern keine weiteren Informationen zum Auffinden des richtigen Benutzers bereitgestellt werden.

## NOTE

Damit die Informationen für Benutzer mit ähnlichen Namen ordnungsgemäß verwendet werden können, müssen Sie den Titel, die Abteilung und Standortinformationen für die Empfänger in Ihrer Microsoft Exchange-Organisation bereitstellen.

Weitere Verwaltungsaufgaben im Zusammenhang mit um-Wählpläne finden Sie unter [Planen von Verfahren UM einwählen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren eines UM-Wählplans für Benutzer mit ähnlichen Namen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der

Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**



2. Klicken Sie auf der Seite **UM-Wähleinstellungen Konfigurieren > Übertragung & Suche**, und wählen Sie unter **für Benutzer mit dem gleichen Namen einzufügenden Informationen** eine der folgenden Optionen:

- **Titel:** die Wähleinstellungen enthält die Position des Benutzers beim Auffinden von zwei oder mehr Benutzer mit ähnlichen Namen.
- **Abteilung:** die Wähleinstellungen Abteilung des Benutzers enthält, wenn es zwei oder mehr Benutzer mit ähnlichen Namen findet.
- **Speicherort:** die Wähleinstellungen enthält die Position des Benutzers beim Auffinden von zwei oder mehr Benutzer mit ähnlichen Namen.
- **None:** die Wähleinstellungen werden keine zusätzlichen Informationen einschließen, wenn Benutzer ähnliche Namen aufweisen. Obwohl dies die Standardeinstellung ist, wird empfohlen, dass Sie eine der verfügbaren Optionen für Anrufer einschließen. Wenn dies nicht der Fall, werden Anrufer kann nicht die Differenz zwischen zwei oder mehr Benutzer mit ähnlichen Namen informiert.
- **Prompt für Alias:** die Wähleinstellungen fordert den Anrufer in der Aliasname des Benutzers. Ein Alias ist der Teil des Benutzers e-Mail oder SMTP-Adresse, die vor der unter (@) Symbol.

3. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie eine automatische UM-Wählplan für Benutzer mit ähnlichen Namen

In diesem Beispiel wird die mit Benutzern mit ähnlichen Namen aufgefordert für des Benutzers alias auf einem UM-Wähleinstellungen, die mit dem Namen einzufügenden Informationen `MyDialPlan`.

```
Set-UMDialplan -Identity MyDialPlan -MatchedNameSelectionMethod PromptForAlias
```

In diesem Beispiel wird die Informationen für Benutzer mit ähnlichen Namen Abteilung auf einem um-Wählplan mit dem Namen einzufügenden `MyDialPlan`.

```
Set-UMDialplan -Identity MyDialPlan -MatchedNameSelectionMethod Department
```

In diesem Beispiel wird die Informationen für Benutzer mit ähnlichen Namen zum Verzeichnis auf einem um-Wählplan mit dem Namen einzufügenden `MyDialPlan`.

```
Set-UMDialplan -Identity MyDialPlan -MatchedNameSelectionMethod Location
```

# Löschen von einem um-Wählplan

18.12.2018 • 2 minutes to read

Sie können einen vorhandenen Unified Messaging-Wählplan (UM) löschen. Wenn Sie den UM-Wählplan löschen, steht er nicht mehr für UM-IP-Gateways, UM-Postfachrichtlinien und UM-Sammelanschlüsse zur Verfügung. Sie können einen UM-Wählplan nicht löschen, wenn er von UM-Postfachrichtlinien, automatischen UM-Telefonzentralen, UM-IP-Gateways oder UM-Sammelanschlüssen verwendet wird bzw. damit verknüpft ist.

Weitere Verwaltungsaufgaben im Zusammenhang mit um-Wählpläne finden Sie unter [Planen von Verfahren UM einwählen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Löschen vorhandener Wählpässe mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie die zu löschenende UM-Wählplan aus, und klicken Sie dann auf **Löschen**  

3. Klicken Sie auf der Seite mit der Warnung auf **Ja**.

## Verwenden Sie zum Löschen einer vorhandenen Wählpas Exchange Online PowerShell

Dieses Beispiel löscht einen UM-Wählplan mit dem Namen `MyUMDialPlan`.

```
RemoveUMDialplan -identity MyUMDialPlan
```

# UM-IP-Gateways

18.12.2018 • 14 minutes to read

Ein Unified Messaging-IP-Gateway (UM) repräsentiert ein physisches VoIP-Gateway (Voice over IP), eine IP-Nebenstellenanlage oder SBC-Hardwaregerät (Session Border Controller). Ehe ein VoIP-Gateway, eine IP-Nebenstellenanlage oder ein SBC zum Annehmen eingehender Anrufe und zum Senden ausgehender Anrufe für Voicemailbenutzer genutzt werden kann, muss im Verzeichnisdienst ein UM-IP-Gateway erstellt werden.

## Übersicht über UM-IP-Gateways

Ursprünglich bezeichnete Gateway ein physisches Gerät, über das zwei inkompatible Netzwerke verbunden werden. Bei Exchange Unified Messaging und in anderen Unified Messaging-Lösungen wird das VoIP-Gateway verwendet, um zwischen dem öffentlichen Telefonnetz/Time Division Multiplex (TDM) oder dem leitungsvermittelten Telefonnetz und einem IP- oder paketvermittelten Datennetzwerk zu übersetzen. Eine IP-Nebenstellenanlage übersetzt auch zwischen dem öffentlichen Telefonnetz und einem paketvermittelten Netzwerk. Bei Verwenden einer IP-Nebenstellenanlage ist deshalb kein VoIP-Gateway erforderlich. Ein VoIP-Gateway ist nur erforderlich, wenn Sie ein älteres Nebenstellenanlagengerät mit Ihrer UM-Bereitstellung verbinden.

### NOTE

Ein paketvermitteltes Netzwerk ist ein Netzwerk, in dem Pakete (Nachrichten oder Fragmente von Nachrichten) einzeln zwischen Geräten wie Routern, Switches, VoIP-Gateways, IP-Nebenstellenanlagen und SBCs geroutet werden. Dagegen richtet ein leitungsvermitteltes Netzwerk eine dedizierte Verbindung zwischen zwei Knoten zur ausschließlichen Verwendung für die Dauer der Kommunikation ein.

Exchange Unified Messaging basiert auf der Fähigkeit des VoIP-Gateways, TDM-Protokolle oder Protokolle für leitungsvermittelte Telefonie, wie z. B. ISDN (Integrated Services Digital Network) oder QSIG, aus einer Nebenstellenanlage in auf VoIP oder IP basierende Protokolle, wie z. B. SIP (Session Initiation Protocol), RTP (Realtime Transport Protocol) oder T.38 für die Faxübermittlung, in Echtzeit zu übersetzen.

IP-Nebenstellenanlagen werden auch genutzt, um ein leitungsvermitteltes Telefonnetz mit einem daten- oder paketvermittelten Netzwerk zu verbinden. Sie dienen auch zum Übersetzen leitungsvermittelter Protokolle in Protokolle, die auf VoIP oder IP basieren, z. B. SIP, RTP und SRTP (Secure RTP).

SBCs (Session Border Controllers) unterscheiden sich leicht von VoIP-Gateways und IP-Nebenstellenanlagen. Anstatt ein leitungsvermitteltes Netzwerk mit einem paketvermittelten Netzwerk zu verbinden, dienen sie zum Verbinden zweier Datennetzwerke über ein öffentliches Netzwerk wie das Internet oder über eine private WAN-Verbindung. Beim Unified Messaging (UM) werden SBCs in einer Hybridbereitstellung von UM eingesetzt, bei der UM einige Komponenten verwendet, die lokal vorhanden sind, und andere nutzt, z. B. Postfächer, die sich in der Cloud befinden.

### VoIP-Gerätekonfigurationen

Zwar gibt es viele verschiedene Typen und Hersteller von Nebenstellenanlagen, VoIP-Gateways, IP-Nebenstellenanlagen und SBCs, doch gibt es im Wesentlichen drei Typen von VoIP-Gerätekonfigurationen:

- **IP-Nebenstellenanlage:** ein einzelnes Gerät, die zwischen dem öffentlichen FESTNETZ/TDM oder leitungsvermittelten basierend Netzwerk und ein IP- oder paketvermittelten Datennetzwerk übersetzt
- **Nebenstellenanlage (älteres Modell) und VoIP-Gateway:** zwei getrennte Komponenten, die gemeinsam zwischen dem öffentlichen FESTNETZ/TDM oder leitungsvermittelten Netzwerk und ein IP-

oder paketvermittelten Datennetzwerk übersetzen

- **SBC:** einzelne oder mehrere Geräte, die zwei Arten von IP-Netzwerken wie ein LAN und ein Datencenter zu verbinden.

Zur Unterstützung von Unified Messaging werden ein oder beide Typen von IP/VoIP-Gerätekonfigurationen verwendet, wenn eine Telefonnetzinfrastruktur mit einer Datennetzwerkinfrastruktur oder eine lokale Bereitstellung mit einer UM-Bereitstellung in der Cloud verbunden werden.

## UM-IP-Gateways

Das UM-IP-Gateway enthält einen oder mehrere UM-Sammelanschlüsse und Konfigurationseinstellungen. UM-Sammelanschlüsse dienen zum Verbinden eines UM-IP-Gateways mit einem UM-Wählplan. Durch die Kombination des UM-IP-Gateways mit einem UM-Sammelanschluss wird eine Verknüpfung zwischen einem VoIP-Gateway, einer IP-Nebenstellenanlage bzw. einem SBC und einem UM-Wählplan eingerichtet. Durch Erstellen mehrerer UM-Sammelanschlüsse kann ein einzelnes UM-IP-Gateway mehreren UM-Wähleinstellungen zugeordnet werden.

Nach dem Erstellen eines UM-IP-Gateways senden die mit dem UM-IP-Gateway verbundenen Exchange-Server eine SIP-Anforderung vom Typ OPTIONS an das VoIP-Gateway, die IP-Nebenstellenanlage oder den SBC, um zu prüfen, ob das Gerät antwortet. Wenn das VoIP-Gateway, die IP-Nebenstellenanlage oder der SBC nicht auf die Anforderung antwortet, protokolliert ein Exchange-Server ein Ereignis mit der ID 1400, das besagt, dass die Anforderung keinen Erfolg hatte. Sollte dies geschehen, stellen Sie sicher, dass das VoIP-Gateway, die IP-Nebenstellenanlage oder der SBC verfügbar und online ist und dass eine ordnungsgemäße Unified Messaging-Konfiguration vorliegt.

Ein Postfachserver kommuniziert nur mit VoIP-Gateways, IP-Nebenstellenanlagen und SBCs, die als vertrauenswürdige SIP-Peers aufgeführt sind. Wenn in einigen Fällen zwei VoIP-Gateways, IP-Nebenstellenanlagen oder SBCs für die Verwendung derselben IP-Adresse konfiguriert sind, wird ein Ereignis mit der ID 1175 protokolliert. Unified Messaging schützt vor nicht autorisierten Anforderungen, indem die interne URL des virtuellen Unified Messaging-Webdiensteverzeichnisses abgerufen wird, auf dem der Clientzugriffsserver installiert ist. Anschließend wird mithilfe dieser URL die Liste der FQDNs für die vertrauenswürdigen SIP-Peers erstellt. Wenn zwei FQDNs in dieselbe IP-Adresse aufgelöst werden, wird dieses Ereignis protokolliert.

## IPv6-Unterstützung für UM-IP-Gateways

Internetprotokoll, Version 6, (IPv6) ist die aktuelle Version des Internetprotokolls (IP). Mit IPv6 sollen zahlreiche der Defizite von IPv4, der vorherigen IP-Version, korrigiert werden. In lokalen und Hybridbereitstellungen von Microsoft Exchange Server 2010 wird IPv6 vollständig unterstützt, allerdings nur, wenn auch IPv4 verwendet wird.

In Exchange Server lokal und hybridbereitstellungen, UM-bezogene Komponenten und Sprachdienste nur auf Clientzugriffs- und Postfachservern ausgeführt. Da die UM-Architektur geändert wurde und erfordert nun Unified Communications Managed API (UCMA) 4.0 zur Unterstützung von sowohl IPv4 und IPv6-als auch anderen Exchange-Features, die Clientzugriffs- und Postfachservern, die Unified Messaging-Komponenten und Dienste vollständig aufweisen Unterstützung von IPv6-Netzwerke und IPv4 ist nicht erforderlich.

In lokalen Hybrid und Exchange Online-Bereitstellungen können Unternehmen und Exchange Online UM Administratoren IPv6 verwenden, beim Verbinden UM mit IPv6-fähigen Geräte, einschließlich Geräte wie Router, IP-Gateways, IP-PBX-Anlagen und Microsoft Office Communications Server 2007 R2 und Microsoft Lync Server. Jedoch für Interoperabilität und Abwärtskompatibilität IPv4 verwendet werden können stattdessen ohne zusätzliche Konfiguration geändert wird, wenn der Parameter *IPAddressFamily*, um festgelegt ist `Any` auf UM-IP-Gateways.

Exchange UM muss weiter direkt mit SIP-Peers (VoIP-Gateways, IP-Nebenstellenanlagen und SBCs) kommunizieren, die IPv6 in ihrer Software oder Firmware möglicherweise nicht unterstützen. Wenn diese IPv6 nicht unterstützen, muss UM direkt mit SIP-Peers kommunizieren können, die IPv4 verwenden. Wird Voicemail gehostet, kommuniziert UM mit Telefonieanlagen über SBCs, Lync Server 2010 oder Lync Server 2013. In gehosteten Umgebungen können IPv6-SIP-fähige Clients wie SBCs und Server mit Lync bereitgestellt werden, um die Umwandlung von IPv6 in IPv4 durchzuführen.

Für lokale und Hybridbereitstellungen müssen Sie nach der Installation der Clientzugriffs- und Postfachserver sowie für Exchange Online UM-Bereitstellungen UM-IP-Gateways erstellen. Wenn Ihre UM-IP-Gateways IPv6 unterstützen müssen, führen Sie außerdem die folgenden Schritte aus:

1. Erstellen Sie ein neues UM-IP-Gateway, oder konfigurieren Sie ein vorhandenes UM-IP-Gateway mit einer IPv6-Adresse für jedes IP-Gateway, jede IP-Nebenstellenanlage oder jeden SBC in Ihrem Netzwerk. Wenn Sie die erforderlichen UM-IP-Gateways erstellen und konfigurieren, müssen Sie die IPv6-Adresse oder den FQDN (Fully Qualified Domain Name) für das UM-IP-Gateway hinzufügen. Wenn Sie dem UM-IP-Gateway den FQDN hinzufügen, müssen Sie zuvor die richtigen DNS-Einträge erstellt haben, um den FQDN des UM-IP-Gateways in die IPv6-Adresse aufzulösen. Für ein vorhandenes UM-IP-Gateway können Sie das Cmdlet **Set-UMIPgateway** verwenden, um die IPv6-Adresse oder den FQDN zu konfigurieren.
2. Konfigurieren Sie den Parameter *IPAddressFamily* auf jedes UM-IP-Gateway. Um die VoIP-Gateway zum Akzeptieren von IPv6-Paketen zu aktivieren, müssen Sie das UM-IP-Gateway entweder IPv4 und IPv6-Verbindungen akzeptiert, oder übernehmen Sie nur IPv6-Verbindungen mit dem Cmdlet **Set-UMIPgateway** festlegen.
3. Nach der Konfiguration Ihrer UM-IP-Gateways müssen Sie auch die VoIP-Gateways, IP-Nebenstellenanlagen und SBCs in Ihrem Netzwerk für die Unterstützung von IPv6 konfigurieren. Erkundigen Sie sich bei Ihrem Hardwareanbieter nach einer Liste der Geräte, die IPv6 unterstützen, und nach Informationen zu einer ordnungsgemäßen Konfiguration dieser Geräte.

#### NOTE

Die maximale Anzahl von UM-IP-Gateways pro Wählplan beträgt 200. Wenn Sie mehr als 200 erstellen, wird der UM-Dienst nicht gestartet.

## Aktivieren und Deaktivieren von UM-IP-Gateways

Standardmäßig wird ein UM-IP-Gateway nach seiner Erstellung im aktivierte Zustand belassen. Das UM-IP-Gateway kann jedoch aktiviert oder deaktiviert werden. Wenn Sie ein UM-IP-Gateway deaktivieren, können Sie es so einrichten, dass alle Exchange-Server gezwungen werden, bestehende Anrufe abzubrechen. Alternativ können Sie es so einrichten, dass dem UM-IP-Gateway zugeordnete Exchange-Server gezwungen werden, neue vom VoIP-Gateway, von der IP-Nebenstellenanlage oder vom SBC eingehende Anrufe anzunehmen.

Wenn Sie Unified Messaging in Office Communications Server R2 oder Microsoft Lync Server integrieren möchten, müssen Sie zulassen nur ein UM-IP-Gateway zum Tätigen von ausgehenden Anrufen für Benutzer, und deaktivieren Sie ausgehende Anrufe auf allen anderen Ihre SIP-URI-Wählplan zugeordnet UM-IP-gateways Pläne. Verwenden Sie Exchange Online PowerShell oder der Exchange-Verwaltungskonsole, um ausgehende Anrufe deaktivieren.

Entscheiden Sie sich bei der Auswahl des UM-IP-Gateways, für das ausgehende Anrufe für lokale und Hybridbereitstellungen zugelassen werden, für dasjenige, das voraussichtlich den meisten Datenverkehr verarbeiten muss. Verhindern Sie, dass ausgehender Datenverkehr über ein IP-Gateway geleitet wird, das über eine Verbindung zu einem Pool mit Lync Server-Directors verfügt. Dies ist erforderlich, um sicherzustellen, dass ausgehende Anrufe externer Benutzer durch einen Postfachserver, auf dem der Microsoft Exchange Unified

Messaging-Dienst ausgeführt wird (z. B. in "Wiedergabe über Telefon"-Szenarien) zuverlässig durch die Firewall des Unternehmens geleitet werden.

# UM-IP-Gateway - Verfahren

18.12.2018 • 2 minutes to read

[Erstellen eines UM-IP-Gateways](#)

[Verwalten eines UM-IP-Gateways](#)

[Aktivieren eines UM-IP-Gateways](#)

[Deaktivieren eines UM-IP-Gateways](#)

[Konfigurieren eines vollqualifizierten Domänenamens](#)

[Konfigurieren der IP-Adresse](#)

[Konfigurieren Sie den Überwachungsport](#)

[Löschen eines UM-IP-Gateways](#)

# Erstellen eines UM-IP-Gateways

18.12.2018 • 7 minutes to read

Wenn Sie ein Unified Messaging-IP-Gateway erstellen, ermöglichen Sie Exchange-Servern das Herstellen einer Verbindung mit einem neuen VoIP-Gateway (Voice over IP), einer SIP-fähigen (Session Initiation Protocol) Nebenstellenanlage, einer IP-Nebenstellenanlage oder einem SBC (Session Border Controller). Unmittelbar nach dem Erstellen eines UM-IP-Gateways sollten Sie einen UM-Sammelanschluss erstellen und den UM-Sammelanschluss dann dem UM-IP-Gateway zuordnen. Das UM-IP-Gateway kann mehreren UM-Wähleinstellungen zugeordnet werden, indem ein oder mehrere UM-Sammelanschlüsse erstellt werden.

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen eines UM-IP-Gateways mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-IP-Gateways**, und klicken Sie dann auf **New**
2. Geben Sie auf der Seite **Neues UM-IP-Gateway** die folgenden Informationen ein:
  - **Name:** in diesem Feld können Sie einen eindeutigen Namen für das UM-IP-Gateway angeben. Dies ist ein Anzeigename, der in der Exchange-Verwaltungskonsole angezeigt wird. Wenn Sie den Anzeigenamen des UM-IP-Gateways zu ändern haben, nachdem es erstellt wurde, müssen Sie zuerst Löschen der vorhandenen UM-IP-Gateways, und erstellen Sie ein anderes UM-IP-Gateway mit dem Namen, den Sie möchten. Der Name der UM-IP-Gateway ist erforderlich, aber es wird nur für die Anzeige verwendet. Da Ihre Organisation mehrere UM-IP-Gateways verwenden kann, wird empfohlen, aussagekräftige Namen für die UM-IP-Gateways zu verwenden. Die maximale Länge eines UM-IP-Gatewaynamens beträgt 64 Zeichen, und er kann Leerzeichen enthalten. Es kann keine jedoch enthalten die folgenden Zeichen: "/\[];|=, + \* ? < >.
  - **Adresse:** Sie können ein UM-IP-Gateway mit einer IP-Adresse oder einen vollqualifizierten

Domänennamen (FQDN) konfigurieren. Verwenden Sie dieses Feld, um die IP-Adresse auf die VoIP-Gateway, SIP-aktivierte PBX, IP-Nebenstellenanlage oder SBC oder einen vollqualifizierten Domänennamen konfiguriert anzugeben. In diesem Feld akzeptiert nur FQDNs, die gültige und formatierte richtig sind.

Sie können alphabetische und numerische Zeichen in dieses Feld eingeben. IPv4-Adressen, IPv6-Adressen und FQDNs werden unterstützt. Wenn Sie gegenseitige verwenden möchten Transport Layer Security (MTLS) zwischen einem UM-IP-Gateway und einem Wählplan Betrieb in einem SIP-gesicherte oder gesicherte Modus, müssen Sie das UM-IP-Gateway mit dem FQDN konfigurieren. Sie müssen auch konfigurieren, um zu Lauschen Port 5061, und stellen Sie sicher, dass alle VoIP-Gateways oder IP-PBX-Anlagen auch Port 5061 mutual TLS-Anforderungen abzuhören konfiguriert wurde. Um ein UM-IP-Gateway zu konfigurieren, führen Sie den folgenden Befehl:

```
et-UMIPGateway -identity MyUMIPGateway -Port 5061 .
```

Wenn Sie einen FQDN verwenden, müssen Sie außerdem sicherstellen, dass Sie für das VoIP-Gateway einen gültigen DNS-Hosteintrag konfiguriert haben, sodass der Hostname fehlerfrei in eine IP-Adresse aufgelöst werden kann. Auch wenn Sie anstelle einer IP-Adresse einen vollqualifizierten Domänennamen (FQDN) verwenden und die DNS-Konfiguration für das UM-IP-Gateway ändern, müssen Sie das UM-IP-Gateway deaktivieren und erneut aktivieren, um sicherzustellen, dass die Konfigurationsinformationen für das UM-IP-Gateway ordnungsgemäß aktualisiert werden.

- **UM-Wähleinstellungen:** Klicken Sie auf **Durchsuchen**, wählen Sie den UM-Wählplan, die Sie mit dem UM-IP-Gateway zuordnen möchten. Bei der Auswahl von eines um-Wählplans ein UM-IP-Gateway zugeordnet wird ein Standard-UM-Sammelanschluss auch erstellt und zugeordnete UM-Wählplan, den Sie ausgewählt haben. Wenn Sie einen um-Wählplan nicht aktivieren, müssen Sie manuell erstellen ein um-Sammelanschlusses und ordnen Sie anschließend, UM-Sammelanschluss mit dem UM-IP-Gateway, das Sie erstellen.

3. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell, Erstellen eines UM-IP-Gateways

Dieses Beispiel erstellt ein UM-IP-Gateway mit dem Namen `yUMIPGateway` ermöglicht, die Exchange-Server die Annahme von Anrufen von einem VoIP-Gateway, einer Nebenstellenanlage aktiviert für SIP, eine IP-Nebenstellenanlage oder ein SBC, der eine IP-Adresse 10.10.10.1 hat, starten.

```
New-UMIPGateway -Name MyUMIPGateway -Address 10.10.10.1
```

Dieses Beispiel erstellt ein UM-IP-Gateway mit dem Namen `MyUMIPGateway` ermöglicht, die Exchange-Server zum Starten der Annahme von Anrufen von einem VoIP-Gateway, einer Nebenstellenanlage aktiviert für SIP, eine IP-Nebenstellenanlage oder ein SBC, der ein FQDN MyUMIPGateway.contoso.com und hört Port 5061.

```
New-UMIPGateway -Name MyUMIPGateway -Address "MyUMIPGateway.contoso.com" -Port 5061
```

Dieses Beispiel erstellt ein UM-IP-Gateway mit dem Namen `yUMIPGateway` und verhindert, dass das UM-IP-Gateway eingehende Anrufe oder sendenden ausgehende Anrufe abgesetzt wird eine IPv6-Adresse und ermöglicht das UM-IP-Gateway IPv4 und IPV6-Adressen verwendet werden.

```
New-UMIPGateway -Identity MyUMIPGateway -Address fe80::39bd:88f7:6969:d223%11 -IPAddressFamily Any -Status Disabled -OutcallsAllowed $false
```

# Verwalten eines UM-IP-Gateways

18.12.2018 • 9 minutes to read

Nachdem Sie ein UM-IP-Gateway erstellt haben, können Sie verschiedene Einstellungen anzeigen bzw. konfigurieren. Sie können beispielsweise die IP-Adresse oder einen vollqualifizierten Domäennamen (Fully Qualified Domain Name, FQDN) sowie Einstellungen für ausgehende Anrufe konfigurieren und die MWI-Funktion (Message Waiting Indicator) aktivieren bzw. deaktivieren.

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Anzeigen oder Konfigurieren der Eigenschaften von UM-IP-Gateways mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-IP-Gateways**. In der Listenansicht, wählen Sie den UM-IP-Gateway, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten**.
2. Verwenden Sie die Seite **UM-IP-Gateway**, um die Einstellungen für das UM-IP-Gateway anzuzeigen und zu konfigurieren. Sie können außerdem die folgenden Einstellungen anzeigen oder konfigurieren:
  - **Status:** dieses reine Anzeigefeld zeigt den Status des UM-IP-Gateways.
  - **Name:** in diesem Feld können Sie einen eindeutigen Namen für das UM-IP-Gateway angeben. Dies ist ein Anzeigename, der in der Exchange-Verwaltungskonsole angezeigt wird. Wenn Sie den Anzeigennamen des UM-IP-Gateways zu ändern haben, nachdem es erstellt wurde, müssen Sie zuerst Löschen der vorhandenen UM-IP-Gateways, und erstellen Sie ein anderes UM-IP-Gateway mit dem entsprechenden Namen. Der Name der UM-IP-Gateway ist erforderlich, aber es wird nur für die Anzeige verwendet. Da Ihre Organisation mehrere UM-IP-Gateways verwenden kann, wird empfohlen, aussagekräftige Namen für

die UM-IP-Gateways zu verwenden. Die maximale Länge eines UM-IP-Gatewaynamens beträgt 64 Zeichen, und er kann Leerzeichen enthalten.

- **Adresse:** Sie können ein UM-IP-Gateway mit einer IP-Adresse oder einen vollqualifizierten Domänennamen (FQDN) konfigurieren. Verwenden Sie dieses Feld, um die IP-Adresse oder auf die VoIP-Gateway, SIP-aktivierte PBX, IP-Nebenstellenanlage oder SBC konfigurierten FQDN anzugeben.

Sie können in diesem Feld Buchstaben und Zahlen eingeben. Es werden IPv4-Adressen, IPv6-Adressen und FQDNs unterstützt. Wenn Sie einen FQDN verwenden, müssen Sie außerdem sicherstellen, dass Sie für das VoIP-Gateway einen gültigen DNS-Hosteintrag konfiguriert haben, sodass der Hostname fehlerfrei in eine IP-Adresse aufgelöst werden kann. Auch wenn Sie anstelle einer IP-Adresse einen vollqualifizierten Domänennamen (FQDN) verwenden und die DNS-Konfiguration für das UM-IP-Gateway ändern, müssen Sie das UM-IP-Gateway deaktivieren und erneut aktivieren, um sicherzustellen, dass die Konfigurationsinformationen für das UM-IP-Gateway ordnungsgemäß aktualisiert werden.

Wenn Sie gegenseitige verwenden möchten Transport Layer Security (MTLS) zwischen einem UM-IP-Gateway und einem Wählplan Betrieb in einem SIP-gesicherte oder gesicherte Modus, müssen Sie das UM-IP-Gateway mit dem FQDN konfigurieren. Sie müssen auch konfigurieren, um Lauschen Port 5061, und stellen Sie sicher, dass die IP-Gateways oder IP-PBX-Anlagen auch Port 5061 mutual TLS-Anforderungen abzu hören konfiguriert wurde. Um ein UM-IP-Gateway zu konfigurieren, führen Sie den folgenden Befehl: `Set-UMIPGateway -identity MyUMIPGateway -Port 5061`.

- **Ausgehende Anrufe über dieses UM-IP-Gateway zulassen:** Aktivieren Sie dieses Kontrollkästchen, um das UM-IP-Gateway annimmt und verarbeitet ausgehende Anrufe zu ermöglichen. Diese Einstellung wirkt sich nicht Call gehandelt oder von einem VoIP-Gateway eingehende Anrufe aus.

Beim Erstellen des UM-IP-Gateways ist diese Einstellung standardmäßig aktiviert. Wenn Sie diese Einstellung deaktivieren, können Anrufer, die dem Wählplan zugeordnet sind, keine ausgehenden Anrufe über das im Feld **Adresse** angegebene VoIP-Gateway, die definierte IP-Nebenstellenanlage oder den SBC tätigen.

- **Zulassen Nachricht wartet Indikator:** Aktivieren Sie dieses Kontrollkästchen, um e-Mail-Benachrichtigungen für das UM-IP-Gateway getroffenen Anrufe an Benutzer gesendet werden VoIP zu ermöglichen. Diese Einstellung ermöglicht das UM-IP-Gateway zum Benachrichtigen SIP-Nachrichten für Benutzer senden und empfangen. Diese Einstellung ist standardmäßig aktiviert und kann Nachricht wartenden Benachrichtigungen an Benutzer gesendet werden.

MWI (Message Waiting Indicator) kann sich auf jeden Mechanismus beziehen, der das Vorhandensein einer neuen oder noch nicht abgehörten Nachricht signalisiert. Der Hinweis auf den Eingang einer neuen Sprachnachricht befindet sich bei Clients wie Outlook und Outlook Web App im Posteingang. Er kann in Form einer SMS (Short Messaging Service) oder Textnachricht an ein registriertes Mobiltelefon, als ausgehender Anruf von einem Exchange-Server an eine vorkonfigurierte Telefonnummer oder als Signalleuchte am Telefon eines Benutzers erfolgen.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie UM-IP-Gateway-Eigenschaften

In diesem Beispiel wird die IP-Adresse eines UM-IP-Gateways mit dem Namen `MyUMIPGateway`.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address 10.10.10.1
```

In diesem Beispiel wird verhindert, dass das UM-IP-Gateway mit dem Namen `MyUMIPGateway` akzeptiert, eingehende Anrufe und verhindert, dass ausgehende Anrufe.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address voipgateway.contoso.com -Status 2 -OutcallsAllowed $false
```

In diesem Beispiel wird es dem UM-IP-Gateway ermöglicht, als VoIP-Gatewaysimulator zu fungieren. Das Beispiel kann mit dem Cmdlet **Test-UMConnectivity** verwendet werden.

```
Set-UMIPGateway -Identity MyUMIPGateway -Simulator $true
```

#### IMPORTANT

Es tritt eine gewisse Latenz auf, bevor alle Änderungen, die Sie an der Konfiguration eines UM-IP-Gateways vorgenommen haben, auf alle Exchange-Server repliziert wurden, die sich in demselben UM-Wählplan wie das UM-IP-Gateway befinden.

In diesem Beispiel wird verhindert, dass das UM-IP-Gateway mit dem Namen `MyUMIPGateway` akzeptiert, eingehende Anrufe und verhindert, dass ausgehende Anrufe, legt eine IPv6-Adresse und ermöglicht das UM-IP-Gateway verwenden IPv4 und IPv6-Adressen.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address fe80::39bd:88f7:6969:d223%11 -IPAddressFamily Any -Status Disabled -OutcallsAllowed $false
```

## Verwenden von Exchange Online PowerShell, UM-IP-Gateway-Eigenschaften anzeigen

In diesem Beispiel wird eine formatierte Liste aller UM-IP-Gateways in der Active Directory-Gesamtstruktur angezeigt.

```
Get-UMIPGateway |Format-List
```

Dieses Beispiel zeigt die Eigenschaften für ein UM-IP-Gateway mit dem Namen `MyUMIPGateway`.

```
Get-UMIPGateway -Identity MyUMIPGateway
```

In diesem Beispiel werden alle UM-IP-Gateways einschließlich der VoIP-Gatewaysimulatoren in der Active Directory-Gesamtstruktur angezeigt.

```
Get-UMIPGateway -IncludeSimulator $true
```

# Aktivieren eines UM-IP-Gateways

18.12.2018 • 2 minutes to read

Beim Erstellen eines UM-IP-Gateways (Unified Messaging) wird dessen Status standardmäßig auf "Aktiviert" festgelegt. Möglicherweise müssen Sie das UM-IP-Gateway jedoch deaktivieren, um es offline zu schalten und zu verhindern, dass es eingehende und ausgehende Anrufe annimmt. Nach dem Erstellen eines UM-IP-Gateways können Sie die Funktionalität über seine Statusvariable aktivieren oder deaktivieren.

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt und deaktiviert wurde. Weitere Informationen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren eines UM-IP-Gateways mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu > **Unified Messaging > UM-IP-Gateways**, wählen Sie das UM-IP-Gateway, das Sie aktivieren möchten, und klicken Sie dann auf den **Pfeil nach oben ↑**.
2. Klicken Sie auf der Seite **Warnung** auf **Ja**.

## Verwenden von Exchange Online PowerShell zum Aktivieren eines UM-IP-Gateways

In diesem Beispiel wird ein UM-IP-Gateway mit dem Namen ermöglicht `MyUMIPGateway`.

```
Enable-UMIPGateway -Identity MyUMIPGateway
```

# Deaktivieren eines UM-IP-Gateways

18.12.2018 • 3 minutes to read

Beim Erstellen eines UM-IP-Gateways (Unified Messaging) wird dessen Status standardmäßig auf "Aktiviert" festgelegt. Nachdem Sie das UM-IP-Gateway erstellt haben, können Sie dessen Betrieb deaktivieren, indem Sie seinen Status auf "Deaktiviert" festlegen. Nachdem Sie das UM-IP-Gateway deaktiviert haben, können das VoIP-Gateway (Voice over IP), die IP-Nebenstellenanlage (Private Branch eXchange, PBX) bzw. der Session Border Controller (SBC) eingehende Unified Messaging-Anrufe nicht länger verarbeiten.

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt und aktiviert wurde. Weitere Informationen finden Sie unter [Erstellen eines UM-IP-Gateways](#) und [Aktivieren eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Deaktivieren eines UM-IP-Gateways mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-IP-Gateways**, wählen Sie den UM-IP-Gateway, den Sie deaktivieren möchten, und klicken Sie dann auf den **Pfeil nach unten** ▾.
2. Klicken Sie auf der Seite **Warnung** auf **Ja**.

Verwenden Sie Exchange Online PowerShell, um ein UM-IP-Gateway zu deaktivieren.

In diesem Beispiel wird ein UM-IP-Gateway mit dem Namen `yUMIPGateway` und verhindert, dass Sie eingehende Anrufe von einer VoIP-Gateways, IP-Nebenstellenanlage oder SBC akzeptieren.

```
Disable-UMIPGateway -Identity MyUMIPGateway
```

In diesem Beispiel wird ein UM-IP-Gateway mit dem Namen `yUMIPGateway` und sofort alle aktuellen Anrufe getrennt.

```
Disable-UMIPGateway -Identity MyUMIPGateway -Immediate $true
```

# Konfigurieren eines vollqualifizierten Domänenamens

18.12.2018 • 4 minutes to read

Sie können ein Unified Messaging-IP-Gateway entweder mit einer IP-Adresse oder mit einem vollqualifizierten Domänenamen (Fully Qualified Domain Name, FQDN) konfigurieren. Wenn Sie ein UM-IP-Gateway erstellen, müssen Sie die IP-Adresse oder den FQDN definieren, die bzw. der für das verwendete VoIP-Gateway, die verwendete IP-Nebenstellenanlage oder den verwendeten Session Border Controller (SBC) konfiguriert ist. Sie können die IP-Adresse oder den FQDN nach dem Erstellen des UM-IP-Gateways ändern.

Wenn Sie ein UM-IP-Gateway mit einem FQDN erstellen, müssen Sie in Ihrer DNS-Forward-Lookupzone die geeigneten HOST (A)-Einträge erstellen. Wenn Sie ein UM-IP-Gateway mit einem FQDN erstellen und die DNS-Konfiguration für das UM-IP-Gateway geändert wird, müssen Sie das UM-IP-Gateway deaktivieren und dann wieder aktivieren, damit sichergestellt ist, dass die Konfigurationsinformationen ordnungsgemäß aktualisiert werden.

Wenn Sie gegenseitige verwenden möchten Transport Layer Security (MTLS) zwischen einem UM-IP-Gateway und einem Wählplan Betrieb in einem SIP-gesicherte oder gesicherte Modus, müssen Sie das UM-IP-Gateway mit dem FQDN konfigurieren. Sie müssen auch konfigurieren, dass er Lauschen Port 5061, und überprüfen Sie, ob die VoIP-Gateways, IP-Nebenstellenanlage oder SBC auch anhören für mutual TLS-Anfragen an Port 5061 konfiguriert wurde. Um ein UM-IP-Gateway zu konfigurieren, führen Sie den folgenden Befehl:

```
Set-UMIPGateway -Identity MyUMIPGateway -Port 5061 .
```

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren eines FQDN mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-IP-Gateways**, wählen

Sie den UM-IP-Gateway, das Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

2. Geben Sie auf der Seite **UM-IP-Gateway** in **Adresse** den FQDN für das VoIP-Gateway, die für SIP aktivierte Nebenstellenanlage, die IP-Nebenstellenanlage oder den SBC ein.

3. Klicken Sie auf **Speichern**.

**IMPORTANT**

Wenn Sie anstelle einer IP-Adresse einen FQDN für das UM-IP-Gateway verwenden, vergewissern Sie sich, dass die richtigen DNS-Einträge erstellt wurden.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie einen vollqualifizierten Domänennamen

In diesem Beispiel wird ein UM-IP-Gateway mit dem Namen konfiguriert **MyUMIPGateway** mit dem FQDN mit dem Namen voipgateway.contoso.com.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address voipgateway.contoso.com
```

In diesem Beispiel wird ein UM-IP-Gateway mit dem Namen konfiguriert **MysBC** mit dem FQDN sbc.contoso.com und überwacht für SIP-Anforderungen auf TCP-port 5061.

```
Set-UMIPGateway -Identity MySBC -Address sbc.contoso.com -Port 5061
```

# Konfigurieren der IP-Adresse

18.12.2018 • 4 minutes to read

Bevor Sie ein Unified Messaging-IP-Gateway (UM) erstellen, müssen Sie die IP-Adresse oder den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) für das VoIP-Gateway, die IP-Nebenstellenanlage oder den Session Border Controller (SBC) definieren. Beim Erstellen des UM-IP-Gateways geben Sie diese IP-Adresse oder diesen FQDN an. Sie können die IP-Adresse oder den FQDN später ändern.

Sie können die IP-Adresse oder über die Exchange-Verwaltungskonsole oder Exchange Online PowerShell FQDN konfigurieren. In der Exchange-Verwaltungskonsole kann das Feld **Adresse** auf der Seite **UM-IP-Gateway** IPv4-IP-Adresse, eine IPv6-Adresse oder einen vollqualifizierten Domänennamen akzeptieren. Sie können auch die Parameter *Address* im Cmdlet **Set-UMIPGateway** in Exchange Online PowerShell verwenden, um eine IPv4-IP-Adresse, eine IPv6-Adresse oder einen vollqualifizierten Domänennamen festzulegen. Wenn Sie ein UM-IP-Gateway über einen vollqualifizierten Domänennamen erstellen, müssen Sie die entsprechenden HOST-A-Einträge in DNS-forward-Lookupzone erstellen. Wenn die DNS-Konfiguration für den UM-IP-Gateway geändert wird, müssen Sie deaktivieren und aktivieren das UM-IP-Gateway dafür sorgen, dass die Konfigurationsinformationen korrekt aktualisiert wird.

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der IP-Adresse für ein UM-IP-Gateway mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-IP-Gateways**, wählen Sie den UM-IP-Gateway, den Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Geben Sie auf der Seite **UM-IP-Gateway** im Feld **Adresse** die IP-Adresse für das VoIP-Gateway, die IP-

Nebenstellenanlage oder den Session Border Controller (SBC) ein.

3. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

#### IMPORTANT

Wenn Sie anstelle einer IP-Adresse einen FQDN für das UM-IP-Gateway verwenden, vergewissern Sie sich, dass die richtigen DNS-Datensätze erstellt wurden.

## Verwenden Sie Exchange Online PowerShell, um die IP-Adresse auf einem UM-IP-Gateway zu konfigurieren

In diesem Beispiel wird ein UM-IP-Gateway mit dem Namen konfiguriert `MyUMIPGateway` mit der IP-Adresse 10.10.10.1.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address 10.10.10.1
```

In diesem Beispiel wird ein UM-IP-Gateway mit dem Namen konfiguriert `MyUMIPGateway` mit einer IP-Adresse 10.10.10.10 und überwacht für SIP-Adresse anfordert, TCP-Port 5061.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address 10.10.10.10 -Port 5061
```

In diesem Beispiel wird verhindert, dass das UM-IP-Gateway mit dem Namen `MyUMIPGateway` von eingehenden und ausgehenden Anrufe annehmen, wird eine IPv6-Adresse und ermöglicht das UM-IP-Gateway IPv4 und IPV6-Adressen verwendet werden.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address fe80::39bd:88f7:6969:d223%11 -IPAddressFamily Any -Status Disabled -OutcallsAllowed $false
```

# Konfigurieren Sie den Überwachungsport

18.12.2018 • 5 minutes to read

Sie können den TCP-Port konfigurieren, der für die Überwachung auf SIP-Anforderungen (Session Initiation-Protokoll) für ein UM-IP-Gateway (Unified Messaging) verwendet wird. Beim Erstellen eines UM-IP-Gateways wird die Nummer des TCP-Ports für die Überwachung auf SIP-Anforderungen standardmäßig auf 5060 festgelegt. Der TCP-SIP-Überwachungsport kann nicht mithilfe der Exchange-Verwaltungskonsole konfiguriert oder geändert werden. Sie müssen die Nummer des TCP-SIP-Überwachungsports mithilfe des Cmdlets **Set-UMIPGateway** konfigurieren.

Möglicherweise müssen Sie die Nummer des TCP-Überwachungsports auf 5061 festlegen, um folgende Aufgaben ausführen zu können:

- Festlegen der VoIP-Sicherheitseinstellung für einen Satz UM-Wähleinstellungen auf "SIP-gesichert".
- Festlegen der VoIP-Sicherheitseinstellung für einen Satz UM-Wähleinstellungen auf "Gesichert".
- Integration mit Microsoft Office Communications Server 2007 R2 oder Microsoft Lync Server.
- Verwenden Sie MTLS (Mutual Transport Layer Security) zur Verschlüsselung von Netzwerkdaten zwischen Exchange-Servern und einem VoIP-Gateway, einer SIP-fähigen Nebenstellenanlage (Private Branch eXchange, PBX), einer IP-Nebenstellenanlage oder einem SBC (Session Border Controller).

Wenn Sie MTLS zwischen einem UM-IP-Gateway und einen Wählplan Betrieb in SIP-gesicherte oder gesicherte Modus beim Erstellen des UM-IP-Gateways muss mit einem vollqualifizierten Domänenamen (FQDN) konfigurieren, und klicken Sie dann Exchange Online PowerShell so konfigurieren Sie die U verwenden möchten M-IP-Gateway für TCP-Port 5061 abhören. Sie müssen außerdem sicher, dass alle VoIP-Gateways, Nebenstellenanlagen für SIP-IP-PBX-Anlagen, aktiviert und SBCs auch anhören für mutual TLS-Anfragen an Port 5061 konfiguriert wurden.

## IMPORTANT

Wenn Sie ein UM-IP-Gateway mit einem FQDN erstellen, müssen Sie in Ihrer DNS-Forward-Lookupzone die geeigneten HOST (A)-Einträge erstellen. Wenn Sie ein UM-IP-Gateway mit einem FQDN erstellen und die DNS-Konfiguration für das UM-IP-Gateway geändert wird, müssen Sie das UM-IP-Gateway deaktivieren und dann wieder aktivieren, damit sichergestellt ist, dass die Konfigurationsinformationen des UM-IP-Gateways ordnungsgemäß aktualisiert werden.

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).

- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

**TIP**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell so konfigurieren Sie den TCP-Überwachungsport

In diesem Beispiel wird ein UM-IP-Gateway mit dem Namen konfiguriert `MyUMIPGateway`, TCP-Port 5061 SIP-Anforderungen lauscht und FQDN eines mTLS.MyUMIPGateway.contoso.com ist.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address mTLS.MyUMIPGateway.contoso.com -Port 5061
```

In diesem Beispiel wird ein UM-IP-Gateway mit dem Namen konfiguriert `MyUMIPGateway`, die ein FQDN SIPSecured.MyUMIPGateway.contoso.com hat und TCP-Port 5061 SIP-Anforderungen lauscht.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address SIPSecured.MyUMIPGateway.contoso.com -Port 5061
```

In diesem Beispiel wird ein UM-IP-Gateway mit dem Namen konfiguriert `MyUMIPGateway`, die ein FQDN MyOCSUMIPGateway.contoso.com hat und TCP-Port 5061 SIP-Anforderungen lauscht.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address MyOCSUMIPGateway.contoso.com -Port 5061
```

# Löschen eines UM-IP-Gateways

18.12.2018 • 2 minutes to read

Wenn Sie ein UM-IP-Gateway (Unified Messaging) löschen, können Exchange-Server eingehende Anrufe von dem VoIP-Gateway (Voice over IP), der SIP-fähigen Nebenstellenanlage (Session Initiation Protocol), der IP-Nebenstellenanlage oder dem Session Border Controller (SBC), die dem UM-IP-Gateway zugeordnet sind, nicht länger annehmen.

## IMPORTANT

Sie sollten ein UM-IP-Gateway nur löschen, wenn Sie genau wissen, wie sich die Deaktivierung der Kommunikation mit einem VoIP-Gateway, einer IP-Nebenstelle oder einem SBC auswirkt.

Informationen zu weiteren Aufgaben in Bezug auf UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Löschen eines UM-IP-Gateways mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-IP-Gateways**, wählen Sie das UM-IP-Gateway, das Sie löschen möchten, und klicken Sie dann auf **Löschen**
2. Klicken Sie auf der Seite **Warnung** auf **Ja**.

Verwenden Sie Exchange Online PowerShell, um ein UM-IP-Gateway zu löschen.

Dieses Beispiel löscht das UM-IP-Gateway mit dem Namen `MyUMIPGateway`.

```
Remove-UMIPGateway -Identity MyUMIPGateway
```

# UM-Sammelanschlüsse

18.12.2018 • 14 minutes to read

Ein telefonischer Sammelanschluss bietet eine Möglichkeit, Telefonanrufe einer einzelnen Nummer an mehrere Durchwahlen oder Telefonnummern zu verteilen. In Unified Messaging (UM) ist ein UM-Sammelanschluss die logische Abbildung eines telefonischen Sammelanschlusses und dient zum Verbinden eines UM-IP-Gateways mit einem UM-Wählplan.

Möchten Sie wissen, welche anderen Verwaltungsaufgaben es im Zusammenhang mit Unified Messaging-Sammelanschlüssen gibt? Weitere Informationen finden Sie unter [Um-Sammelanschlüsse Gruppieren von Prozeduren](#).

## Was ist ein Sammelanschluss?

Der Begriff Sammelanschluss dient der Bezeichnung einer Gruppe von Durchwahlnummern von Nebenstellenanlagen bzw. IP-Nebenstellenanlagen, die von Benutzern gemeinsam verwendet werden. Sammelanschlüsse werden für das effiziente Verteilen der eingehenden und ausgehenden Anrufe einer bestimmten Unternehmenseinheit verwendet. Das Erstellen und Definieren eines Sammelanschlusses verringert die Wahrscheinlichkeit, dass der Anrufer bei einem eingehenden Anruf ein Besetztzeichen hört, wenn sein Anruf empfangen wird.

Sammelanschlüsse dienen zum Bestimmen offener Leitungen, Durchwahlen oder Kanäle, wenn ein Anruf eingeht. Anrufe werden an die nächste verfügbare Leitung weitergeleitet, wenn die Haupttelefonleitung besetzt ist oder der Anruf nicht entgegengenommen wird. Der Anrufer erhält ein Besetztzeichen oder wird an Voicemail weitergeleitet, wenn keine Durchwahlen in der Gruppe verfügbar sind. Eine Nebenstellenanlage- oder IP-Nebenstellenanlage kann z. B. so konfiguriert sein, dass sie 10 Durchwahlnummern für die Vertriebsabteilung besitzt. Diese 10 Vertriebsdurchwahlnummern würden als ein Sammelanschluss konfiguriert.

Zu den Einstellungen eines einfachen Sammelanschlusses gehören Name, Durchwahlnummer, Liste verfügbarer Mitglieder und Auswahlmethode für den Sammelanschluss. Die Methode zur Auswahl des Sammelanschlusses bestimmt die Reihenfolge, in der eingehende Anrufe an die Mitglieder des Sammelanschlusses weitergeleitet werden.

Es gibt mehrere Algorithmen oder Methoden, gemäß denen eine Nebenstellenanlage bzw. IP-Nebenstellenanlage geöffnete Leitungen, Durchwahlen oder Kanäle bestimmen können. Dabei handelt es sich um folgende Verfahren:

- **Gruppe von Sammelanschlüssen oder alle Erweiterungen Klingeln:** Wenn auf die Durchwahlnummer für Sammelanschlüsse Gruppe ein eingehender Anruf empfangen wird, die Nebenstellenanlage oder der IP-Nebenstellenanlage Läuten alle Durchwahlnummern in der Gruppe.
- **Beginnen Sie mit der kleinste Zahl oder linear Jagd:** Dies ist die Standardeinstellung für die meisten Nebenstellenanlagen und IP-PBX-Anlagen. Mit dieser Methode werden Anrufe an die erste im Leerlauf Zeile in der angegebenen Reihenfolge beginnend mit der ersten Zeile in der Gruppe weitergeleitet. Diese Konfiguration ist in den meisten Fällen auf multiline Telefonen Kleinunternehmen gefunden.
- **Round-Robin oder kreisförmige Jagd:** mit dieser Methode werden Anrufe an die erste im Leerlauf Zeile, beginnend mit der Zeile nach diejenige, die zuletzt ein Anruf verarbeitet weitergeleitet. Wenn Anrufe mithilfe der Methode "Roundrobin"-, verteilt werden, wenn Sie ein Anruf in Zeile 1 übermittelt werden, die das nächste aufrufen, wechselt zu Zeile 2, Zeile 3 usw. neben. Dieser Prozess wird fortgesetzt, auch wenn eine der vorherigen Zeilen frei wird. Wenn das Ende des Sammelanschlusses erreicht ist, wird die Jagd in der ersten Zeile. Zeilen werden übersprungen, nur, wenn sie bei einem vorherigen Aufruf noch beschäftigt sind. Kreisförmige oder Roundrobin-Jagd verbreitet Anruf Unterbrechung gleichmäßig in der gesamten alle

Anrufe, die Möglichkeit für eine größere Unterbrechung im Dienst zu minimieren.

- **Die meisten im Leerlauf oder Uniform-Verteilung damit:** mit dieser Methode wird der Anruf zur ersten verfügbaren Zeile in der Gruppe, die der am längsten untätig war weitergeleitet. Diese Methode verwendet die Zeitdauer, die die Person den Anruf nutzen beschäftigt wurde anstelle von gibt an, ob die Zeile verfügbar ist. Diese Methode wird typischerweise in großen Callcentern, in dem die eingehenden Anrufe werden von Personen beantwortet wird und die Last wird auf die Gruppe von Durchwahlnummern gleichmäßig verteilt.

Sie können einen oder mehrere Sammelanschlüsse konfigurieren. Jeder Sammelanschluss muss mindestens zwei Leitungen aufweisen. Wenn eine Nummer bereits zu einem Sammelanschluss gehört, steht sie für den anderen nicht zur Verfügung.

Es folgen Beispiele einfacher telefonischer Sammelanschlüsse und ihrer Funktionsweise.

### **Beispiel 1**

Die Durchwahl 300 (Pilotnummer) ist so programmiert, dass bei einem eingehenden Anruf erst die Durchwahl 301, dann 302, dann 303, dann 304 angerufen wird.

1. Durchwahl 301 ist besetzt.
2. Durchwahl 302 klingelt und wird nicht beantwortet.
3. Durchwahl 303 beantwortet den Anruf.
4. Durchwahl 304 ist frei und wartet auf einen eingehenden Anruf.

### **Beispiel 2**

Die Durchwahl 1000 (Pilotnummer) ist so programmiert, dass bei einem eingehenden Anruf alle Durchwahlen von 2000 bis 2003 gleichzeitig klingeln:

1. Durchwahl 2000 ist frei.
2. Durchwahl 2001 ist frei.
3. Durchwahl 2002 ist frei.
4. Durchwahl 2003 beantwortet den Anruf.

## **Was ist eine Pilotnummer?**

In einem Telefonienetzwerk kann eine Nebenstellenanlage oder IP-Nebenstellenanlage so konfiguriert werden, dass sie eine mehrere Sammelanschlussgruppen hat. Jeder Sammelanschluss, der für eine Nebenstellenanlage oder IP-Nebenstellenanlage erstellt wird, muss eine zugehörige Pilotnummer aufweisen. Wenn eine Pilotnummer verwendet wird, werden Besetzeichen vermieden und eingehende Anrufe an die Durchwahlen weitergeleitet, die verfügbar sind. Die Nebenstellenanlage oder IP-Nebenstellenanlage verwendet die Pilotnummer, um den Sammelanschluss und die Telefondurchwahlnummer zu ermitteln, an der der eingehende Anruf empfangen wurde, und die Durchwahlen zu bestimmen, die dem Sammelanschluss zugewiesen sind. Ohne eine definierte Pilotnummer kann die Nebenstellenanlage- oder IP-Nebenstellenanlage nicht ermitteln, wo der eingehende Anruf empfangen wurde.

Eine Pilotnummer ist die Adresse, Durchwahl oder Position des Sammelanschlusses in der Nebenstellenanlage oder IP-Nebenstellenanlage. Sie wird im Allgemeinen als leere Durchwahlnummer oder Durchwahlnummer eines aus mehreren Durchwahlnummern bestehenden Sammelanschlusses definiert, die keiner Person bzw. keinem Telefon zugeordnet ist. Angenommen, Sie konfigurieren einen Sammelanschluss in einer Nebenstellenanlage oder IP-Nebenstellenanlage so, dass die Durchwahlnummern 4100, 4101, 4102, 4103, 4104 und 4105 enthalten sind. Die Pilotnummer für den Sammelanschluss wird als Durchwahl 4100 konfiguriert. Wenn ein Anruf für die

Durchwahl 4100 eingeht, sucht die Nebenstellenanlage oder IP-Nebenstellenanlage nach der nächsten verfügbaren Durchwahlnummer, um so zu ermitteln, wohin der Anruf weitergeleitet werden soll. In diesem Beispiel untersucht die Nebenstellenanlage oder IP-Nebenstellenanlage mithilfe eines programmierten Suchalgorithmus die Durchwahlnummern 4101, 4102, 4103, 4104 und 4105.

Wenn eine Pilotnummer verwendet wird, werden Besetztzeichen vermieden und eingehende Anrufe an die Durchwahlnummern weitergeleitet, die verfügbar sind. In Unified Messaging wird die Pilotnummer der Nebenstellenanlage oder IP-Nebenstellenanlage als Ziel verwendet. Wenn keine der Durchwahlnummern des Sammelanschlusses einen eingehenden Anruf beantwortet, wird der Anruf an einem Postfachserver weitergeleitet, auf dem der Microsoft Exchange Unified Messaging-Dienst ausgeführt wird.

## Was ist ein UM-Sammelanschluss?

Unified Messaging-Sammelanschlüsse sind für den Betrieb des Unified Messaging-Systems wichtig. Der UM-Sammelanschluss ist eine logische Darstellung eines vorhandenen Sammelanschlusses einer Nebenstellenanlage oder IP-Nebenstellenanlage. Seit Zweck ist die Verbindung eines UM-IP-Gateways mit einem UM-Wählplan. Mithilfe eines einzelnen UM-Sammelanschlusses können mehrere UM-IP-Gateways mit einem UM-Wählplan verbunden werden. Wenn Sie ein UM-IP-Gateway erstellen und mit einem UM-Wählplan verknüpfen, wird standardmäßig ein UM-Sammelanschluss erstellt. Sie können außerdem weitere Sammelanschlüsse erstellen. Sie müssen mindestens einen UM-Sammelanschluss erstellen.

UM-Sammelanschlüsse werden zum Ermitteln des Sammelanschlusses der Nebenstellenanlage oder IP-Nebenstellenanlage verwendet, von dem der eingehende Anruf empfangen wurde. Eine für einen Sammelanschluss in der Nebenstellenanlage oder IP-Nebenstellenanlage definierte Pilotnummer muss auch innerhalb des UM-Sammelanschlusses definiert werden. Die Pilotnummer wird zum Zuordnen der Informationen verwendet, die für eingehende Anrufe über die SIP-Signalnachrichteninformationen (Session Initiation Protocol) zu der Sprachnachricht bereitgestellt werden. Anhand der Pilotnummer können Exchange-Server den Anruf zusammen mit dem richtigen Wählplan interpretieren, damit der Anruf ordnungsgemäß weitergeleitet werden kann. Wenn kein Sammelanschluss vorhanden ist, können Exchange-Server den Ort des eingehenden Anrufs nicht ermitteln. Wenn Exchange-Server den Ort eingehender Anrufe feststellen, können sie die Anrufheaderinformationen übernehmen, die vom VoIP-Gateway, von der IP-Nebenstellenanlage oder der SIP-fähigen Nebenstellenanlage übermittelt werden. Es ist außerordentlich wichtig, die UM-Sammelanschlüsse ordnungsgemäß zu konfigurieren, weil eingehende Anrufe, die der für den UM-Sammelanschluss definierten Pilotnummer nicht eindeutig entsprechen, nicht beantwortet werden und die Weiterleitung eingehender Anrufe nicht funktioniert.

Wenn Sie in lokalen und Hybridbereitstellungen einen UM-Sammelanschluss erstellen, ermöglichen Sie allen Clientzugriffs- und Postfachservern die Kommunikation mit einem VoIP-Gateway, einer IP-Nebenstellenanlage oder einer SIP-fähigen Nebenstellenanlage - unabhängig davon, ob sie einem UM-Wählplan hinzugefügt wurden. Dies liegt daran, dass alle Clientzugriffs- und Postfachserver eingehende Anrufe für alle Wählpläne beantworten anstatt für einen bestimmten UM-Wählplan (wie der UM-Server in Vorgängerversionen von Exchange). Wenn Sie den UM-Sammelanschluss löschen, kann das dazugehörige UM-IP-Gateway keine von einem VoIP-Gateway, einer IP-Nebenstellenanlage oder SIP-fähigen Nebenstellenanlage eingehenden Anrufe beantworten oder ausgehende Anrufe über das VoIP-Gateway, die IP-Nebenstellenanlage oder SIP-fähige Nebenstellenanlage mithilfe der angegebenen Pilotnummer ausführen.

Wenn Sie in lokalen und Hybridbereitstellungen jedoch UM in Microsoft Office Communications Server 2007 R2 oder Microsoft Lync Server integrieren, müssen Sie alle Clientzugriffs- und Postfachserver allen SIP-URI-Wählplänen hinzufügen, die für die Arbeit mit Communications Server 2007 R2 oder Lync Server erstellt wurden. Dadurch können Anrufweiterleitung und Outdialing ordnungsgemäß funktionieren.

Weitere Informationen zu UM-IP-Gateways finden Sie unter [UM-IP-Gateways](#).

# Um-Sammelanschlüsse Gruppieren von Prozeduren

18.12.2018 • 2 minutes to read

[Erstellen eines UM-Sammelanschlusses](#)

[Anzeigen eines um-Sammelanschlusses](#)

[Dient zum Löschen eines UM-Sammelanschlusses.](#)

# Erstellen eines UM-Sammelanschlusses

18.12.2018 • 5 minutes to read

Ein UM-Sammelanschluss ist eine logische Darstellung eines Nebenstellenanlagen- oder IP-Nebenstellenanlagen-Sammelanschlusses. UM-Sammelanschlüsse fungieren als Verbindung oder Verknüpfung zwischen einem UM-IP-Gateway und einem UM-Wählplan.

## NOTE

Wenn Sie beim Erstellen eines UM-IP-Gateways das UM-IP-Gateway einem bestimmten UM-Wählplan zuordnen, wird auch ein UM-Sammelanschluss erstellt.

## NOTE

Wenn Sie die Einstellungen für den UM-Sammelanschluss ändern möchten, müssen Sie den Sammelanschluss löschen und dann einen neuen Sammelanschluss mit den entsprechenden Einstellungen erstellen.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit UM-Sammelanschlüsse finden Sie unter [Um-Sammelanschlüsse Gruppieren von Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Sammelanschlüsse" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Erstellen eines UM-Sammelanschlusses

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Sammelanschlüsse** auf **neu**

3. Geben Sie auf der Seite **Neuer UM-Sammelanschluss** die folgenden Informationen ein:

- **Name:** in diesem Feld können Sie den Anzeigenamen für den um-Sammelanschluss erstellen. Ein um-Sammelanschlüsse Gruppenname ist erforderlich und muss eindeutig sein, aber es wird nur für die Anzeige in der Exchange-Verwaltungskonsole und Exchange Online PowerShell verwendet. Wenn Sie den Anzeigenamen des Sammelanschlusses ändern haben, nachdem es erstellt wurde, müssen Sie zuerst den vorhandenen Sammelanschluss löschen und erstellen Sie eine andere Sammelanschluss mit dem entsprechenden Namen.

Wenn in Ihrer Organisation mehrere Sammelanschlüsse verwendet werden, empfiehlt sich die Verwendung sprechender Namen für die Sammelanschlüsse. Die maximale Länge eines UM-Sammelanschlussnamens beträgt 64 Zeichen, wobei Leerzeichen enthalten sein dürfen. Die folgenden Zeichen dürfen jedoch nicht enthalten sein: "/\[]:;|=,+\*?<>.

- **UM-IP-Gateway:** in diesem Feld Geben Sie das UM-IP-Gateway verwendet werden können. Klicken Sie auf **Durchsuchen**, um das UM-IP-Gateway auszuwählen, und klicken Sie dann auf **OK**.
- **Pilot-ID:** Verwenden Sie dieses Feld, um eine Zeichenfolge anzugeben, die die pilot-ID auf der PBX- oder IP-Nebenstellenanlage konfiguriert eindeutig identifiziert.

In diesem Feld können eine Durchwahlnummer oder ein SIP-URI (Session Initiation-Protokoll - Uniform Resource Identifier) verwendet werden. Alphanumerische Zeichen sind in diesem Feld zulässig. Für ältere Nebenstellenanlagen wird ein numerischer Wert als Pilot-ID verwendet. Einige IP-Nebenstellenanlagen können jedoch SIP-URIs verwenden.

4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell zum Erstellen eines um-WÄHLPLANS Sammelanschlusses

Dieses Beispiel erstellt einen um-Sammelanschluss mit dem Namen , die pilot-ID 12345 hat.

```
New-UMHuntGroup -Name MyUMHuntGroup -PilotIdentifier 12345 -UMDialplan MyUMDialPlan -UMIPGateway MyUMIPGateway
```

Dieses Beispiel erstellt einen um-Sammelanschluss mit dem Namen , die mehreren pilot-IDs hat.

```
New-UMHuntGroup -Name MyUMHuntGroup -PilotIdentifier 5551234,55555 -UMDialplan MyUMDialPlan -UMIPGateway MyUMIPGateway
```

# Anzeigen eines UM-Sammelanschlusses

18.12.2018 • 3 minutes to read

Wenn Sie die Eigenschaften für einen Sammelanschluss Unified Messaging (UM) anzeigen, können Sie die Eigenschaften einer um-Sammelanschluss oder mit einem einzigen UM-IP-Gateway zugeordnet alle um-Sammelanschlüsse zugeordneten anzeigen. Wird kein Parameter angegeben ist, werden alle um-Sammelanschlüsse zurückgegeben. Der Exchange-Verwaltungskonsole können Sie um-Sammelanschlüsse Gruppeneigenschaften anzeigen. Sie müssen Exchange Online PowerShell verwenden.

Nach dem Erstellen eines UM-Sammelanschlusses können die konfigurierten Einstellungen nicht geändert werden. Wenn Sie eine Konfigurationseinstellung ändern möchten, wie z. B. die Pilot-ID eines UM-Sammelanschlusses, müssen Sie den vorhandenen UM-Sammelanschluss löschen und einen neuen UM-Sammelanschluss mit den gewünschten Einstellungen erstellen.

Informationen zu weiteren Aufgaben in Bezug auf UM-Sammelanschlüsse finden Sie unter [Um-Sammelanschlüsse Gruppieren von Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Sammelanschlüsse" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Sammelanschluss erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Sammelanschlusses](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell zum Anzeigen der Eigenschaften eines um-Sammelanschlusses

In diesem Beispiel werden alle UM-Sammelanschlüsse in der Active Directory-Gesamtstruktur angezeigt.

```
Get-UMHuntGroup
```

In diesem Beispiel werden die Details zu einem UM-Sammelanschluss mit dem Namen `MyUMHuntGroup` in einer formatierten Liste.

```
Get-UMHuntGroup -identity MyUMIPGateway\MyUMHuntGroup | Format-List
```

#### NOTE

Bei Verwendung des Cmdlets **Get-UMHuntGroup** ist es nicht ausreichend, nur den Namen des UM-Sammelanschlusses anzugeben. Sie müssen auch den Namen des UM-IP-Gateways angeben, das dem UM-Sammelanschluss zugeordnet ist.

# Dient zum Löschen eines UM-Sammelanschlusses.

18.12.2018 • 3 minutes to read

Nachdem Sie den Unified Messaging-Sammelanschluss (UM) gelöscht haben, verarbeitet oder beantwortet das zum UM-Sammelanschluss gehörende UM-IP-Gateway keine eingehenden Anrufe mehr. Wenn das Löschen des UM-Sammelanschlusses dazu führt, dass keine konfigurierten Sammelanschlüsse für das UM-IP-Gateway verbleiben, ist das UM-IP-Gateway nicht mehr in der Lage, UM-Anrufe anzunehmen oder zu verarbeiten.

Informationen zu weiteren Aufgaben im Zusammenhang mit UM-Sammelanschlüssen finden Sie unter [Um-Sammelanschlüsse Gruppieren von Prozeduren](#).

#### Caution

Wenn Sie die Einstellungen für den UM-Sammelanschluss ändern möchten, müssen Sie den Sammelanschluss löschen und dann einen neuen Sammelanschluss mit den entsprechenden Einstellungen erstellen.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Sammelanschlüsse" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-Sammelanschluss erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Sammelanschlusses](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Löschen eines UM-Sammelanschlusses mit der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, klicken Sie auf dem um-Wählplan, die Sie ändern möchten, und klicken Sie auf der Symbolleiste auf **Bearbeiten**.
2. Auf der Seite **UM-Wählplan** unter **UM-Sammelanschlüsse**, wählen Sie den Sammelanschluss, die Sie löschen möchten, und klicken Sie auf der Symbolleiste auf **Löschen**.
3. Klicken Sie auf der Seite **Warnung** auf **Ja**.

## Mit Exchange Online PowerShell So löschen Sie eine automatische UM-Sammelanschlusses

Dieses Beispiel löscht einen UM-Sammelanschluss mit dem Namen `MyUMHuntGroup`.

```
Remove-UMHuntGroup -identity MyUMHuntGroup
```

# Automatisches Beantworten und Weiterleiten eingehender Anrufe

18.12.2018 • 19 minutes to read

Microsoft Exchange Unified Messaging (UM) ermöglicht je nach den Anforderungen Ihrer Organisation die Einrichtung einer oder mehrerer automatischer UM-Telefonzentralen. Im Gegensatz zu anderen Unified Messaging-Komponenten, z. B. UM-Wähleinstellungen und UM-IP-Gateways, ist die Einrichtung automatischer UM-Telefonzentralen nicht unbedingt erforderlich. Automatische Telefonzentralen helfen internen und externen Anrufern jedoch beim Auffinden von Benutzern oder Abteilungen in einer Organisation, um Anrufe an diese weiterzuleiten. In diesem Thema wird das automatische UM-Telefonzentralenfeature in Unified Messaging erläutert.

## Automatische Telefonzentralen

In Telefonie- bzw. Unified Messaging-Umgebungen verbindet eine automatische Telefonzentrale bzw. deren Menüsystem Anrufer mit der Durchwahl eines Benutzers oder einer Abteilung ohne Eingriffe durch Mitarbeiter der Vermittlungsstelle. Bei vielen automatischen Telefonzentralensystemen kann durch das Drücken von bzw. die Spracheingabe "Null" eine Verbindung mit der Telefonvermittlung hergestellt werden. Eine automatische Telefonzentrale ist in den meisten modernen Nebenstellenanlagen, IP-Nebenstellenanlagen und Unified Messaging-Lösungen vorhanden.

Bei einigen automatischen Telefonzentralensystemen gibt es rein informative Ansagemenüs und Sprachmenüs, über die eine Organisation ihre Geschäftszeiten, Hinweise zur Anfahrt zu ihren Standorten, Informationen zu freien Stellen und Antworten auf häufig gestellte Fragen bekannt geben kann. Nach Wiedergabe der Ansage wird der Anrufer mit der Vermittlungsstelle verbunden oder kann zum Hauptmenü zurückkehren.

In komplexeren automatischen Telefonzentralensystemen dient das Menüsystem zum Suchen nach anderen Menüs der automatischen Telefonzentrale, zum Auffinden eines Benutzers im System oder zum Verbinden mit einer anderen Amtsleitung. Das Menüsystem ermöglicht dem Anrufer auch die Interaktion mit dem System in bestimmten Situationen, z. B. wenn ein Student sich bei einem Seminar anmeldet, seine Noten abfragt oder eine Kreditkarte per Telefon aktiviert wird.

Obgleich automatische Telefonzentralen meist sehr nützlich sind, können sie bei falscher Planung und Konfiguration Anrufer verwirren und frustrieren. Insbesondere in großen Organisationen können Anrufer bei nicht ordnungsgemäß konfigurierter automatischer Telefonzentrale durch eine Vielzahl von Fragen und Menüansagen geführt werden, ehe sie letztlich mit einer Person verbunden werden, die ihre Frage beantworten kann.

## Automatische UM-Telefonzentralen

Unified Messaging ermöglicht je nach den Anforderungen Ihrer Organisation die Einrichtung einer oder mehrerer automatischer UM-Telefonzentralen. Automatische UM-Telefonzentralen dienen zum Erstellen eines sprachgesteuerten Menüsystems für eine Organisation, mit dessen Hilfe sich interne und externe Anrufer im Menüsystem der automatischen UM-Telefonzentrale bewegen können, um Benutzer und Abteilungen in einer Organisation auffinden und Anrufe an diese richten oder weiterleiten zu können.

Wenn anonyme oder nicht authentifizierte Benutzer eine externe geschäftliche Telefonnummer oder interne Anrufer eine bestimmte Durchwahlnummer anrufen, wird eine Folge von Ansagen wiedergegeben, mit deren Hilfe sie sich mit einem Benutzer verbinden bzw. einen Benutzer in der Organisation auffinden und sich anschließend mit diesem Benutzer verbinden können. Die automatische UM-Telefonzentrale gibt eine Folge von Telefonansagen bzw. WAV-Dateien wieder, die Anrufer anstelle eines Mitarbeiters der Vermittlungsstelle hören, wenn sie eine

Organisation anrufen, die mit Unified Messaging arbeitet. Die automatische UM-Telefonzentrale ermöglicht Anrufern, sich mithilfe von MFV-Tasten- oder Spracheingaben durch das Menüsystem zu bewegen, Anrufe zu tätigen oder Benutzer aufzufinden. Damit die automatische Spracherkennung oder Spracheingaben verwendet werden können, muss die automatische Spracherkennung jedoch für die automatische UM-Telefonzentrale aktiviert werden.

Eine automatische UM-Telefonzentrale bietet Folgendes:

- Geschäftliche oder informative Begrüßungsansagen.
- Benutzerdefinierte unternehmensbezogene Menüs. Sie können diese Menüs auf mehrere Ebenen erweitern.
- Eine Telefonbuchsuefunktion, mit deren Hilfe ein Anrufer das Telefonbuch der Organisation nach einem Namen durchsuchen kann.
- Eine Möglichkeit für den Anrufer, sich mit einem Mitarbeiter verbinden zu lassen oder diesem eine Nachricht zu hinterlassen.

Sie können eine unbegrenzte Anzahl von automatischen UM-Telefonzentralen erstellen. Jede automatische Unified Messaging-Telefonzentrale kann eine unbeschränkte Anzahl von Durchwahlnummern unterstützen. Eine automatische UM-Telefonzentrale kann nur auf einen einzigen Satz mit UM-Wähleinstellungen verweisen. Automatische UM-Telefonzentralen können auch auf andere automatische UM-Telefonzentralen verweisen oder mit diesen verknüpft werden.

Ein eingehender Anruf von einer externen Telefonnummer oder eine interne Telefondurchwahl werden zwischen Exchange-Servern übergeben und anschließend an eine automatische UM-Telefonzentrale gesendet. Die automatische UM-Telefonzentrale wird vom Administrator für die Verwendung von vorab aufgezeichneten Sprachdateien (WAV-Dateien) konfiguriert, die für Anrufer wiedergegeben werden und ihnen ermöglichen, durch das Unified Messaging-Menüsystem zu navigieren. Sie können bei der Konfiguration einer automatischen UM-Telefonzentrale alle verwendeten WAV-Dateien an die Anforderungen Ihrer Organisation anpassen.

## Automatische Telefonzentrale mit mehreren Sprachen

Es sind Situationen vorstellbar, in denen Sie für Anrufer automatische Telefonzentralen in verschiedenen Sprachen bereitstellen müssen. Mit der für eine automatische UM-Telefonzentrale verfügbaren Spracheinstellung können Sie die Standardansagesprache für die automatische Telefonzentrale konfigurieren. Wenn Sie die Standardsystemansagen für die automatische Telefonzentrale verwenden, ist dies die Sprache, die ein Anrufer hört, wenn die automatische Telefonzentrale den eingehenden Anruf beantwortet. Diese Spracheinstellung wirkt sich nur auf die verfügbaren standardmäßigen Systemansagen aus. Diese Spracheinstellung wirkt sich nicht auf benutzerdefinierte Ansagen aus, die für eine automatische Telefonzentrale konfiguriert werden.

Wenn Sie bei lokalen oder Hybridbereitstellungen die US-englische Version installieren, ist Englisch (USA) die einzige Sprache, die zum Konfigurieren automatischer UM-Telefonzentralen verfügbar ist. Wenn Sie eine lokalisierte Version installieren, beispielsweise Japanisch, können Sie für die von Ihnen erstellte automatische Telefonzentrale festlegen, ob als Standardsprache Japanisch oder Englisch (USA) verwendet wird. Auf einem Unified Messaging-Server können zusätzliche UM-Sprachpakete installiert werden, um andere Standardsprachen für eine automatische Telefonzentrale zu verwenden.

Wenn Sie z. B. ein Geschäft an einem Standort in den Vereinigten Staaten betreiben und dennoch ein Menüsystem erforderlich ist, das für Anrufer die Optionen Englisch (USA), Spanisch und Französisch bereitstellt, müssen Sie zuerst die benötigten UM-Sprachpakete installieren. Wenn Sie die englische Version (USA) installiert haben, installieren Sie in diesem Fall die UM-Sprachpakete für Spanisch und Französisch. Da für eine automatische Unified Messaging-Telefonzentrale jedoch immer nur jeweils eine Sprache konfiguriert sein kann, müssen vier automatische Telefonzentralen erstellt werden: eine automatische Haupttelefonzentrale, die für die Verwendung von Englisch (USA) konfiguriert ist, sowie eine weitere automatische Telefonzentrale für jede weitere Sprache: Englisch (USA), Spanisch und Französisch. Anschließend konfigurieren Sie die automatische Haupttelefonzentrale

so, dass sie über die richtigen Tastenzuordnungen bzw. die richtige Menünavigation für den Zugriff auf die anderen automatischen Telefonzentralen verfügt, die Sie für jede Sprache erstellt haben. In diesem Beispiel beantwortet die automatische Haupttelefonzentrale den eingehenden Anruf, und der Anrufer hört "Welcome to Contoso, Ltd. For English, press or say 1. For Spanish, press or say 2. For French, press or say 3."

**TIP**

In Exchange UM können authentifizierte und nicht authentifizierte Outlook Voice Access Benutzer nicht in allen Sprachen per Sprachangabe im Verzeichnis nach Benutzern suchen. Anrufer, die in einer automatischen Telefonzentrale anrufen, können die Spracheingabe jedoch in mehreren Sprachen für die Navigation im Menü der automatischen Telefonzentrale und die Suche nach Benutzern in dem Verzeichnis verwenden.

## Begrüßungen für außerhalb und während der Geschäftszeiten

Nachdem Sie eine automatische UM-Telefonzentrale erstellt haben, wird für Anrufer eine Standardsystemansage als Begrüßungsansage für das Hauptmenü außerhalb der Geschäftszeiten wiedergegeben, nachdem die Begrüßung außerhalb der Geschäftszeiten wiedergegeben wurde. Auch wenn Systemansagen nicht ersetzt oder geändert werden dürfen, möchten Sie möglicherweise die Begrüßungen und Ansagen für das Menü anpassen, die für automatische UM-Telefonzentralen verwendet werden. Häufig möchten Sie wahrscheinlich nicht nur eine benutzerdefinierte Begrüßung außerhalb der Geschäftszeiten konfigurieren, sondern auch eine benutzerdefinierte Ansage für das Hauptmenü außerhalb der Geschäftszeiten erstellen und konfigurieren. Nachdem Sie eine benutzerdefinierte Ansage für das Hauptmenü außerhalb der Geschäftszeiten konfiguriert haben, müssen Sie für die automatische UM-Telefonzentrale Tastenzuordnungen außerhalb der Geschäftszeiten aktivieren.

Eine benutzerdefinierte Geschäftszeiten Hauptmenü Prompt Begrüßung ist eine Liste der Optionen, die Anrufer, während der Geschäftszeiten hören. Damit um Anrufer eine außerhalb der Geschäftszeiten Hauptmenü Prompt Begrüßung hören zu können, müssen Sie zuerst mithilfe der Exchange-Verwaltungskonsole oder das Cmdlet **Set-UMAutoAttendant** im Exchange Online PowerShell den Zeitplan Geschäfts- und außerhalb der Geschäftszeiten konfigurieren. Beispielsweise "haben Sie Trey Research Geschäftszeiten erreicht. Wenn Sie eine medizinische Emergency auftreten, wenden Sie sich legen Sie auf, und wählen Sie 911. Um eine Nachricht für eine der unsere Ärzten zu lassen, geben Sie 1. Um eine Nachricht an eine der unsere physische Physiotherapeuten zu lassen, drücken Sie die 2. Um eine allgemeine Meldung eines unsere Front Office Koordinatoren zu lassen, drücken Sie 3. Verbindung mit einer nach Stunden Operator, drücken Sie die 0. "

Wenn Sie eine automatische UM-Telefonzentrale erstellen, sind standardmäßig die Begrüßungen und Telefonansagen innerhalb und außerhalb der Geschäftszeiten nicht konfiguriert, und es sind keine Menünavigationseinträge für Telefonansagen für das Hauptmenü innerhalb und außerhalb der Geschäftszeiten definiert. Um die benutzerdefinierten Begrüßungen und Ansagen für das Hauptmenü außerhalb der Geschäftszeiten ordnungsgemäß zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

1. Konfigurieren der Zeiten während und außerhalb der Geschäftszeiten auf der Seite **Geschäftszeiten**.
2. Erstellen der Begrüßungsdatei, die für die Begrüßung außerhalb der Geschäftszeiten verwendet wird.
3. Konfigurieren der Begrüßung außerhalb der Geschäftszeiten auf der Seite **Begrüßungen**.
4. Erstellen der Begrüßungsdatei, die für die Ansage für das Hauptmenü außerhalb der Geschäftszeiten verwendet wird.
5. Konfigurieren der Begrüßungsansage für das Hauptmenü außerhalb der Geschäftszeiten auf der Seite **Begrüßungen**.
6. Aktivieren der Menünavigation und Hinzufügen von Menünavigationseinträgen auf der Seite **Menünavigation**.

## Menünavigationseinträge

Wenn Sie die standardmäßige Telefonansage für das Hauptmenü verwenden und einen oder mehrere Menünavigationseinträge definieren, synthetisiert das UM-TTS-Modul (Text-zu-Sprache) eine Telefonansage für das Hauptmenü. Das TTS-Modul synthetisiert eine Telefonansage für das Hauptmenü jedoch nur, wenn die Standardbegrüßung konfiguriert und mindestens ein Menünavigationseintrag definiert wurde. Das TTS-Modul synthetisiert keine Telefonansage für das Hauptmenü, wenn Sie eine benutzerdefinierte Telefonansage für das Hauptmenü verwenden. Beispiel: "Drücken Sie die 1, wenn Sie mit der Vertriebsabteilung sprechen möchten. Drücken Sie die 2, wenn Sie mit dem Kundensupport sprechen möchten." Zum Erstellen dieser Telefonansage für das Hauptmenü müssen Sie zwei Menünavigationseinträge erstellen: eine mit der Bezeichnung "Vertriebsabteilung" und eine weitere mit der Bezeichnung "Kundensupport". Anschließend wird der Tastenzuordnungseintrag zum Abspielen einer Audiodatei, zur Weiterleitung an eine Durchwahl oder zur Weiterleitung des Anrufers an eine andere automatische Telefonzentrale konfiguriert.

Beim Konfigurieren von Menünavigationseinträgen definieren Sie die Optionen und Vorgänge, die durchgeführt werden, wenn ein Anrufer bei Verwendung einer sprachaktivierten automatischen Telefonzentrale ein bestimmtes Wort sagt oder bei Verwendung einer nicht sprachaktivierten automatischen Telefonzentrale eine Taste auf der Telefontastatur drückt. Zum Konfigurieren von Menünavigationseinträgen für eine automatische Telefonzentrale müssen Sie folgende Aktionen ausführen:

- Aktivieren die Menünavigation während der Geschäftszeit.
- Hinzufügen von Menünavigationseinträgen.
- Eingeben des Namens des Menünavigationseintrags.
- Auswählen einer Option in der Liste **Wenn diese Taste gedrückt wird** und Hochladen der wiederzugebenden Audiodatei über das Feld **Folgende Audiodatei wiedergeben**.
- Konfigurieren der auszuführenden Aktion:
  - Weiterleiten an diese Durchwahl
  - Weiterleiten an diese automatische UM-Telefonzentrale
  - Sprachnachricht für diesen Benutzer hinterlassen
  - Unternehmensstandort ansagen
  - Geschäftszeiten ansagen

## Beispiele für automatische Telefonzentralen

Die folgenden Beispiele veranschaulichen die Verwendung von automatischen UM-Telefonzentralen mit Unified Messaging:

- **Beispiel 1:** externe Kunden können an einer Firma namens Contoso, Ltd. drei externe Telefonnummern: 425-555-0111 (Zweigstellen) 425-555-0122 (Produktsupport) und 425-555-0133 (Sales). Die Personalabteilung, Verwaltung und Buchhaltung Abteilungen interne Telefon Erweiterungen verfügen und müssen von der Corporate Büros automatische um-Telefonzentrale zugegriffen werden.

Um eine automatische UM-Telefonzentralenstruktur einzurichten, die dieses Szenario unterstützt, müssen drei automatische UM-Telefonzentralen mit jeweils der entsprechenden externen Telefonnummer erstellt und konfiguriert werden. Erstellen Sie für jede Abteilung von "Unternehmensstandorte" drei weitere automatische UM-Telefonzentralen. Anschließend konfigurieren Sie jede weitere automatische UM-Telefonzentrale basierend auf den jeweiligen Anforderungen, z. B. mit einer Begrüßungsansage oder anderen Informationen zur Navigation.

- **Beispiel 2:** bei einer Firma namens Contoso, Ltd. externe Kunden eine Hauptfenster Zahl für das Unternehmen, 425-555-0100 aufrufen. Wenn ein externer Anrufer externe Nummer aufruft, UM-Telefonzentrale beantwortet und fordert den Aufrufer durch sagen, "Willkommen an Contoso, Ltd. Drücken Sie die, oder sagen Sie "1" corporate Administration übertragen werden. Drücken Sie die, oder sagen Sie "2" Produktsupport übertragen werden. Drücken Sie die, oder sagen Sie "Drei" Unternehmensinformationen übertragen werden. Drücken Sie oder sagen Sie "NULL" in den Operator übertragen werden." Um eine UM automatische Telefonzentrale-Struktur zu erstellen, die in diesem Szenario unterstützt, erstellen Sie eine automatische um-Telefonzentrale, die Erweiterungen angepasst wurde, die den Anruf an die entsprechende Durchwahlnummer weiterleiten.

# DTMF-Schnittstelle

18.12.2018 • 14 minutes to read

In Unified Messaging (UM) können Anrufer DTMF (Dual Tone Multi-Frequency), auch als Tonwahl bezeichnet, und Spracheingaben für die Interaktion mit dem System verwenden. Welches Verfahren Benutzer verwenden können, hängt davon ab, wie der UM-Wählplan und automatischen Telefonzentralen konfiguriert sind.

Die DTMF-Schnittstelle ermöglicht Anrufern, die Telefontastatur für die Suche nach Benutzern und für die Navigation im UM-Voicemail-Menüsyste zu verwenden, wenn sie eine Outlook Voice Access-Nummer anrufen, die für einen Wählplan konfiguriert ist, oder wenn sie eine Telefonnummer anrufen, die für eine automatische Telefonzentrale konfiguriert ist. In diesem Thema wird die DTMF-Schnittstelle und ihre Verwendung durch Anrufer bei der Suche nach Benutzern und der Navigation im UM-Voicemail-Menüsyste behandelt.

## DTMF (Übersicht)

Für DTMF ist es erforderlich, dass ein Anrufer eine Taste auf der Tastatur des Telefons drückt, die einer Unified Messaging-Menüoption entspricht, oder den Namen eines Benutzers mithilfe der Buchstaben auf den Tasten eingibt, indem er den Namen oder den E-Mail-Alias des Benutzers buchstabiert. Anrufer verwenden ggf. DTMF, weil die automatische Spracherkennung (Automatic Speech Recognition, ASR) nicht aktiviert wurde bzw. das Verwenden von Sprachbefehlen zu einem Fehler geführt hat. In beiden Fällen werden DTMF-Eingaben für die Navigation in Menüs und die Suche nach Benutzern verwendet.

In UM werden DTMF-Eingaben standardmäßig für Wählpläne verwendet und stellen die Anruferstandardschnittstelle für automatische UM-Telefonzentralen dar.

Anrufer können DTMF-Eingaben für Folgendes verwenden:

- Wählplan-Teilnehmerzugriff mithilfe von Outlook Voice Access.
- Wähleinstellungen-Verzeichnissuchvorgänge und Suchvorgänge nach Benutzern.
- Automatische Telefonzentralen, die nicht sprachaktiviert sind.
- Automatische Telefonzentralen, die sprachaktiviert sind und für die ggf. eine automatische DTMF-Fallback-Telefonzentrale konfiguriert ist.
- Automatische DTMF-Fallback-Telefonzentralen (nicht sprachaktiviert).

## UM-Wählpläne und "Wahl nach Namen"

Wenn Sie einen Satz UM-Wähleinstellungen erstellen, können Sie die primäre und die sekundäre Eingabemethode konfigurieren, die Anrufer zum Nachschlagen von Namen verwenden, wenn sie nach einem Benutzer suchen oder mit diesem Kontakt aufnehmen möchten. Diese Einstellungen werden auf der Seite **Einstellungen** des Wählplans vorgenommen und als **Primäre Methode für Namenssuche** und **Sekundäre Methode für Namenssuche** bezeichnet. Nachstehende Optionen sind für die primäre und die sekundäre Methode für Namenssuche verfügbar:

- Nachname Vorname
- Vorname Nachname
- SMTP-Adresse

Zusätzlich steht **Keine** als Option für die sekundäre Methode für Namenssuche zur Verfügung.

Standardmäßig ist **Nachname Vorname** als primäre Methode für Namenssuche ausgewählt, und **SMTP-Adresse** ist als sekundäre Methode für Namenssuche angegeben. Wenn sich ein Anrufer daher in die Teilnehmerzugriffssnummer einwählt, die für den UM-Wählplan konfiguriert ist, wird die Begrüßungsnachricht des Wähleinstellungswahlplans wiedergegeben, und die Vermittlungsstelle sagt z. B.: "Willkommen bei Contoso Outlook Voice Access. Wenn Sie auf Ihr Postfach zugreifen möchten, geben Sie Ihre Durchwahl ein. Um jemanden zu kontaktieren, drücken Sie die Rautetaste." Nachdem der Anrufer die Rautetaste gedrückt hat, antwortet das System mit "Buchstabieren Sie den Namen der Person, die Sie anrufen möchten. Geben Sie zuerst den Nachnamen an. Oder buchstabieren Sie den E-Mail-Alias. Drücken Sie dann zweimal die Rautetaste". In diesem Szenario fordert das System den Anrufer abhängig von der Konfiguration der Wähleinstellungen anschließend auf, zuerst den Nachnamen und dann den Vornamen des Benutzers (Nachname Vorname) einzugeben oder den E-Mail-Alias ohne den Domänennamen zu buchstabieren. Wenn der E-Mail-Alias des Benutzers z. B. "tscholl@contoso.com" lautet, gibt der Anrufer "tscholl" ein.

Wenn Sie diese Konfiguration ändern möchten, weil die Standardeinstellung nicht Ihren Anforderungen entspricht, können Sie Benutzern auch ermöglichen, zuerst den E-Mail-Alias des Benutzers oder den Vornamen, gefolgt vom Nachnamen, einzugeben. In diesem Fall konfigurieren Sie die Option **Primäre Methode für Namenssuche** mit der Einstellung **SMTP-Adresse** und die Option **Sekundäre Methode für Namenssuche** mit der Einstellung **Vorname Nachname**. Die Einstellungen für die Wahlmethoden nach Namen gelten auch für alle automatischen UM-Telefonzentralen, die den Wähleinstellungen zugeordnet sind. Damit Anrufer den Namen des Benutzers mithilfe von DTMF-Eingaben oder der Tasten auf der Telefontastatur eingeben können, müssen eine DTMF-Zuordnung und Werte für den Benutzer im Verzeichnis Ihrer Organisation vorhanden sein.

Weitere Informationen zum Ändern der primären und sekundären Wahlmethoden nach Namen für einen Satz UM-Wähleinstellungen finden Sie unter [Konfigurieren Sie die primäre Methode für Outlook Voice Access-Benutzer suchen](#) und [Konfigurieren Sie die sekundäre Methode für Outlook Voice Access-Benutzer suchen](#).

## DTMF-Zuordnungen

In einer Exchange-Organisation wird ein Attribut namens **msExchUMDtmfMap** jedem Benutzer zugeordnet, der im Verzeichnis erstellt wird. Unified Messaging verwendet dieses Attribut für die Zuordnung des Vornamens, Nachnamens und des E-Mail-Alias zu einem Nummernsatz. Diese Zuordnung wird als DTMF-Zuordnung bezeichnet. Eine DTMF-Zuordnung ermöglicht Anrufern die Eingabe von Zahlen auf der Telefontastatur, die den Buchstaben des Namens oder des E-Mail-Alias des Benutzers entsprechen. Dieses Attribut enthält die Werte, die zum Erstellen einer DTMF-Zuordnung für den Vornamen des Benutzers, gefolgt vom Nachnamen, für den Nachnamen des Benutzers, gefolgt vom Vornamen, und für den E-Mail-Alias des Benutzers benötigt werden.

Die folgende Tabelle zeigt die DTMF-Zuordnungswerte, die in Active Directory für das Attribut **msExchUMDtmfMap** für einen UM-aktivierten Benutzer namens "Thorsten Scholl" mit dem Alias "tscholl@contoso.com" gespeichert werden.

### Für einen UM-aktivierten Benutzer namens "Thorsten Scholl" gespeicherte DTMF-Werte

VERZEICHNISEINGABE	NAME DES BENUTZERS
firstNameLastName:866976484	thorstenscholl
lastNameFirstName:764848669	schollthorsten
emailAddress:876484	tscholl

Namen und E-Mail-Aliase dürfen auch andere, nicht alphanumerische Zeichen enthalten (z. B. Kommas, Bindestriche, Unterstriche oder Punkte). Solche Zeichen werden jedoch nicht in einer DTMF-Zuordnung für einen Benutzer verwendet. Wenn der E-Mail-Alias für Thorsten Scholl z. B. "thorsten-scholl@contoso.com" lautet, ist der Wert der DTMF-Zuordnung 866976484. Der Bindestrich wird nicht berücksichtigt. Wenn der E-Mail-Alias eines

Benutzers jedoch mindestens eine Ziffer enthält, z. B. "thorstenscholl123@contoso.com", werden die Ziffern in der DTMF-Zuordnung verwendet, die erstellt wird. Die DTMF-Zuordnung für "thorstenscholl123" lautet 866976484123.

Für einen Benutzer muss eine DTMF-Zuordnung vorhanden sein, damit Anrufer den Namen oder E-Mail-Alias des Benutzers eingeben können. Es ist jedoch nicht für alle Benutzer eine DTMF-Zuordnung mit ihrem Benutzerkonto verknüpft.

## DTMF-Zuordnungen für Benutzer, die nicht für Unified Messaging aktiviert sind

Benutzer sind nicht standardmäßig für Unified Messaging aktiviert. Dies gilt auch für postfachaktivierte Benutzer.

Für das Attribut **msExchUMDtmfMap** werden die für DTMF-Zuordnungen erforderliche Werte für Benutzer eingegeben, die nicht für UM aktiviert wurden. Standardmäßig werden die folgenden DTMF-Zuordnungen für alle Benutzer erstellt, wenn für diese ein Postfach erstellt wird.

1. emailAddress
2. firstNameLastName
3. lastNameFirstName

Wenn ein Benutzer DTMF-Werte für ihr Konto definierten zuordnen hat, werden nicht Anrufer an den Benutzer zu kontaktieren, wenn sie eine Telefon aus einem UM Auto attendant Menü Taste oder führen Sie eine Verzeichnissuche finden. Darüber hinaus möglich nicht UM-aktivierte Benutzer Nachrichten senden oder übergeben von Anrufen für Benutzer, die eine DTMF-Zuordnung verfügen, es sei denn, diese automatische Spracherkennung Spracherkennung (ASR) verwenden können. Um Anrufer Weiterleiten von Anrufen oder wenden Sie sich an Benutzer zu aktivieren, die UM-aktivierten nicht mithilfe der Telefontastatur sind, müssen Sie die erforderlichen Werte für die DTMF-Zuordnung für diese Benutzer erstellen. Sie können das Cmdlet **Set-User** mit dem *CreateDtmfMap* - Parameter verwenden, erstellen und Aktualisieren eines einzelnen Benutzers DTMF-Zuordnung oder Update einer DTMF für einen Benutzer zuordnen, wenn der Name des Benutzers geändert wurde, nachdem eine DTMF-Zuordnung erstellt wurde. Optional können Sie ein PowerShell-Skript erstellen, mit diesem Cmdlet DTMF-Zuordnung für mehrere Benutzer zu aktualisieren.

Weitere Informationen zum Cmdlet **Set-User** finden Sie unter [Set-User](#).

## DTMF-Zuordnungen für Benutzer, die für Unified Messaging aktiviert sind

Standardmäßig wird eine DTMF-Zuordnung für Benutzer erstellt, wenn diese für Unified Messaging aktiviert werden. Dadurch können Anrufe von externen Anrufern UM-aktivierten Benutzern, nicht UM-aktivierten Benutzern und von anderen UM-aktivierten Benutzern weitergeleitet werden, die die Telefontastatur zum Buchstabieren des Namens oder E-Mail-Alias des Benutzers verwenden.

Nachdem die DTMF-Zuordnungswerte für einen UM-aktivierten Benutzer erstellt wurden, können Anrufer die Verzeichnissuche verwenden. Anrufer nutzen die Verzeichnissuche, wenn sie in den folgenden Situationen die Telefontastatur verwenden:

- So identifizieren oder suchen Sie einen Benutzers, wenn sie eine Outlook Voice Access-Nummer anrufen.
- Suchen nach einem UM-aktivierten Benutzer oder Übergeben von Anrufen an diesen, wenn sie eine automatische UM-Telefonzentrale anrufen.

Weitere Informationen zum Aktivieren eines Benutzers für Unified Messaging finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).

In einigen Fällen ändert eines Benutzers Vornamen, Nachnamen, oder e-Mail-alias, nachdem der Benutzer für UM aktiviert ist. DTMF-Zuordnungswerte des Benutzers werden nicht automatisch aktualisiert. Wenn ein Anrufer gibt den neuen Namen oder die e-Mail-Alias des Benutzers und der Benutzer die DTMF-Zuordnung nicht aktualisiert wurde, um die Änderung an den Namen oder die e-Mail-Alias, der Anrufer nicht suchen den Benutzer im Verzeichnis, das dem Benutzer eine Nachricht senden können , oder übergeben von Anrufen für den Benutzer. Wenn Sie die DTMF-Zuordnung eines Benutzers zu aktualisieren haben, nachdem der Benutzer für UM aktiviert wurde, können Sie das Cmdlet **Set-User** mit dem *CreateDtmfMap* - Parameter verwenden. Sie können auch PowerShell erstellen, die mit diesem Cmdlet aus, wenn Sie die DTMF aktualisieren möchten Skript für mehrere UM-aktivierten Benutzer zugeordnet ist.

**Caution**

Es wird davon abgeraten, die DTMF-Werte für Benutzer manuell mithilfe eines Tools wie ADSI-Editor zu ändern, da diese Vorgehensweise zu inkonsistenten Konfigurationen oder anderen Fehlern führen kann. Zum Erstellen oder Aktualisieren von DTMF-Zuordnungen für Benutzer wird ausschließlich die Verwendung das Cmdlet **Set-UMService** oder das Cmdlet **Set-User** empfohlen.

## Weitere Informationen

[ADSI-Bearbeitung - Übersicht](#)

# Automatische UM-Telefonzentrale - Verfahren

18.12.2018 • 2 minutes to read

[Einrichten einer automatischen UM-Telefonzentrale](#)

[Erstellen einer automatischen UM-Telefonzentrale](#)

[Hinzufügen einer Durchwahlnummer der automatischen Telefonzentrale](#)

[Konfigurieren von Geschäftszeiten](#)

[Erstellen eines Feiertagszeitplans](#)

[Eingeben eines Firmennamens](#)

[Festlegen eines Unternehmensstandorts](#)

[Konfigurieren der Zeitzone](#)

[Aktivieren einer benutzerdefinierten Begrüßung während der Geschäftszeit](#)

[Aktivieren einer benutzerdefinierten Menüansage innerhalb der Geschäftszeiten](#)

[Aktivieren einer benutzerdefinierten Begrüßung außerhalb der Geschäftszeit](#)

[Aktivieren einer benutzerdefinierten Menüansage außerhalb der Geschäftszeiten](#)

[Aktivieren einer Informationsansage](#)

[Erstellen einer Menünavigation](#)

[Erstellen von Navigationsmenüs für Geschäftszeiten](#)

[Erstellen Sie außerhalb der Geschäftszeiten Navigationsmenüs](#)

[Verwalten einer automatischen UM-Telefonzentrale](#)

[Konfigurieren Sie eine automatische DTMF-fallback-Telefonzentrale](#)

[Aktivieren einer automatischen UM-Telefonzentrale](#)

[Deaktivieren einer automatischen UM-Telefonzentrale](#)

[Löschen einer automatischen UM-Telefonzentrale](#)

[Aktivieren oder Deaktivieren der automatischen Spracherkennung](#)

[Ermöglichen oder verhindern, dass Weiterleiten von Anrufen von einer automatischen Telefonzentrale](#)

[Aktivieren oder Deaktivieren des Versands von Sprachnachrichten an Benutzer](#)

[Aktivieren oder Deaktivieren der Verzeichnissuche](#)

[Konfigurieren Sie die Gruppe von Benutzern, die kontaktiert werden können](#)

[Konfigurieren einer automatischen Telefonzentrale für Benutzer mit ähnlichen Namen](#)

# Einrichten einer automatischen UM-Telefonzentrale

18.12.2018 • 9 minutes to read

Bei Verwendung von Unified Messaging (UM) können Benutzer nicht nur auf Voicemail zugreifen, sondern Sie können darüber hinaus abhängig von den Anforderungen Ihrer Organisation eine oder mehrere automatische UM-Telefonzentralen erstellen. Automatische UM-Telefonzentralen dienen zum Erstellen eines sprachgesteuerten Menüsystems für eine Organisation, mit dessen Hilfe externe und interne Anrufer Benutzer und Abteilungen in einer Organisation suchen und Anrufe an diese tätigen oder durchstellen können.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Automatische Telefonzentralen

In Telefonie- bzw. Unified Messaging-Umgebungen verbindet eine automatische Telefonzentrale bzw. deren Menüsystem Anrufer mit der Durchwahl eines Benutzers oder einer Abteilung ohne Eingriffe durch Mitarbeiter der Vermittlungsstelle. Bei vielen automatischen Telefonzentralensystemen kann durch das Drücken von bzw. die Spracheingabe "Null" eine Verbindung mit der Telefonvermittlung hergestellt werden. Bei einigen automatischen Telefonzentralensystemen gibt es rein informative Ansagemenüs und Sprachmenüs, über die eine Organisation ihre Geschäftszeiten, Hinweise zur Anfahrt zu ihren Standorten, Informationen zu freien Stellen und Antworten auf häufig gestellte Fragen bekannt geben kann. Nach Wiedergabe der Ansage wird der Anrufer mit der Vermittlungsstelle verbunden oder kann zum Hauptmenü zurückkehren.

Obgleich automatische Telefonzentralen meist sehr nützlich sind, können sie bei falscher Planung und Konfiguration Anrufer verwirren und frustrieren. Insbesondere in großen Organisationen können Anrufer bei nicht ordnungsgemäß konfigurierter automatischer Telefonzentrale durch eine Vielzahl von Fragen und Menüansagen geführt werden, ehe sie letztlich mit einer Person verbunden werden, die ihre Frage beantworten kann.

## Wie richte ich eine automatische Telefonzentrale ein?

In der Exchange-Verwaltungskonsole (EAC) einrichten und Verwalten von automatischen UM-Telefonzentralen, um automatisch Anrufe für Ihre Organisation beantworten und Anrufern Self aus verschiedenen Optionen die Tasten auf selbst per Telefon verwenden. Können Sie nur einen UM-Telefonzentrale, die grundlegende Menünavigation für Anrufer zu Ihrer Organisation bereitstellt können, oder Sie mehrere geschachtelte und Verzweigung Telefonzentralen, die für die Anrufer eine bessere Leistung bieten. In beiden Fällen müssen Sie jedoch planen und Einrichten der automatischen Telefonzentralen sorgfältig.

Gehen Sie folgendermaßen vor, um eine neue automatische UM-Telefonzentrale zu planen und zu erstellen:

1. Entscheiden Sie, ob Benutzer die Möglichkeit haben sollen, über Spracheingaben mit der automatischen Telefonzentrale zu interagieren.
2. Entscheiden Sie, welche Sprache für Ihre automatische Haupttelefonzentrale verwendet werden soll und ob weitere automatische Telefonzentralen zur Unterstützung zusätzlicher Sprachen erstellt werden müssen.
3. Entscheiden Sie, welche Geschäftszeiten für die automatische Telefonzentrale gelten sollen, und legen Sie diese über die Option **Geschäftszeiten** fest. Wenngleich dies nicht erforderlich ist, können Sie auch einen Feiertagszeitplan für diese automatische Telefonzentrale festlegen.

**NOTE**

Außerdem sollten Sie die Zeitzone für die Telefonzentrale angeben.

4. Entscheiden Sie, ob standardmäßige, vom System generierte Begrüßungen während und außerhalb der Geschäftszeiten verwendet werden sollen, oder ob Sie benutzerdefinierte Aufzeichnungen erstellen möchten.

Wenn Sie benutzerdefinierte Begrüßungen verwenden möchten, sollten Sie die Begrüßungen planen und aufzeichnen, die während und außerhalb der Geschäftszeiten für Anrufer wiedergegeben werden. Bei Bedarf können Sie auch eine benutzerdefinierte Informationsansage als Begrüßung erstellen. Beispielsweise können Sie als Begrüßung während der Geschäftszeiten folgende Ansage aufzeichnen: „Herzlich willkommen bei Contoso. Wenn Sie technischen Support benötigen, drücken oder sagen Sie 1. Wenn Sie mit einem Vertriebsmitarbeiter sprechen möchten, drücken oder sagen Sie 2.“ Für eine Begrüßung außerhalb der Geschäftszeiten können Sie beispielsweise das folgende Skript aufzeichnen: „Herzlich willkommen bei Contoso. Unser Büro ist vorübergehend geschlossen. Wir sind ab Montag, 8:00 Uhr, wieder für Sie da.“

5. Planen Sie die Struktur Ihrer automatischen Telefonzentrale gemäß Ihren individuellen Geschäftsanforderungen. Ein multinationales Unternehmen mit Niederlassungen in Deutschland und Großbritannien würde z. B. eine Struktur mit mehreren Sprachen benötigen. Und ein Unternehmen mit verschiedenen Niederlassungen für Zentrale, Vertrieb und Kundendienst würde eine automatische Telefonzentrale benötigen, die direkt mit der Unternehmensstruktur verknüpft ist.
6. Entscheiden Sie, ob Sie automatische DTMF-Fallback-Telefonzentralen oder andere automatische Telefonzentralen benötigen, wenn die Sprachbefehle der automatischen Telefonzentrale nicht funktionieren.
7. Planen Sie die Menünavigation für Zeitspannen innerhalb und außerhalb der Geschäftszeiten. Für jede automatische Telefonzentrale (einschließlich automatische DTMF-Telefonzentralen) müssen Menüansagen und Einträge für die Menünavigation geplant und konfiguriert werden. Diese Schritte sind sowohl für Zeitspannen innerhalb als auch außerhalb der Geschäftszeiten erforderlich.
8. Folgendes ist ein Beispiel für ein Arbeitsblatt, mit dem Sie die Menünavigation außerhalb der Geschäftszeiten planen können.

Schlüssel	Aufforderung/Navigation Eintrag Menüname	So zeichnen Sie Antwort
1	Sprachauswahl für Englisch.	„Drücken oder sagen Sie 1, um zur englischen Navigation zu wechseln.“
2	Kontostand	„Drücken oder sagen Sie 2, um Ihren Kontostand abzurufen.“
3	Weiterleitung zum Vertrieb	„Drücken oder sagen Sie 3, um zu unserer Verkaufsabteilung durchgestellt zu werden.“
4	Weiterleitung zum Kundendienst	„Drücken oder sagen Sie 4, um mit einem Kundendienstmitarbeiter verbunden zu werden.“
5	Geschäftszeiten	Keine Antwort erforderlich.
6	Geschäftsstandort	Keine Antwort erforderlich.

9. Zeichnen Sie anhand des Menünavigationsplans Ansagen auf, mit denen die Anrufer über ihre Optionen informiert werden: Zum Beispiel können Sie bei der in der Tabelle dargestellten Menünavigation außerhalb der Geschäftszeiten das folgende Skript aufzeichnen: "Um eine Nachricht an die Vertriebsabteilung zu hinterlassen, drücken Sie die Eins. Drücken Sie die Zwei, um unsere Geschäftszeiten zu erfahren. Drücken Sie die Drei, um unsere Adresse zu erfahren."
10. Legen Sie fest, wie Anrufer auf Ihre Organisation zugreifen werden. Berücksichtigen Sie, wie diese Anrufer nach Benutzern in Ihrer Organisation suchen und diese kontaktieren werden. Berücksichtigen Sie außerdem, wie Anrufer weitergeleitet werden. Dies umfasst u. a., wie Anrufer mit einem Mitarbeiter verbunden werden bzw. ob Anrufer während und außerhalb der Geschäftszeiten an eine Vermittlungsstelle weitergeleitet werden.
11. Legen Sie fest, welche Anrufe Anrufer tätigen können, wenn sie eine bestimmte automatische Telefonzentrale verwenden. Bestimmen Sie z. B., ob Anrufer Benutzer in einem einzigen Wählplan oder mit einer beliebigen Durchwahl anrufen dürfen bzw. ob externe Anrufe getätigt werden können.
12. Nachdem Sie die Einstellungen für die automatische Telefonzentrale, Begrüßungen und Menünavigation geplant haben und Audiodateien mit den aufgezeichneten Begrüßungen sowie den Menünavigationsansagen und -antworten erstellt haben, kann die automatische Telefonzentrale erstellt und konfiguriert werden. Vorgehensweise:
  - [Erstellen einer automatischen UM-Telefonzentrale](#)
  - [Verwalten einer automatischen UM-Telefonzentrale](#)
13. Wenn Sie die Struktur und die Einstellungen der automatischen Telefonzentrale erstellt und konfiguriert haben, aktivieren Sie die automatische UM-Telefonzentrale, sodass Anrufe entgegengenommen werden können.

# Erstellen einer automatischen UM-Telefonzentrale

18.12.2018 • 8 minutes to read

Nachdem Sie eine automatische Telefonzentrale von Unified Messaging (UM) erstellt haben, werden eingehende Anrufe an eine externe Telefonnummer, die ein human Operator normalerweise beantwortet werden von der automatischen Telefonzentrale beantwortet. Im Gegensatz zu mit anderen Komponenten Unified Messaging sind nicht wie UM einwählen Pläne und UM-IP-Gateways, Sie erforderlich, um automatischen UM-Telefonzentralen erstellen. Allerdings Telefonzentralen unterstützen interne und externe Anrufer suchen, Benutzer oder Abteilungen, die in einer Organisation vorhanden und durchstellen von Anrufen an diese.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Erstellen einer automatischen UM-Telefonzentrale

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**, wählen Sie den UM-Wählplan, für die Sie eine automatische Telefonzentrale hinzufügen möchten, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen** **neu**
3. Geben Sie auf der Seite **neue UM-Telefonzentrale** die folgenden Informationen ein:
  - **Name:** in diesem Feld können Sie den Anzeigenamen für die automatische Telefonzentrale erstellen. Ein um-Name der automatischen Telefonzentrale ist erforderlich und muss eindeutig sein. Es wird jedoch nur für die Anzeige in der Exchange-Verwaltungskonsole und Exchange Online PowerShell verwendet.

Falls Sie den Namen für die automatische Telefonzentrale nach ihrer Erstellung ändern möchten,

müssen Sie zunächst die vorhandene automatische UM-Telefonzentrale löschen und anschließend eine andere automatische Telefonzentrale mit dem gewünschten Namen erstellen. Wenn in Ihrer Organisation mehrere automatische UM-Telefonzentralen eingesetzt werden, sollten Sie aussagekräftige Namen für Ihre automatischen UM-Telefonzentralen verwenden. Die maximale Länge für den Namen einer automatischen UM-Telefonzentrale beträgt 64 Zeichen inklusive Leerzeichen.

Auch wenn Sie eine neue automatische um-Telefonzentrale einschließen von Leerzeichen, benennen können, wenn Sie Unified Messaging mit Office Communications Server 2007 R2 oder Microsoft Lync Server integriert werden soll, kann nicht der Name der automatischen Telefonzentrale Leerzeichen enthalten. Aus diesem Grund, wenn Sie eine automatische Telefonzentrale mit Leerzeichen in den Anzeigenamen erstellt, und Sie eine mit Office Communications Server 2007 R2 oder Lync Server Integration haben, muss zuerst gelöscht, automatische Telefonzentrale und erstellen Sie dann eine andere automatische Telefonzentrale, die Leerzeichen enthalten nicht in der Anzeigename.

- **Diese automatische Telefonzentrale als aktiviert erstellen:** Aktivieren Sie dieses Kontrollkästchen aktivieren die automatische Telefonzentrale auf eingehende Anrufe entgegennehmen, wenn neue UM automatische Telefonzentrale des Assistenten ausführen. Standardmäßig wird eine neue automatische Telefonzentrale erstellt als deaktiviert.

Wenn Sie die automatische Telefonzentrale als deaktiviert erstellen möchten, können Sie die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell die automatische Telefonzentrale aktiviert werden, nachdem Sie den Assistenten zu beenden.

- **Legen Sie die automatische Telefonzentrale zum Reagieren auf Sprachbefehle:** Aktivieren Sie dieses Kontrollkästchen Speech-UM-Telefonzentrale aktivieren. Wenn die automatische Telefonzentrale sprachaktiviert ist, können Anrufer an das System Antworten oder benutzerdefinierte Ansagen, die von dem UM verwendete auto attendant mit Tonwahl oder VoIP-Eingaben. In der Standardeinstellung wird nicht die automatischen Telefonzentrale sprachaktivierte werden bei der Erstellung.

Für Anrufer eine Sprachaktivierte automatische Telefonzentrale verwenden müssen Sie das entsprechende UM-Sprachpaket, das Unterstützung der automatischen Spracherkennung Spracherkennung (ASR) enthält installieren und konfigurieren Sie die Eigenschaften der automatischen Telefonzentrale zur Verwendung dieser Sprache.

- **Zugriffsnummern:** in diesem Feld geben die Durchwahlnummern oder Rufnummern, die Anrufer verwendet werden, um die automatische Telefonzentrale erreichen können. Geben Sie eine Durchwahlnummer oder eine Telefonnummer in das Feld, und klicken Sie dann auf **Hinzufügen**  die Nummer der Liste hinzufügen. Die Anzahl der Nachkommastellen in die Durchwahlnummer oder die Telefonnummer, die Sie bereitstellen muss nicht die Anzahl der Nachkommastellen für eine Durchwahlnummer ein auf der zugehörigen um-Wählplan konfiguriert übereinstimmen. Dies ist, da direkte Aufrufe zum automatischen UM-Telefonzentralen zulässig sind.

Die Anzahl der Durchwahlnummern oder Telefonnummern eingegeben ist unbegrenzt. Sie können jedoch die neue automatische Telefonzentrale ohne einer Durchwahlnummer aufgeführt erstellen. Eine Durchwahlnummer oder die Telefonnummer ist nicht erforderlich.

Sie können bearbeiten oder Entfernen eines vorhandenen Durchwahlnummer oder die Telefonnummer ein. Klicken Sie auf **Bearbeiten**, zum Bearbeiten einer vorhandenen Durchwahlnummer oder Telefonnummer . Um eine vorhandene Durchwahlnummer oder eine Telefonnummer aus der Liste entfernen möchten, klicken Sie auf **Entfernen** .

4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell zum Erstellen einer automatischen UM-Telefonzentrale

Dieses Beispiel erstellt eine UM-Telefonzentrale mit dem Namen `MyUMAutoAttendant` können eingehende Anrufe jedoch nicht sprachaktiviert akzeptieren.

```
New-UMAutoAttendant -Name MyUMAutoAttendant -UMDialPlan MyUMDialPlan -PilotIdentifierList 55000 -  
Enabled $false
```

Dieses Beispiel erstellt eine Sprachaktivierte automatische Telefonzentrale mit dem Namen `MyUMAutoAttendant`.

```
New-UMAutoAttendant -Name MyUMAutoAttendant -UMDialPlan MyUMDialPlan -PilotIdentifierList 56000,56100 -  
SpeechEnabled $true
```

# Fügen Sie eine automatische Telefonzentrale Durchwahlnummer ein hinzu

18.12.2018 • 4 minutes to read

Sie können in einer automatischen UM-Telefonzentrale (Unified Messaging) eine oder mehrere Durchwahlnummern konfigurieren. Wenn Sie einer automatischen UM-Telefonzentrale eine Durchwahlnummer hinzufügen, kann diese Nummer von Anrufern zum Anrufen der automatischen Telefonzentrale verwendet werden. Außerdem müssen Sie mitunter Durchwahlnummern hinzufügen, weil Anrufer mehr als eine Durchwahlnummer für den Zugriff auf eine automatische Telefonzentrale verwenden können. Standardmäßig werden bei der Erstellung einer automatischen Telefonzentrale keine Durchwahlnummern konfiguriert.

Sie können eine neue automatische Telefonzentrale erstellen, ohne dass Sie hierfür eine Durchwahlnummer einrichten. Sie können einer einzigen automatischen Telefonzentrale auch mehrere Telefon- oder Durchwahlnummern zuordnen. Sie können die Durchwahlnummern entweder beim Erstellen der automatischen UM-Telefonzentrale oder nach der Konfiguration der automatischen Telefonzentrale hinzufügen. Die Anzahl der Ziffern der Durchwahlnummer, die Sie für die automatische UM-Telefonzentrale konfigurieren, muss der Anzahl der Ziffern einer Durchwahlnummer entsprechen, die in dem der automatischen UM-Telefonzentrale zugeordneten UM-Wählplan konfiguriert ist.

## NOTE

Sie können auch eine SIP-Adresse (Session Initiation Protocol) anstelle einer Durchwahlnummer hinzufügen. Eine SIP-Adresse wird von einigen IP-Nebenstellenanlagen und von Office Communications Server 2007 R2 oder Microsoft Lync Server verwendet.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Hinzufügen von Durchwahl- oder Telefonnummern für eine automatische UM-Telefonzentrale mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. Wählen Sie in der Listenansicht den UM-Wählplan zu bearbeiten, und klicken Sie auf **Bearbeiten**  

2. Wählen Sie auf der Seite **UM-Wählplan** unter **Automatische UM-Telefonzentralen** die automatische UM-Telefonzentrale aus, zu der Sie Durchwahl- oder Telefonnummern hinzufügen möchten.
3. Klicken Sie auf der Symbolleiste auf **Bearbeiten**  

4. Klicken Sie auf der Seite **UM-Telefonzentrale > Allgemein** unter **Zugriffsnummern** in das Textfeld Geben Sie die Erweiterung oder die Rufnummer ein, die Sie verwenden möchten und klicken Sie auf **Hinzufügen**  

5. Klicken Sie auf **Speichern**, um die Nummer hinzuzufügen.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie eine Durchwahlnummer ein auf einer automatischen UM-Telefonzentrale

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert **MyUMAutoAttendant** mit mehreren Durchwahlnummern.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -PilotIdentifierList "12345, 72000, 75000"
```

# Konfigurieren von Geschäftszeiten

18.12.2018 • 4 minutes to read

Bei der Konfiguration der Geschäftszeiten für eine automatische Unified Messaging (UM)-Telefonzentrale definieren Sie die Zeit, in der Ihre Organisation täglich zu erreichen ist, sowie die Begrüßung während der Geschäftszeiten und die Menüansagen, die Anrufer hören, wenn sie eine in der automatischen Telefonzentrale konfigurierte Durchwahlnummer anwählen. Wenn ein Anrufer die automatische Telefonzentrale während der Stunden erreicht, die außerhalb der von Ihnen definierten Geschäftszeiten liegen, hört der Anrufer die Ansagen und Begrüßungen, die außerhalb der Geschäftszeiten wiedergegeben werden.

In der Exchange-Verwaltungskonsole stehen einige Zeitplanoptionen zur Verfügung. Die Geschäftszeiten der meisten Unternehmen sind Montag bis Freitag zwischen 8:00 Uhr und 17:00 Uhr. In einigen Fällen entsprechen die Standardoptionen vielleicht nicht Ihren Anforderungen und Sie müssen den Zeitplan anpassen. Wenn Ihre Geschäftszeiten von den vom System definierten Zeitplänen abweichen, können Sie einen angepassten Zeitplan für die automatische Telefonzentrale definieren.

Standardmäßig gibt die automatische UM-Telefonzentrale zu jeder Tageszeit bei einem Anruf die Ansagen und Begrüßungen für die Geschäftszeiten wieder.

## NOTE

Wenn Sie den Zeitplan für die Zeiten während und außerhalb der Geschäftszeiten für eine automatische UM-Telefonzentrale festlegen, vergewissern Sie sich, dass die Zeitzone ordnungsgemäß konfiguriert ist.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Festlegen der Geschäftszeiten für eine automatische UM-Telefonzentrale

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  

2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie die Geschäftszeiten festlegen möchten, und klicken Sie dann auf **Bearbeiten**  

3. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale > Geschäftszeiten** unter **Geschäftszeiten** auf **Geschäftszeiten konfigurieren**.
4. Wählen Sie auf der Seite **Geschäftszeiten konfigurieren** die Stunden aus, die für die einzelnen Wochentage als Geschäftszeiten gelten sollen.
5. Klicken Sie auf **OK** und dann auf **Speichern**.

## Verwenden von Exchange Online PowerShell Geschäftszeiten für eine automatische um-Telefonzentrale an

In diesem Beispiel wird der Geschäftszeiten für einen UM-Telefonzentrale mit dem Namen **MyUMAutoAttendant**.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.13:15,1.09:00-  
1.17:00,6.09:00-6.16:30
```

# Erstellen eines Feiertagszeitplans

18.12.2018 • 6 minutes to read

Sie können die Datums- und Zeitangaben definieren, zu denen Ihre Organisation an Feiertagen oder zu anderen Gelegenheiten geschlossen ist. Innerhalb der von Ihnen festgelegten Start- und Enddatumsangaben erreichen Anrufer die automatische Unified Messaging (UM)-Telefonzentrale und hören die entsprechende Feiertagsansage, die Sie beim Konfigurieren des Feiertagszeitplans angeben. Nach der von Ihnen angegebenen Feiertagsansage werden die Begrüßungen und Menüansagen außerhalb der Geschäftszeiten zur Information für den Anrufer wiedergegeben.

Sie können auch einen Feiertagszeitplan innerhalb eines vorhandenen Feiertagszeitplans erstellen. Wenn Sie mehrere Feiertagszeitpläne erstellen, erlaubt Unified Messaging die Überschneidung von geplanten Feiertagszeiten. Sie können z. B. einen Feiertagszeitplan vom 15. bis zum 31. Dezember erstellen, weil Ihre Organisation wegen Bauarbeiten geschlossen ist, und Sie können einen weiteren Feiertagszeitplan vom 24. bis zum 26. Dezember definieren. Wenn Anrufer zwischen dem 15. und 23. Dezember und zwischen dem 27. und 31. Dezember die automatische Telefonzentrale anrufen, hören Sie die Feiertagsbegrüßung, die Sie für diesen Zeitraum angegeben haben. Beispiel: "Das Unternehmen ist zurzeit aufgrund von Baumaßnahmen geschlossen." Wenn Anrufer zwischen dem 24. und 26. Dezember anrufen, hören Sie eine andere Feiertagsbegrüßung, z. B. "Wir haben zurzeit aufgrund der Weihnachtsfeiertage geschlossen."

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Angeben eines Feiertagszeitplans für eine automatische UM-Telefonzentrale mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf der Symbolleiste auf **Bearbeiten** .

2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen** **UM-** Telefonzentrale für die Sie den Feiertag Zeitplan festlegen möchten. Klicken Sie auf der Symbolleiste auf **Bearbeiten** .
3. Klicken Sie auf der Seite **UM-Telefonzentrale > Geschäftszeiten** unter **Feiertag Zeitplan**, klicken Sie auf **Hinzufügen** .
4. Konfigurieren Sie auf der Seite **Neuer Feiertag** Folgendes:
  - **Name:** Geben Sie einen Namen für den Terminplan Feiertag.
  - **Feiertag Ansage:** Durchsuchen, um die WAV-Datei, die Sie als der Ansage verwenden möchten. Dies ist ein erforderliches Feld.
  - **Startdatum:** mit dieser Liste können wählen Sie das Datum des Feiertags gestartet werden soll. Der Zeitplan Feiertag beginnt um Mitternacht auf das Datum in dieser Liste angegeben.
  - **Enddatum:** mit dieser Liste können wählen Sie das Datum des Feiertags beendet werden soll. Der Zeitplan Feiertag endet um 23:59 Uhr auf das Datum in dieser Liste angegeben.
5. Nachdem Sie den Feiertagszeitplan konfiguriert haben, klicken Sie auf **OK** und dann auf **Speichern**.

## Mithilfe von Exchange Online PowerShell an einem Feiertag Zeitplan für eine automatische um-Telefonzentrale

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert **MyUMAutoAttendant** Geschäftszeiten so konfiguriert, dass 10:45 bis 13:15 (Sonntag), werden dessen 09:00 Uhr bis 17:00 (Montag), und 09:00 bis 16:30 (Samstag), und wie oft Feiertag und ihre zugeordneten Ansage so konfiguriert, dass Sie auf "Neue Jahr" werden 2 Januar 2013 und "Erstellen von geschlossen zur Bearbeitung" aus dem 24 April 2013 über 28 April 2013.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.13:15,1.09:00-1.17:00,6.09:00-6.16:30 -HolidaySchedule "New Year,newyrgrt.wav,1/2/2013","Building Closed for Construction,construction.wav,4/24/2013,4/28/2013"
```

# Geben Sie einen Namen für die business

18.12.2018 • 3 minutes to read

Sie können für eine automatische UM-Telefonzentrale in das Feld **Firmenname** den Namen Ihres Unternehmens eingeben. Standardmäßig ist kein Firmenname eingegeben. Wenn Sie einen Firmennamen eingeben, wird Anrufer, die die automatische UM-Telefonzentrale anrufen, die standardmäßige Begrüßungsansage mit dem Firmennamen wiedergegeben.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf automatische UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren eines Firmennamens mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie einen Namen für die Business festlegen möchten, und klicken Sie auf der Symbolleiste auf **Bearbeiten** .
3. Geben Sie auf der Seite **Automatische UM-Telefonzentrale > Allgemein** unter **Firmenname** den Namen des Unternehmens ein.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell zum Konfigurieren der

## Name eines Unternehmens

In diesem Beispiel wird der Name des Business auf einer automatischen um-Telefonzentrale mit dem Namen

```
MyUMAutoAttendant .
```

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessName "Northwind Traders"
```

# Business Speicherort festlegen

18.12.2018 • 2 minutes to read

Sie können den Standort eines Unternehmens in einer automatischen UM-Telefonzentrale (Unified Messaging) angeben, sodass dieser den Anrufern wiedergegeben wird. Standardmäßig ist kein Unternehmensstandort eingegeben.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren eines Unternehmensstandorts mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für den Speicherort des Business festgelegt werden soll, und klicken Sie dann auf **Bearbeiten**
3. Geben Sie auf der Seite **Automatische UM-Telefonzentrale > Allgemein**, unter **Unternehmensstandort** den Standort des Unternehmens ein.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell Konfigurieren eines Business-Speicherorts

In diesem Beispiel wird die Unternehmensstandort auf einer automatischen um-Telefonzentrale mit dem Namen MyUMAutoAttendant .

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessLocation 'Redmond'
```

# Konfigurieren der Zeitzone

18.12.2018 • 3 minutes to read

Standardmäßig verwendet die automatische Unified Messaging-Telefonzentrale (UM) die Zeitzone des Postfachservers, auf dem sie erstellt wurde. Es gibt jedoch Situationen, in denen die Zeitzone für die automatische UM-Telefonzentrale in eine andere Zeitzone geändert werden muss. Wenn Sie beispielsweise über zwei UM-Wählpläne verfügen und jeder Wählplan für eine andere Zeitzone steht, müssen Sie eine automatische UM-Telefonzentrale so konfigurieren, dass sie die gleiche Zeitzone wie der Postfachserver aufweist. Die andere automatische UM-Telefonzentrale muss eine vom Postfachserver abweichende Zeitzone haben.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

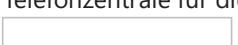
- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der Zeitzone mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  

2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie die Zeitzone festlegen möchten, und klicken Sie dann auf **Bearbeiten**  

3. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale** auf **Geschäftszeiten**, und wählen Sie dann unter **Zeitzone** die Zeitzone aus der Dropdownliste aus.
4. Klicken Sie zum Speichern Ihrer Änderungen auf **OK** und dann auf **Speichern**.

Verwenden von Exchange Online PowerShell so konfigurieren Sie die

## Zeitzone

In diesem Beispiel wird die Zeitzone Pacific Standard Time-Zone auf einem UM-Telefonzentrale mit dem Namen

MyUMAutoAttendant .

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -TimeZoneName Pacific
```

# Aktivieren Sie eine benutzerdefinierte Begrüßung während der Geschäftszeiten

18.12.2018 • 5 minutes to read

Sie können für eine automatische UM-Telefonzentrale eine benutzerdefinierte Begrüßung während der Geschäftszeit aktivieren. Wenn eine automatische UM-Telefonzentrale während der Geschäftszeit einen Anruf beantwortet, hört der Anrufer als Erstes die Begrüßung. Sie können die Begrüßung nach Wunsch anpassen.

Unified Messaging umfasst eine Standardsystemansage, die während der Geschäftszeiten verwendet wird. Sie müssen diese Standardsystemansage zwar weder ersetzen noch ändern, dennoch möchten Sie möglicherweise eine angepasste Begrüßung bereitstellen. Sie können eine benutzerdefinierte Ansage im WAV- oder WMA-Dateiformat erstellen, die verwendet wird, wenn Anrufer während der Geschäftszeiten bei einer automatischen UM-Telefonzentrale anrufen. Beispiel: "Danke für Ihren Anruf bei der Woodgrove Bank."

Wenn Sie den Namen der Organisation oder des Unternehmens in die Standardansage aufnehmen möchten, können Sie den Namen in das Feld **Firmenname** der automatischen UM-Telefonzentrale eingeben. Weitere Informationen finden Sie unter [Geben Sie einen Namen für die business](#).

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Erstellen Sie eine WAV- oder WMA-Datei, die für die Begrüßung verwendet werden soll.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren einer angepassten Begrüßung während der Geschäftszeit mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie eine angepasste Business Begrüßung außerhalb aktivieren möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale > Begrüßungen** unter **Begrüßung während der Geschäftszeit** auf **Ändern**, und klicken Sie dann auf **Durchsuchen**, um die benutzerdefinierte Datei mit der Begrüßung während der Geschäftszeit zu bestimmen, die Sie vor Beginn dieses Schritts erstellt haben.

**IMPORTANT**

Die Datei, die für die Begrüßung verwendet werden soll, muss eine WAV- oder WMA-Datei sein.

4. Nachdem Sie die Datei bestimmt haben, klicken Sie auf **Öffnen** und anschließend auf **Speichern**.

## Verwenden Sie Exchange Online PowerShell, um eine benutzerdefinierte Begrüßung während der Geschäftszeit aktivieren

Dieses Beispiel aktiviert die Begrüßung während der Geschäftszeiten, die eine benutzerdefinierte Begrüßung mit dem Namen verwendet `GreetingFile.wav` für die automatische Telefonzentrale `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursWelcomeGreetingEnabled $true -  
BusinessHoursWelcomeGreetingFilename GreetingFile.wav
```

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert `MyUMAutoAttendant` so konfiguriert, dass 10:45 bis 13:15 (Sonntag), werden von Geschäftszeiten haben 09:00 Uhr bis 17:00 (Montag), und 09:00 bis 16:30 (Samstag) und Feiertag Zeiten und ihre zugehörigen Ansage konfiguriert ist " `New Year`" auf 2 Januar 2013 und " `Building Closed for Construction`" aus dem 24 April 2013 über 28 April 2013.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.13:15,1.09:00-  
1.17:00,6.09:00-6.16:30 -HolidaySchedule "New Year,newyrgrt.wav,1/2/2013","Building Closed for  
Construction,construction.wav,4/24/2013,4/28/2013"
```

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert `MyAutoAttendant` und Geschäftszeiten werden tastenzuordnungen ermöglicht, sodass Anrufer 1 drücken, um eine andere UM-Telefonzentrale mit dem Namen weitergeleitet sind `SalesAutoAttendant`. Wenn sie 2 drücken, sind sie an die Durchwahlnummer 12345 für weitergeleitet `Support`, und wenn sie 3 drücken, sind sie an eine andere automatische Telefonzentrale, die eine Audiodatei abgespielt wird gesendet.

```
Set-UMAutoAttendant -Identity MyAutoAttendant - BusinessHoursKeyMappingEnabled $true -BusinessHoursKeyMapping  
"1,Sales,,SalesAutoAttendant","2,Support,12345","3,Directions,,,directions.wav"
```

# Aktivieren Sie eine benutzerdefinierte Geschäftszeiten Menü Aufforderung

18.12.2018 • 6 minutes to read

Sie können die Menüansage anpassen, die von einer automatischen Unified Messaging-Telefonzentrale (UM) während der Geschäftszeit verwendet werden soll. Nachdem Sie eine automatische UM-Telefonzentrale erstellt haben, wird eine Systemansage ("Willkommen bei Unified Messaging") als Menüansage verwendet, die Anrufer hören, nachdem die Begrüßung mit den Geschäftszeiten wiedergegeben wurde. Auch wenn Systemansagen nicht ersetzt oder geändert werden dürfen, können Sie die Begrüßungen und Menüansagen anpassen, die mit automatischen UM-Telefonzentralen verwendet werden. Nachdem Sie eine angepasste Audiodatei für die Menüansage für die Geschäftszeiten erstellt haben, müssen Sie für die automatische UM-Telefonzentrale Menünavigationseinträge für die Geschäftszeiten aktivieren.

Wenn Sie lediglich den Namen Ihrer Organisation oder Firma in die standardmäßige Systemansage aufnehmen möchten, können Sie den Namen im Feld **Firmenname** der automatischen UM-Telefonzentrale eingeben. Weitere Informationen finden Sie unter [Geben Sie einen Namen für die business](#).

## IMPORTANT

Sie müssen die Geschäftszeiten in der automatischen Telefonzentrale konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren von Geschäftszeiten](#).

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Erstellen Sie eine WAV- oder WMA-Datei, die als Menüansage verwendet werden soll.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Aktivieren einer angepassten Menüansage während der Geschäftszeit mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  

2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie eine benutzerdefinierte Geschäftszeiten Menü Aufforderung aktivieren möchten, und klicken Sie dann auf **Bearbeiten**  

3. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale > Menünavigation** unter **Menünavigation während der Geschäftszeit** auf **Ändern**, und klicken Sie dann auf **Durchsuchen**, um die angepasste Datei mit der Menüansage während der Geschäftszeit zu bestimmen.

## IMPORTANT

Die Datei, die für die Menüansage verwendet werden soll, muss eine WAV- oder WMA-Datei sein.

4. Nachdem Sie die Datei bestimmt haben, klicken Sie auf **Öffnen** und anschließend auf **Speichern**.

## Verwenden Sie Exchange Online PowerShell, um eine benutzerdefinierte Geschäftszeiten Menü Aufforderung zu aktivieren

In diesem Beispiel wird eine Geschäftszeiten hauptmenüansage aktiviert und verwendet eine benutzerdefinierte Aufforderung `businesshoursprompts.wav` auf die automatische Telefonzentrale `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursMainMenuCustomPromptEnabled $true -BusinessHoursMainMenuCustomPromptFilename BusinessHoursPrompts.wav
```

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert `MyUMAutoAttendant` Geschäftszeiten so konfiguriert, dass 10:45 bis 13:15 (Sonntag), werden dessen 09:00 Uhr bis 17:00 (Montag), und 09:00 bis 16:30 (Samstag) und Feiertag Zeiten und ihre zugehörigen Ansage konfiguriert ist " `New Year` " auf 2 Januar 2013 und " `Building Closed for Construction` " aus dem 24 April 2013 über 28 April 2013.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.13:15,1.09:00-1.17:00,6.09:00-6.16:30 -HolidaySchedule "New Year,newyrgrt.wav,1/2/2013","Building Closed for Construction,construction.wav,4/24/2013,4/28/2013"
```

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert `MyAutoAttendant` und Geschäftszeiten Navigationsmenüs ermöglicht, sodass Anrufer 1 drücken, um eine andere UM-Telefonzentrale mit dem Namen weitergeleitet sind `SalesAutoAttendant`. Wenn sie 2 drücken, sind sie an die Durchwahlnummer 12345 für weitergeleitet `Support`, und wenn sie 3 drücken, sind sie an eine andere automatische Telefonzentrale, die eine Audiodatei abgespielt wird gesendet.

```
Set-UMAutoAttendant -Identity MyAutoAttendant - BusinessHoursKeyMappingEnabled $true -BusinessHoursKeyMapping "1,Sales,,SalesAutoAttendant","2,Support,12345","3,Directions,,,directions.wav"
```

# Aktivieren Sie eine benutzerdefinierte Geschäftszeiten Begrüßung

18.12.2018 • 6 minutes to read

Sie können für eine automatische Unified Messaging-Telefonzentrale (Unified Messaging) eine benutzerdefinierte Begrüßung außerhalb der Geschäftszeit aktivieren. Wenn eine automatische UM-Telefonzentrale außerhalb der Geschäftszeit einen Anruf beantwortet, hört der Anrufer als Erstes die Begrüßung. Sie können die Begrüßung nach Wunsch anpassen.

Unified Messaging bietet eine Standardsystemansage zur Verwendung außerhalb der Geschäftszeit. Sie müssen diese Standardsystemansage zwar weder ersetzen noch ändern, dennoch möchten Sie möglicherweise eine angepasste Begrüßung bereitstellen. Sie können eine benutzerdefinierte Ansage im WAV- oder WMA-Dateiformat erstellen, die verwendet wird, wenn Anrufer außerhalb der Geschäftszeiten bei einer automatischen UM-Telefonzentrale anrufen. Diese kann beispielsweise wie folgt lauten: "Hallo, hier ist die Woodgrove Bank. Leider rufen Sie außerhalb unserer Geschäftszeiten an."

Wenn Sie den Namen der Organisation oder des Unternehmens in die Standardansage aufnehmen möchten, können Sie den Namen in das Feld **Firmenname** der automatischen UM-Telefonzentrale eingeben. Weitere Informationen finden Sie unter [Geben Sie einen Namen für die business](#).

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Erstellen Sie eine WAV- oder WMA-Datei, die für die Begrüßung verwendet werden soll.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

**Aktivieren einer angepassten Begrüßung außerhalb der Geschäftszeit mithilfe der Exchange-Verwaltungskonsole**

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  

- Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie eine benutzerdefinierte Geschäftszeiten Begrüßung aktivieren möchten, und klicken Sie dann auf **Bearbeiten**  

- Klicken Sie auf der Seite **Automatische UM-Telefonzentrale > Begrüßungen** unter **Begrüßung außerhalb der Geschäftszeit** auf **Ändern**, und klicken Sie dann auf **Durchsuchen**, um die benutzerdefinierte Datei mit der Begrüßung außerhalb der Geschäftszeit zu bestimmen, die Sie vor Beginn dieses Schritts erstellt haben.

**IMPORTANT**

Die Datei, die für die Begrüßung verwendet werden soll, muss eine WAV- oder WMA-Datei sein.

- Nachdem Sie die Datei bestimmt haben, klicken Sie auf **Öffnen** und anschließend auf **Speichern**.

## Verwenden Sie Exchange Online PowerShell, um eine benutzerdefinierte Geschäftszeiten Begrüßung aktivieren

Dieses Beispiel aktiviert die außerhalb der Geschäftszeiten Ansage, die eine benutzerdefinierte Begrüßung mit dem Namen verwendet `GreetingFile.wav` für die automatische Telefonzentrale `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AfterHoursWelcomeGreetingEnabled $true -  
AfterHoursWelcomeGreetingFilename GreetingFile.wav
```

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert `MyUMAutoAttendant` Geschäftszeiten so konfiguriert, dass 10:45 bis 13:15 (Sonntag), werden dessen 09:00 Uhr bis 17:00 (Montag), und 09:00 bis 16:30 (Samstag) und Feiertag Zeiten und ihre zugehörigen Ansage konfiguriert ist " `New Year`" auf 2 Januar 2013 und " `Building Closed for Construction`" aus dem 24 April 2013 über 28 April 2013.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.13:15,1.09:00-  
1.17:00,6.09:00-6.16:30 -HolidaySchedule "New Year,newyrgrt.wav,1/2/2013","Building Closed for  
Construction,construction.wav,4/24/2013,4/28/2013"
```

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert `MyAutoAttendant` und außerhalb der Geschäftszeiten werden Tastenzuordnungen ermöglicht, sodass Anrufer 1 drücken, um eine andere UM-Telefonzentrale mit dem Namen weitergeleitet sind `SalesAutoAttendant`. Wenn sie 2 drücken, sind sie an die Durchwahlnummer 12345 für weitergeleitet `Support`, und wenn sie 3 drücken, sind sie an eine andere automatische Telefonzentrale, die eine Audiodatei abgespielt wird gesendet.

```
Set-UMAutoAttendant -Identity MyAutoAttendant - BusinessHoursKeyMappingEnabled $true -BusinessHoursKeyMapping  
"1,Sales,,SalesAutoAttendant","2,Support,12345","3,Directions,,,directions.wav"
```

# Aktivieren einer benutzerdefinierten Menüansage außerhalb der Geschäftszeiten

18.12.2018 • 5 minutes to read

Sie können die Menüansage anpassen, die von der automatischen UM-Telefonzentrale (Unified Messaging) außerhalb der Geschäftszeiten verwendet werden soll. Nach der Erstellung einer automatischen UM-Telefonzentrale wird eine standardmäßige Systemansage ("Willkommen bei Unified Messaging") als Menüansage verwendet, die Anrufer hören, nachdem die Begrüßung für Zeiten außerhalb der Geschäftszeiten wiedergegeben wurde. Auch wenn Systemansagen nicht ersetzt oder geändert werden dürfen, können Sie die Begrüßungen und Menüansagen anpassen, die für automatische UM-Telefonzentralen verwendet werden. Nachdem Sie eine Audiodatei für Menüansagen außerhalb der Geschäftszeiten erstellt haben, müssen Sie die Menünavigationseinträge der automatischen UM-Telefonzentrale für Zeiten außerhalb der Geschäftszeiten aktivieren.

Wenn Sie lediglich den Namen Ihrer Organisation oder Firma in die standardmäßige Systemansage aufnehmen möchten, können Sie den Namen im Feld **Firmenname** der automatischen UM-Telefonzentrale eingeben. Weitere Informationen finden Sie unter [Geben Sie einen Namen für die business](#).

## IMPORTANT

Sie müssen die Geschäftszeiten für die automatische Telefonzentrale konfigurieren. Beim Konfigurieren von Geschäftszeiten werden die Zeiten außerhalb der Geschäftszeiten automatisch festgelegt. Weitere Informationen finden Sie unter [Konfigurieren von Geschäftszeiten](#).

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Erstellen Sie eine WAV- oder WMA-Datei, die als Menüansage verwendet werden soll.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren einer angepassten Menüansage für Zeiten außerhalb der Geschäftszeiten mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie eine benutzerdefinierte Geschäftszeiten Menü Aufforderung aktivieren möchten, und klicken Sie dann auf **Bearbeiten**
3. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale > Menünavigation** unter **Menünavigation außerhalb der Geschäftszeiten** auf **Ändern**. Klicken Sie dann auf **Durchsuchen**, um nach der Datei mit der angepassten Menüansage für Zeiten außerhalb der Geschäftszeiten zu suchen.

### IMPORTANT

Bei der Datei, die Sie für die Menüansage verwenden, muss es sich um eine WAV- oder WMA-Datei handeln.

4. Nachdem Sie die Datei bestimmt haben, klicken Sie auf **Öffnen** und anschließend auf **Speichern**.

## Verwenden Sie Exchange Online PowerShell, um eine benutzerdefinierte Geschäftszeiten Menü Aufforderung zu aktivieren

Dieses Beispiel aktiviert die eine automatischen um-Telefonzentrale mit dem Namen **MyUMAutoAttendant** Geschäftszeiten so konfiguriert, dass 10:45 bis 13:15 (Sonntag), werden dessen 09:00 Uhr bis 17:00 (Montag), und 09:00 bis 16:30 (Samstag) und Feiertag Zeiten und ihre zugehörigen Ansage konfiguriert ist " **New Year** " Januar 1, 2013, und " **Building Closed for Construction** " aus dem 24 April 2013 über 28 April 2013.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.13:15,1.09:00-1.17:00,6.09:00-6.16:30 -HolidaySchedule "New Year,newyrgrt.wav,1/2/2013","Building Closed for Construction,construction.wav,4/24/2013,4/28/2013"
```

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert **MyAutoAttendant** und außerhalb der Geschäftszeiten Navigationsmenüs ermöglicht, sodass Anrufer 1 drücken, um eine andere UM-Telefonzentrale mit dem Namen weitergeleitet sind **SalesAutoAttendant**. Wenn sie 2 drücken, sind sie an die Durchwahlnummer 12345 für weitergeleitet **Support**, und wenn sie 3 drücken, sind sie an einer anderen UM-Telefonzentrale, die eine Audiodatei abgespielt wird gesendet.

```
Set-UMAutoAttendant -Identity MyAutoAttendant -AfterHoursKeyMappingEnabled $true -AfterHoursKeyMapping "1,Sales,,SalesAutoAttendant","2,Support,12345","3,Directions,,,directions.wav"
```

# Aktivieren einer Informationsansage

18.12.2018 • 3 minutes to read

Sie können eine Informationsansage für eine automatische Unified Messaging-Telefonzentrale (UM) aktivieren. Wenn eine Informationsansage aktiviert wird, erfolgt die Wiedergabe unmittelbar nach der Begrüßung während oder außerhalb der Geschäftszeiten. Standardmäßig ist keine Informationsansage konfiguriert. Wenn Sie eine Informationsansage aktivieren möchten, erstellen Sie eine WAV- oder WMA-Datei, die als Informationsansage verwendet werden soll. Konfigurieren Sie die automatische Telefonzentrale dann für die Verwendung dieser Audiodatei.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Erstellen Sie eine WAV- oder WMA-Datei, die als Informationsansage verwendet werden soll.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren einer Informationsansage mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie eine Informationsansage aktivieren möchten, und klicken Sie dann auf **Bearbeiten**
3. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale > Begrüßungen** unter **Informationsansage** auf **Ändern** und dann auf **Durchsuchen**, um die Datei mit der Informationsansage zu suchen, die Sie vor der Ausführung dieses Verfahrens erstellt haben.

**IMPORTANT**

Bei der Datei, die Sie für die Begrüßung verwenden, muss es sich um eine WAV- oder WMA-Datei handeln.

4. Nachdem Sie die Datei bestimmt haben, klicken Sie auf **Öffnen** und anschließend auf **Speichern**.

## Verwenden von Exchange Online PowerShell, eine Informationsansage aktivieren

In diesem Beispiel wird eine Informationsansage an, die verwendet ermöglicht die `MyInfoAnnouncement.wav` -Datei für die automatische Telefonzentrale mit dem Namen `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -InfoAnnouncementEnabled $true -InfoAnnouncementFilename  
MyInfoAnnouncement.wav
```

# Erstellen einer Menünavigation

18.12.2018 • 11 minutes to read

Können Sie der Seite **neue menünavigationseintrags** zum Erstellen von einzelnen oder mehreren tastenzuordnungen Business oder Hauptmenü außerhalb der Geschäftszeiten für automatische Telefonzentralen aufgefordert wird. Sie können die Aktion definieren, die ausgeführt wird, wenn eine Taste auf der Telefontastatur den Aufruf von einer Durchwahlnummer oder eine andere automatische Telefonzentrale übertragen gedrückt wird, beispielsweise.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## UM automatische Telefonzentrale Navigationsmenüs konfigurieren mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen** **UM-Telefonzentrale für die Sie Menünavigation erstellen möchten**. Klicken Sie auf der Symbolleiste auf **Bearbeiten**
3. Auf der Seite **UM-Telefonzentrale** klicken Sie auf **Menünavigation**, wählen Sie **aktivieren die Menünavigation Geschäftszeiten** oder **Aktivieren der Menünavigation außerhalb der Geschäftszeiten** aus, und klicken Sie dann auf **Hinzufügen**
4. Konfigurieren Sie auf der Seite **neue menünavigationseintrags** Folgendes ein:
  - **Auffordern:** Verwenden Sie dieses Feld den Namen der im Navigationsmenü neu eingeben. Der Name des

Navigation wird nur für die Anzeige verwendet. Dies ist ein erforderliches Feld.

Da Sie möglicherweise mehrere neue Navigationsmenüs festlegen möchten, sollten Sie für die Tastenzuordnungen aussagekräftige Namen verwenden. Die maximale Länge des Namens für eine Tastenzuordnung beträgt 64 Zeichen inklusive Leerzeichen. Die folgenden Zeichen dürfen jedoch nicht enthalten sein: "/\[]:;|=,+\*?<>".

- **Wenn diese Taste gedrückt wird:** mit dieser Liste können tastenzuordnung aktivieren. Die tastaturzuordnung ist die Taste, die ein Anrufer drückt der automatischen Telefonzentrale einen bestimmten Vorgang ausführen Weiterleiten des Anrufers an eine andere automatische Telefonzentrale oder an einen Operator. Standardmäßig sind keine Einträge definiert.

Verwenden Sie die Dropdown-Liste, um den numerischen Schlüssel (von 1 bis 9) auswählen, den der Anrufer drücken muss. Null (0) ist für die automatische Telefonzentrale-Operator reserviert.

Wenn Sie in der Dropdownliste die Option **Timeout** auswählen, können Anrufer an eine Durchwahlnummer oder eine andere automatische Telefonzentrale weitergeleitet werden, vorausgesetzt, sie drücken keine Taste auf der Wähltafel des Telefons. Zum Beispiel "Bitte legen Sie nicht auf. Ihr Anruf wird vom nächsten freien Mitarbeiter entgegengenommen." Die Standardeinstellung ist 5 Sekunden. Wenn Sie diese Option aktivieren, wird eine leere Tastenzuordnung erstellt.

- **Die folgende Audiodatei wiedergeben:** Verwenden Sie diese Option, um eine zuvor aufgezeichnete Audiodatei für Anrufer auszuwählen. Klicken Sie auf **Ändern**, und klicken Sie dann auf **Durchsuchen**, um die Audiodatei zu suchen.
- **Diese zusätzliche Aktion ausführen:** Wählen Sie eine der folgenden Optionen, um die Aktion definieren, die Sie die automatische Telefonzentrale für den Anrufer durchführen möchten:
- **None:** Wenn Sie nicht an die automatische Telefonzentrale Weiterleiten des Anrufs an eine Erweiterung oder an eine andere automatische Telefonzentrale oder für einen Benutzer eine Nachricht hinterlassen möchten, verwenden Sie diese Option.
- **Weiterleiten an diese Durchwahl:** Wählen Sie diese Option, um Anrufe in einer Durchwahlnummer übertragen werden können. Wenn Sie diese Option aktivieren, verwenden Sie das Feld die Erweiterung, in dem der Anruf weitergeleitet werden. In diesem Feld können nur numerische Zeichen. Es kann keine der folgenden Zeichen enthalten: "/\[]:;|=,+\*?<>".
- **Weiterleiten an diese automatische um-Telefonzentrale:** Wählen Sie diese Option, um den Anruf an eine automatische Telefonzentrale weiterleiten aus. Klicken Sie auf **Durchsuchen**, um die automatische Telefonzentrale zu suchen, die Sie verwenden möchten. Bevor Sie diese Option aktivieren, müssen Sie zuerst erstellen und konfigurieren die automatischen Telefonzentrale. Diese Option wird verwendet, wenn Sie eine hierarchische Struktur von automatischen UM-Telefonzentralen erstellen.
- **Eine Sprachnachricht hinterlassen für diesen Benutzer:** Wählen Sie diese Option, um ein Anrufer eine Nachricht für einen Benutzer hinterlassen, die auf dem selben Wählplan wie die automatische Telefonzentrale ist, die Sie konfigurieren können. Wenn ein Anrufer diese Option aus einem Auto attendant Menü auswählt, werden sie aufgefordert, eine Sprachnachricht für den Benutzer hinterlassen, die ausgewählt wurde. Klicken Sie auf **Durchsuchen**, um den UM-aktivierten Benutzer zu suchen.
- **Unternehmensstandort Announce:** Wählen Sie diese Option aktivieren Sie einen Anrufer wählen eine automatische Telefonzentrale Menüoption und zu hören den Speicherort des Unternehmens, die für die automatische Telefonzentrale konfiguriert ist. Hierzu ordnungsgemäß funktioniert müssen Sie zuerst den Unternehmensstandort im Feld **Business Speicherort** auf der Seite **Allgemein** auf die automatische Telefonzentrale eingeben.
- **Geschäftszeiten Announce:** Wählen Sie diese Option aktivieren Sie einen Anrufer wählen eine automatische Telefonzentrale Menüoption und zu hören die Betriebszeiten für das Unternehmen, der für die

automatische Telefonzentrale konfiguriert ist. Hierzu ordnungsgemäß funktioniert, müssen Sie zuerst die Geschäftszeiten auf der Seite **Geschäftszeiten** der automatischen UM-Telefonzentrale konfigurieren.

5. Klicken Sie auf **OK**, um die neue Menünavigation zu erstellen.
6. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale** auf **Speichern**, um die Änderungen zu speichern.

## Verwenden Sie Exchange Online PowerShell, UM Auto attendant tastenzuordnungen konfigurieren

Dieses Beispiel aktiviert die Geschäftszeiten den tastenzuordnungen, damit:

- Wenn Anrufer 1 drücken, werden sie an eine andere UM-Telefonzentrale mit dem Namen weitergeleitet **SalesAutoAttendant**.
- Wenn sie 2 drücken, werden diese Durchwahlnummer 12345 für den Support weitergeleitet werden.
- Wenn sie 3 drücken, werden sie an eine andere automatische Telefonzentrale gesendet werden, die eine Audiodatei wiedergegeben werden.

```
Set-UMAutoAttendant -Identity MyAutoAttendant -BusinessHoursKeyMappingEnabled $true -BusinessHoursKeyMapping "1,Sales,,SalesAutoAttendant","2,Support,12345","3,Directions,,,directions.wav"
```

Dieses Beispiel legt den tastenzuordnungen, die in einer durch Trennzeichen getrennten Werten (CSV)-Datei definiert. Sie müssen zuerst die CSV-Datei mit den folgenden Überschriften und der AutoKorrektur-Eintrag erstellen: <Schlüssel>, <Beschreibung>, [<Erweiterung>], [<Autoattendant Name>], [<Promptfilenamepath>], [<asrphrase1; asrphrase2>], [<Leavevoicemailfor>], [<Transfertomailbox>]. Die Werte in Klammern sind optional. Importieren Sie nach dem Erstellen der CSV-Datei, die CSV-Datei mithilfe des **Import-Csv** -Cmdlet.

```
$o = Import-csv -path "C:\UMFiles\AutoAttendants\keymappings.csv"  
Set-UMAutoAttendant MyAutoAttendant -BusinessHoursKeyMapping $o
```

In diesem Beispiel wird den tastenzuordnungen aus einer vorhandenen UM-Telefonzentrale in eine CSV-Datei exportiert und importiert dann die gleichen tastenzuordnungen in eine andere UM-Telefonzentrale. Sie konnte den tastenzuordnungen auch in eine CSV-Datei exportieren, bearbeiten oder ändern die Zuordnung für den Schlüssel in der CSV-Datei und dann diese tastenzuordnungen in einer anderen UM-Telefonzentrale zu importieren.

```
$aa = Get-UMAutoAttendant -Identity MyAutoAttendant  
$aa1 = Get-UMAutoAttendant -Identity MyAutoAttendant2  
$aa.BusinessHoursKeyMapping | Export-csv -path "C:\UMFiles\AutoAttendants\keymappings.csv"  
$aa1.BusinessHoursKeyMapping = (Import-csv -path "C:\UMFiles\AutoAttendants\keymappings.csv")
```

# Erstellen von Geschäftszeiten Navigationsmenüs

18.12.2018 • 11 minutes to read

Für eine automatische UM-Telefonzentrale (Unified Messaging) können Sie Tastenzuordnungen für Geschäftszeiten aktivieren. Nachdem Sie eine automatische UM-Telefonzentrale erstellt haben, wird für Anrufer eine Standardsystemansage als Begrüßungsansage für das Hauptmenü während der Geschäftszeiten wiedergegeben, nachdem die Begrüßung während der Geschäftszeiten wiedergegeben wurde. Die standardmäßige Hauptmenüansage während der Geschäftszeiten lautet "Willkommen bei der automatischen Telefonzentrale von Microsoft Exchange." Da standardmäßig keine Tastenzuordnungen definiert sind, stehen den Anrufern keine Menüoptionen zur Verfügung, und sie hören nur die standardmäßige Hauptmenüansage.

Beim Konfigurieren von Tastenzuordnungen definieren Sie die Optionen und Vorgänge, die durchgeführt werden, wenn ein Anrufer bei Verwendung einer sprachaktivierten automatischen Telefonzentrale ein bestimmtes Wort sagt oder bei Verwendung einer nicht sprachaktivierten automatischen Telefonzentrale eine Taste auf der Telefontastatur drückt.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren von Tastenzuordnungen für Geschäftszeiten für eine automatische UM-Telefonzentrale mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen** UM-Telefonzentrale ein Navigationsmenü Geschäftszeiten erstellt werden soll. Klicken Sie auf der Symbolleiste

auf **Bearbeiten**

3. Klicken Sie auf der Seite **UM-Telefonzentrale Menünavigation** unter **Geschäftszeiten Menünavigation**, wählen Sie **aktivieren die Menünavigation Geschäftszeiten** und klicken Sie dann auf **Hinzufügen**
4. Verwenden Sie auf der Seite **Neuer Menünavigationseintrag** die folgenden Optionen, um einen neuen Navigationseintrag zu erstellen:
  - **Auffordern:** Verwenden Sie dieses Feld den Namen der im Navigationsmenü neu eingeben. Der Name des Navigation wird nur für die Anzeige verwendet. Dies ist ein erforderliches Feld.

Da Sie möglicherweise mehrere neue Navigationsmenüs festlegen möchten, sollten Sie für die Tastenzuordnungen aussagekräftige Namen verwenden. Die maximale Länge des Namens für eine Tastenzuordnung beträgt 64 Zeichen inklusive Leerzeichen. Die folgenden Zeichen dürfen jedoch nicht enthalten sein: "/\[]:;|=,+\*?<>.
  - **Wenn diese Taste gedrückt wird:** mit dieser Liste können tastenzuordnung aktivieren. Die tastaturzuordnung ist die Taste, die ein Anrufer drückt der automatischen Telefonzentrale einen bestimmten Vorgang ausführen Weiterleiten des Anrufers an eine andere automatische Telefonzentrale oder an einen Operator. Standardmäßig sind keine Einträge definiert.

Verwenden Sie die Dropdownliste, um die Zifferntaste (1 bis 9) auszuwählen, die der Anrufer drücken muss. Null (0) ist für die Vermittlungsstelle der automatischen Telefonzentrale reserviert.

Wenn Sie in der Dropdownliste die Option **Timeout** auswählen, können Anrufer an eine Durchwahlnummer oder eine andere automatische Telefonzentrale weitergeleitet werden, vorausgesetzt, sie drücken keine Taste auf der Wählertastatur des Telefons. Zum Beispiel "Bitte legen Sie nicht auf. Ihr Anruf wird vom nächsten freien Mitarbeiter entgegengenommen." Die Standardeinstellung ist 5 Sekunden. Wenn Sie diese Option aktivieren, wird eine leere Tastenzuordnung erstellt.
  - **Die folgende Audiodatei wiedergeben:** Verwenden Sie diese Option, um eine zuvor aufgezeichnete Audiodatei für Anrufer auszuwählen. Klicken Sie auf **Ändern**, und klicken Sie dann auf **Durchsuchen**, um die Audiodatei zu suchen. Wenn Sie die Audiodatei unverändert lassen <keine>, das Modul Unified Messaging TTS (Text-zu-Sprache) wird ein Geschäftszeiten hauptmenüusage synthetisieren. Alternativ können Sie erstellen eine benutzerdefinierte Audiodatei, die für das Hauptmenü Geschäftszeiten verwendet werden kann Prompt für eine Sprachaktivierte automatische Telefonzentrale. Beispielsweise kann es sagen Sie "zu einer Sprachnachricht hinterlassen für den Vertrieb, sagen Sie 1., Sagen Sie 2, um eine Sprachnachricht für den technischen Support zu lassen. Um eine Sprachnachricht für die Administration lassen möchten, sagen Sie 3."
  - **Diese zusätzliche Aktion ausführen:** Wählen Sie eine der folgenden Optionen, um die Aktion definieren, die Sie die automatische Telefonzentrale für den Anrufer durchführen möchten:
  - **None:** Verwenden Sie diese Option, wenn Sie nicht möchten, dass die automatische Telefonzentrale Weiterleiten des Anrufs an eine Erweiterung oder an eine andere automatische Telefonzentrale oder für einen Benutzer eine Nachricht hinterlassen.
  - **Weiterleiten an diese Durchwahl:** Wählen Sie diese Option, um Anrufe in einer Durchwahlnummer übertragen werden können. Wenn Sie diese Option aktivieren, verwenden Sie das Feld die Durchwahlnummer eingeben, in dem der Anruf weitergeleitet werden. In diesem Feld können nur numerische Zeichen. Es kann keine der folgenden Zeichen enthalten: "/\[]:;|=,+\*?<>.
  - **Weiterleiten an diese automatische um-Telefonzentrale:** Wählen Sie diese Option, um den Anruf an eine automatische Telefonzentrale weiterleiten aus. Klicken Sie auf **Durchsuchen**, um die automatische Telefonzentrale zu suchen, die Sie verwenden möchten. Bevor Sie diese Option aktivieren, müssen Sie zuerst erstellen und konfigurieren die automatischen Telefonzentrale. Diese Option wird verwendet, wenn

Sie eine hierarchische Struktur von automatischen UM-Telefonzentralen erstellen.

- **Eine Sprachnachricht hinterlassen für diesen Benutzer:** Wählen Sie diese Option, um ein Anrufer eine Nachricht für einen Benutzer hinterlassen, die auf dem selben Wählplan wie die automatische Telefonzentrale ist, die Sie konfigurieren können. Wenn ein Anrufer diese Option aus einem Auto attendant Menü auswählt, werden sie aufgefordert, eine Sprachnachricht für den Benutzer hinterlassen, die ausgewählt wurde. Klicken Sie auf **Durchsuchen**, um den UM-aktivierten Benutzer zu suchen.
- **Unternehmensstandort Announce:** Wählen Sie diese Option aktivieren Sie einen Anrufer wählen eine automatische Telefonzentrale Menüoption und zu hören den Speicherort des Unternehmens, die für die automatische Telefonzentrale konfiguriert ist. Hierzu ordnungsgemäß funktioniert müssen Sie zuerst den Unternehmensstandort im Feld **Business Speicherort** auf der Seite **Allgemein** auf die automatische Telefonzentrale eingeben.
- **Geschäftszeiten Announce:** Wählen Sie diese Option aktivieren Sie einen Anrufer wählen eine automatische Telefonzentrale Menüoption und zu hören die Betriebszeiten für das Unternehmen, der für die automatische Telefonzentrale konfiguriert ist. Hierzu ordnungsgemäß funktioniert, müssen Sie zuerst der Geschäftszeiten auf der Seite **Geschäftszeiten** der automatischen UM-Telefonzentrale konfigurieren.

5. Klicken Sie auf **OK**, um die neue Menünavigation zu erstellen.
6. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale** auf **Speichern**, um die Änderungen zu speichern.

Verwenden von Exchange Online PowerShell um Geschäftszeiten zu aktivieren, werden tastenzuordnungen auf einem um-WÄHLPLAN attendant automatisch

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert **MyAutoAttendant** und Geschäftszeiten werden tastenzuordnungen ermöglicht, sodass Anrufer 1 drücken, um eine andere UM-Telefonzentrale mit dem Namen weitergeleitet sind **SalesAutoAttendant**. Wenn sie 2 drücken, sie sind an weitergeleitet Durchwahlnummer 12345 für die Unterstützung, und wenn sie 3 drücken, sind sie an eine andere automatische Telefonzentrale, die eine Audiodatei abgespielt wird gesendet.

```
Set-UMAutoAttendant -Identity MyAutoAttendant - BusinessHoursKeyMappingEnabled $true -BusinessHoursKeyMapping "1,Sales,,SalesAutoAttendant","2,Support,12345","3,Directions,,,directions.wav"
```

# Erstellen von Navigationsmenüs für Nicht-Geschäftszeiten

18.12.2018 • 11 minutes to read

Sie können den tastenzuordnungen außerhalb der Geschäftszeiten für eine automatische Telefonzentrale von Unified Messaging (UM) aktivieren. Nach der Erstellung einer automatischen UM-Telefonzentrale wird eine standardmäßige System Aufforderung für die außerhalb der Geschäftszeiten verwendet werden, die Ansage, die Anrufer hören, nachdem die außerhalb der Geschäftszeiten Begrüßung Willkommen bei den hauptmenüansage wiedergegeben wird. Die standardmäßige außerhalb der Geschäftszeiten hauptmenüansage teilt, "Willkommen bei Microsoft Exchange nach Stunden attendant automatisch". Da standardmäßig keine tastenzuordnungen definiert sind, stehen keine Menüoptionen zu den Anrufern und sie nur das standardmäßige außerhalb der Geschäftszeiten Hauptmenü auffordern hören.

Beim Konfigurieren von Tastenzuordnungen definieren Sie die Optionen und Vorgänge, die durchgeführt werden, wenn ein Anrufer bei Verwendung einer sprachaktivierten automatischen Telefonzentrale ein bestimmtes Wort sagt oder bei Verwendung einer nicht sprachaktivierten automatischen Telefonzentrale eine Taste auf der Telefontastatur drückt.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren von Tastenzuordnungen für Nicht-Geschäftszeiten für eine automatische UM-Telefonzentrale mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen** UM-Telefonzentrale für die Sie außerhalb der Geschäftszeiten Navigationsmenü erstellen möchten. Klicken Sie auf der Symbolleiste auf **Bearbeiten**
3. Auf der Seite **UM-Telefonzentrale Menünavigation**, klicken Sie unter **Geschäftszeit Stunden Menünavigation** auf, wählen Sie **aktivieren die Menünavigation außerhalb der Geschäftszeiten**, und klicken Sie dann auf **Hinzufügen**
4. Verwenden Sie auf der Seite **Neuer Menünavigationseintrag** folgende Optionen, um einen neuen Menünavigationseintrag zu erstellen:
- **Auffordern:** Verwenden Sie dieses Feld den Namen der im Navigationsmenü neu eingeben. Der Name des Navigation wird nur für die Anzeige verwendet. Dies ist ein erforderliches Feld.

Da Sie möglicherweise mehrere neue Navigationsmenüs festlegen möchten, sollten Sie für die Tastenzuordnungen aussagekräftige Namen verwenden. Die maximale Länge des Namens für eine Tastenzuordnung beträgt 64 Zeichen inklusive Leerzeichen. Die folgenden Zeichen dürfen jedoch nicht enthalten sein: "/\[];|=,+\*?<>.
  - **Wenn diese Taste gedrückt wird:** mit dieser Liste können tastenzuordnung aktivieren. Die tastaturzuordnung ist die Taste, die ein Anrufer drückt der automatischen Telefonzentrale einen bestimmten Vorgang ausführen Weiterleiten des Anrufers an eine andere automatische Telefonzentrale oder an einen Operator. Standardmäßig sind keine Einträge definiert.

Verwenden Sie die Dropdownliste, um die Zifferntaste (1 bis 9) auszuwählen, die der Anrufer drücken muss. Null (0) ist für die Vermittlungsstelle der automatischen Telefonzentrale reserviert.

Wenn Sie in der Dropdownliste die Option **Timeout** auswählen, können Anrufer an eine Durchwahlnummer oder eine andere automatische Telefonzentrale weitergeleitet werden, vorausgesetzt, sie drücken keine Taste auf der Wähltastatur des Telefons. Zum Beispiel "Bitte legen Sie nicht auf. Ihr Anruf wird vom nächsten freien Mitarbeiter entgegengenommen." Die Standardeinstellung ist 5 Sekunden. Wenn Sie diese Option aktivieren, wird eine leere Tastenzuordnung erstellt.
  - **Die folgende Audiodatei wiedergeben:** Verwenden Sie diese Option, um eine zuvor aufgezeichnete Audiodatei für Anrufer auszuwählen. Klicken Sie auf **Ändern**, und klicken Sie dann auf **Durchsuchen**, um die Audiodatei zu suchen. Wenn Sie die Audiodatei unverändert lassen <keine>, das Modul Unified Messaging TTS (Text-zu-Sprache) wird ein hauptmenüansage außerhalb der Geschäftszeiten synthetisieren. Alternativ können Sie eine benutzerdefinierte Audiodatei erstellen, die für die außerhalb der Geschäftszeiten hauptmenüansage für eine Sprachaktivierte automatische Telefonzentrale verwendet werden kann, die, z. B. würde "Sie" Contoso "während der Geschäftszeiten erreicht haben. Um eine Sprachnachricht für den Verkauf lassen möchten, sagen Sie 1. Sagen Sie 2, um eine Sprachnachricht für den technischen Support zu lassen. Um eine Sprachnachricht für die Administration lassen möchten, sagen Sie 3. Zum Erreichen einer Geschäftszeiten Operator, drücken Sie 0 (null). "
  - **Diese zusätzliche Aktion ausführen:** Wählen Sie eine der folgenden Optionen, um die Aktion definieren, die Sie die automatische Telefonzentrale für den Anrufer durchführen möchten:
  - **None:** Verwenden Sie diese Option, wenn Sie nicht möchten, dass die automatische Telefonzentrale Weiterleiten des Anrufs an eine Erweiterung oder an eine andere automatische Telefonzentrale oder für einen Benutzer eine Nachricht hinterlassen.,
  - **Weiterleiten an diese Durchwahl:** Wählen Sie diese Option, um Anrufe in einer Durchwahlnummer übertragen werden können. Wenn Sie diese Option aktivieren, verwenden Sie das Feld die Durchwahlnummer eingeben, in dem der Anruf weitergeleitet werden. In diesem Feld können nur numerische Zeichen. Es kann keine der folgenden Zeichen enthalten: "/\[];|=,+\*?<>.

- **Weiterleiten an diese automatische um-Telefonzentrale:** Wählen Sie diese Option, um den Anruf an eine vorhandene automatische Telefonzentrale übertragen. Klicken Sie auf **Durchsuchen**, um die automatische Telefonzentrale zu suchen, die Sie verwenden möchten. Bevor Sie diese Option aktivieren, müssen Sie zuerst erstellen und konfigurieren die automatischen Telefonzentrale. Diese Option wird verwendet, wenn Sie eine hierarchische Struktur von automatischen UM-Telefonzentralen erstellen.
- **Eine Sprachnachricht hinterlassen für diesen Benutzer:** Wählen Sie diese Option, um ein Anrufer eine Nachricht für einen Benutzer hinterlassen, die auf dem selben Wählplan wie die automatische Telefonzentrale ist, die Sie konfigurieren können. Wenn ein Anrufer diese Option aus einem Auto attendant Menü auswählt, werden sie aufgefordert, eine Sprachnachricht für den Benutzer hinterlassen, die ausgewählt wurde. Klicken Sie auf **Durchsuchen**, um den UM-aktivierten Benutzer zu suchen.
- **Unternehmensstandort Announce:** Wählen Sie diese Option aktivieren Sie einen Anrufer wählen eine automatische Telefonzentrale Menüoption und zu hören den Speicherort des Unternehmens, die für die automatische Telefonzentrale konfiguriert ist. Hierzu ordnungsgemäß funktioniert müssen Sie zuerst den Unternehmensstandort im Feld **Business Speicherort** auf der Seite **Allgemein** auf die automatische Telefonzentrale eingeben.
- **Geschäftszeiten Announce:** Wählen Sie diese Option aktivieren Sie einen Anrufer wählen eine automatische Telefonzentrale Menüoption und zu hören die Betriebszeiten für das Unternehmen, der für die automatische Telefonzentrale konfiguriert ist. Hierzu ordnungsgemäß funktioniert, müssen Sie zuerst der Geschäftszeiten auf der Seite **Geschäftszeiten** der automatischen UM-Telefonzentrale konfigurieren.

5. Klicken Sie auf **OK**, um die neue Menünavigation zu erstellen.
6. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale** auf **Speichern**, um die Änderungen zu speichern.

## Verwenden von Exchange Online PowerShell, außerhalb der Geschäftszeiten wichtige Zuordnungen für eine automatische um-Telefonzentrale aktivieren

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert `MyAutoAttendant` und außerhalb der Geschäftszeiten werden tastenzuordnungen ermöglicht, sodass Wenn Anrufer sagen "Nach der Arbeitszeit" die Durchwahlnummer 12345 übermittelt werden wird, und wenn sie "Erfahren Sie, wie" sagen sie an die Durchwahlnummer weitergeleitet werden 23456.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AfterHoursKeyMappingEnabled $true -AfterHoursKeyMapping "AfterhoursOperator,12345","Directions,23456"
```

# Verwalten einer automatischen UM-Telefonzentrale

18.12.2018 • 58 minutes to read

Nach der Erstellung einer automatischen Unified Messaging-Telefonzentrale (UM) können Sie eine Reihe von Einstellungen anzeigen oder konfigurieren. Sie können beispielsweise der automatischen Telefonzentrale zugeordnete Durchwahlnummern hinzufügen, entfernen und ändern. Sie können außerdem die automatische Spracherkennung (Automatic Speech Recognition, ASR) für die automatische Telefonzentrale aktivieren oder deaktivieren und die Begrüßungen ändern, die innerhalb und außerhalb der Geschäftszeiten verwendet werden.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Anzeigen oder Konfigurieren von Eigenschaften einer automatischen UM-Telefonzentrale mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** 
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale, die Sie anzeigen oder konfigurieren möchten, und klicken Sie dann auf der Symbolleiste auf **Bearbeiten** 
3. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale** auf **Allgemein**, um schreibgeschützte Informationen zur automatischen UM-Telefonzentrale anzuzeigen und Verwaltungsaufgaben für eine automatische UM-Telefonzentrale auszuführen:
  - **UM-Wähleinstellungen:** Dieses Feld zeigt den UM-Wählplan die automatische Telefonzentrale

zugeordnet. Nachdem Sie eine automatische Telefonzentrale erstellt haben, kann die Wähleinstellungen die automatische Telefonzentrale zugeordnet geändert werden. Wenn Sie eine automatische Telefonzentrale mit einem anderen Wählplan zuordnen möchten, müssen Sie den Wählplan löschen und dann die automatische Telefonzentrale mit dem richtigen Wählplan zuordnen, nachdem Sie ihn neu erstellen.

- **Name:** Dieses Feld zeigt den Namen, das die automatische Telefonzentrale zugeordnet wurde, wenn es erstellt wurde. Dies ist der Name, der in der Exchange-Verwaltungskonsole angezeigt wird.
- **Status:** Dieses Feld zeigt, ob die automatische Telefonzentrale aktiviert oder deaktiviert ist. Aktivieren oder Deaktivieren der automatischen Telefonzentrale, schließen Sie die **Automatische um-Telefonzentralen** Seite und verwenden Sie die Symbolleiste unter **Automatische UM-Telefonzentralen** auf der Seite **UM-Wählplan**.
- **Zugriffsnummern:** Verwenden Sie dieses Feld eingeben einer Durchwahlnummer oder Zugriffsnummer, der Anrufer an die automatische Telefonzentrale führt. Standardmäßig werden keine Erweiterung oder Access Zahlen konfiguriert, wenn Sie eine automatische Telefonzentrale erstellen.

Die Anzahl von Ziffern der angegebenen Durchwahl- oder Zugriffsnummer muss mit der Anzahl von Ziffern für eine Durchwahlnummer übereinstimmen, die in den UM-Wähleinstellungen konfiguriert ist, die der automatischen UM-Telefonzentrale zugeordnet sind. Darüber hinaus können Sie diesem Feld eine SIP-Adresse (Session Initiation Protocol) hinzufügen. Eine SIP-Adresse wird von einigen IP-Nebenstellenanlagen, SIP-aktivierten Nebenstellenanlagen und Microsoft Office Communications Server 2007 R2 oder Microsoft Lync Server verwendet.

Sie können eine neue automatische Telefonzentrale erstellen, ohne eine Durchwahlnummer oder Zugriffsnummer aufzulisten. Hinzufügen einer Durchwahlnummer, geben Sie die Nummer in dieses Feld ein und klicken Sie dann auf **Hinzufügen**. Sie können eine automatische Telefonzentrale mehr als eine Anzahl zuordnen. Sie können auch bearbeiten oder entfernen eine vorhandenen Zugriffsnummer. Um eine vorhandene Rufnummer bearbeiten möchten, wählen Sie sie aus, und klicken Sie auf **Bearbeiten**. Um einer vorhandenen Durchwahlnummer aus der Liste entfernen möchten, wählen Sie sie aus, und klicken Sie auf **Entfernen**.

- **Legen Sie die automatische Telefonzentrale zum Reagieren auf Sprachbefehle:** Aktivieren Sie dieses Kontrollkästchen aktivieren Anrufer Alternativtext zu automatische Telefonzentrale aufgefordert werden, um das Menüsystem zu navigieren. In der Standardeinstellung Wenn eine automatische Telefonzentrale erstellt wird, ist es nicht sprachaktiviert.

Wenn Sie die automatische Telefonzentrale erstellen, jedoch nicht für Speech-aktivieren möchten, können Sie die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell Speech-es aktivieren, nachdem er erstellt wurde.

- **Verwenden Sie diese automatische Telefonzentrale beim Sprachbefehle nicht ordnungsgemäß funktionieren:** Klicken Sie auf **Durchsuchen**, um die automatische Telefonzentrale auszuwählen, die in die Groß-/Kleinschreibung zu verwenden, die Sprachbefehle nicht verwendet werden soll. Dies wird auch als eine DTMF-fallback-Telefonzentrale bezeichnet. Nur, wenn **die automatische Telefonzentrale zum Reagieren auf Sprachbefehle ordnungsgemäß funktionieren nicht Set** -Option ausgewählt ist, kann eine DTMF-fallback-Telefonzentrale verwendet werden. Sie müssen zuerst erstellen Sie eine automatische DTMF-fallback-Telefonzentrale, und klicken Sie dann auf **Durchsuchen**, um die entsprechenden DTMF-Telefonzentrale zu suchen.

Eine automatische DTMF-Fallback-Telefonzentrale wird verwendet, wenn die sprachaktivierte automatische UM-Telefonzentrale die Spracheingaben des Anrufers nicht erkennen kann. Bei Einsatz der automatischen DTMF-Telefonzentrale muss der Anrufer DTMF-Eingaben verwenden, um durch das Menüsystem zu navigieren, den Namen eines Benutzers zu buchstabieren oder eine benutzerdefinierte Menüansage zu verwenden. Ein Anrufer kann nicht mithilfe von Sprachbefehlen durch diese automatische Telefonzentrale navigieren.

Wenn Sie keine automatische DTMF-Fallback-Telefonzentrale konfigurieren, empfehlen wir die Angabe einer Durchwahlnummer für die Vermittlungsstelle in der automatischen Telefonzentrale. Wenn keine Durchwahlnummer für die Vermittlungsstelle konfiguriert wird und Benutzer eine sprachaktivierte automatische Telefonzentrale verwenden, das System die Spracheingaben aber nicht erkennt, können die Benutzer nicht durch das System navigieren und nicht an eine Vermittlungsstelle weitergeleitet werden.

Obwohl es nicht erforderlich ist, empfehlen wir, für die automatische DTMF-Fallback-Telefonzentrale dieselbe Konfiguration wie für die sprachaktivierte automatische Telefonzentrale zu verwenden. Die automatische DTMF-Fallback-Telefonzentrale darf nicht sprachaktiviert sein.

- **Sprache für automatisierte Sprachbenutzerschnittstelle:** mit dieser Liste können Sie die Sprache auswählen, die Anrufer hören, wenn sie die automatische Telefonzentrale erreichen. Die Standardsprache wird bestimmt, wenn Sie Microsoft Exchange installieren. Für lokale und hybride Bereitstellungen, wird standardmäßig Englisch (USA) verwendet, da die automatische Telefonzentrale die Einstellung für die Standardsprache für die UM-Wählplan verwendet wird. Um die anderen Optionen für die Abfragesprache verfügbar ist, müssen Sie die UM-Sprachpakete für Sprachen installieren, die Sie einschließen möchten. Weitere Informationen zum Installieren eines Sprachpaketes finden Sie unter [Installieren eines Unified Messaging-Sprachpaketes](#). UM in Office 365 ist nicht erforderlich, UM zusätzliche Language Packs zu installieren.

Obwohl eine andere Sprache ausgewählt werden kann als die, die in den der automatischen Telefonzentrale zugeordneten UM-Wähleinstellungen ausgewählt ist, empfehlen wir, dass die Spracheinstellungen in den Wähleinstellungen und in der automatischen Telefonzentrale übereinstimmen. Wenn die Spracheinstellungen nicht übereinstimmen und Anrufer eine in den Wähleinstellungen angegebene Durchwahlnummer anrufen, erhalten Sie Ansagen in einer Sprache. Wenn die Anrufer eine der automatischen Telefonzentrale zugeordnete Durchwahlnummer anrufen, werden Sie mit Ansagen in einer anderen Sprache begrüßt.

- **Firmenname:** in diesem Feld können Sie den Namen des Unternehmens eingeben. Standardmäßig wird kein Name eines Business eingegeben. Wenn Sie ein Firmenname in dieses Feld eingeben, wird eine Aufforderung mit den Namen des Unternehmens zu den Anrufern anstelle der Standard-Ansage wiedergegeben werden.

- **Unternehmensstandort:** in diesem Feld können Sie den Speicherort des Unternehmens eingeben. Standardmäßig wird keine Unternehmensstandort eingegeben. Wenn Sie den Speicherort des Unternehmens in dieses Feld eingeben, wird die Unternehmensstandort für Anrufer wiedergegeben werden.

4. Verwenden Sie die Einstellung **Begrüßungen** in der automatischen Telefonzentrale, um aufgezeichnete Begrüßungen zu verwalten. Sie können Standardbegrüßungen oder zuvor aufgezeichnete benutzerdefinierte Begrüßungen für Zeiten während und außerhalb der Geschäftszeit auswählen. Sie können Folgendes konfigurieren:

- **Geschäftszeiten Ansage:** Hierbei handelt es sich um die anfänglichen Ansage, die wiedergegeben wird, wenn ein Anrufer während der Geschäftszeiten Ihrer Organisation die automatische Telefonzentrale aufruft. In der Standardeinstellung Geschäftszeiten liegen 12:00 Uhr bis 12:00 Uhr und keine außerhalb der Geschäftszeiten werden festgelegt. Wenn Sie nicht, dass eine benutzerdefinierte angeben wird Begrüßung System aufgefordert, die besagt, "Willkommen bei der Exchange-Telefonzentrale" für Anrufer wiedergegeben. Das Unternehmen und außerhalb der Geschäftszeiten werden für die automatische Telefonzentrale **Geschäftszeiten** konfiguriert.

Sie können die Begrüßung anpassen und auf Ihre Organisation abstimmen, wie zum Beispiel "Danke für Ihren Anruf bei der Woodgrove Bank." Sie können eine für die Geschäftszeiten spezifische Begrüßung konfigurieren, indem Sie auf **Ändern** klicken und eine zuvor aufgezeichnete Begrüßungsdatei auswählen. Die benutzerdefinierte Begrüßung muss bereits als WAV- oder WMA-Datei aufgezeichnet worden sein.

- **Begrüßung außerhalb der Geschäftszeit:** Dies wird die anfängliche Ansage wiedergegeben wird, wenn ein Anrufer die automatische Telefonzentrale während Ihrer Organisation außerhalb der Geschäftszeiten aufruft. Standardmäßig werden keine außerhalb der Geschäftszeiten konfiguriert. Aus diesem Grund besteht keine Standard nicht - Begrüßung während der Geschäftszeit. Sie können den geschäftlichen und außerhalb der Geschäftszeiten für die automatische Telefonzentrale **Geschäftszeiten** konfigurieren.

Sie können diese Begrüßung anpassen und auf Ihre Organisation abstimmen, wie zum Beispiel "Danke für Ihren Anruf bei der Woodgrove Bank. Leider rufen Sie außerhalb der Geschäftszeit an.", oder "Dies ist der Anschluss von Contoso, Ltd. Unser Büro ist momentan leider nicht besetzt." Unsere Geschäftszeiten sind Montag und Freitag zwischen 8:00 Uhr und 17:00 Uhr." Sie können eine spezifische Begrüßung außerhalb der Geschäftszeiten konfigurieren, indem Sie auf **Ändern** klicken und eine zuvor aufgezeichnete Begrüßungsdatei auswählen. Die benutzerdefinierte Begrüßung muss bereits als WAV- oder WMA-Datei aufgezeichnet worden sein.

- **Informationsansage:** Bei Aktivierung dieses optionale Aufzeichnung wiedergegeben wird, unmittelbar nach der Business oder nicht - Begrüßung während der Geschäftszeit. Eine Informationsansage möglicherweise state der Organisation Stunden des Vorgangs, z. B. "Unsere Geschäftszeiten 8:30 Uhr bis 17:30 Uhr Montag bis Freitag und 8:30 Uhr bis 1:00 Uhr am Samstag liegen." Eine Informationsansage kann auch für die Einhaltung von Unternehmensrichtlinien erforderlichen Informationen bereitstellen, z. B. "Anrufe können überwacht werden für Schulungszwecke." Wenn sie so wichtig ist, dass die gesamte Informationsansage Anrufer hören, können sie wie unterbrechungsfreie, müssen den Anrufer an die gesamte Ansage anhören markiert.

Standardmäßig ist für UM-Wähleinstellungen oder automatische Telefonzentralen keine Informationsansage konfiguriert. Wenn Sie eine Informationsansage aktivieren und eine benutzerdefinierte Audiodatei speziell für Ihre Organisation verwenden, steht die Option **Unterbrechen der Ansage zulassen** zur Verfügung. Die Aufzeichnungen müssen bereits als aufgezeichnete WAV- oder WMA-Dateien vorliegen. Klicken Sie auf **Ändern**, um eine zuvor aufgezeichnete benutzerdefinierte Informationsansagedatei zu suchen.

**Ankündigung zu einer Unterbrechung zulassen:** Aktivieren Sie dieses Kontrollkästchen, um den Anrufer an die Informationsansage unterbrechen zu aktivieren. Dies sollte aktiviert sein, wenn Sie lange Informationszwecken Ankündigungen verfügen. Anrufer sind möglicherweise enttäuscht, wenn die Informationsansage lang ist und sie können nicht unterbrechen, um die Optionen zur Verfügung gestellt, von der automatischen Telefonzentrale zugreifen.

5. Verwenden Sie die Option **Geschäftszeiten**, um die Öffnungszeiten der Organisation festzulegen. Während der Geschäftszeiten hören Anrufer die für die Geschäftszeiten festgelegte Standardbegrüßung bzw. eine benutzerdefinierte Begrüßung und die Ansage des Hauptmenüs, wenn die entsprechenden Tastenzuordnungen für Zeiten innerhalb der Geschäftszeit im Bereich **Menünavigation** konfiguriert sind. Sie können Folgendes konfigurieren:

- **Zeitzone:** mit dieser Liste können Sie die Zeitzone auswählen. Überlegen Sie, ob die Wähleinstellungen die automatische Telefonzentrale zugeordnet mehr als eine Zeitzone wird behandelt, wenn Sie Terminplan festgelegt.

Bei lokalen und Hybridbereitstellungen wird bei der Installation des Postfachservers, auf dem der Microsoft Exchange Unified Messaging-Dienst ausgeführt wird, die Zeitzone standardmäßig unter Verwendung der Systemzeit des lokalen Servers konfiguriert.

- **Geschäftszeiten:** Klicken Sie auf **Geschäftszeiten konfigurieren**, und klicken Sie dann auf der Seite **Geschäftszeiten konfigurieren** mithilfe des Rasters um Geschäftszeiten Ihrer Organisation zu konfigurieren.
- **Feiertag Zeitplan:** Verwenden Sie diese Tagen von 00:00 bis 23:59 Uhr (24:00 Uhr bis 23:59 Uhr) definieren, an dem Ihre Organisation für einen Feiertag geschlossen. Anrufer, die die automatische

Telefonzentrale der Zeiten zu erreichen, die Sie auf der Seite **neue Feiertag** angeben hören benutzerdefinierte Feiertage Begrüßung Audiodatei, die Sie definieren. Wenn Sie den Feiertag Zeitplan konfigurieren, müssen Sie des Feiertags ein, die Audiodatei für die Begrüßung aufgezeichneten Feiertag und das **Startdatum** und **Enddatum** definieren. Die Ansage müssen bereits als WAV- oder WMA-Dateien aufgezeichnet wurden.

6. Verwenden Sie **Menünavigation** im Menüoptionen an, die für Anrufer innerhalb und außerhalb der Geschäftszeiten angeboten werden. Wenn Sie im Menünavigation aktivieren möchten, müssen Sie diese separat für Unternehmen und außerhalb der Geschäftszeiten durchführen. Beispielsweise wenn Sie Geschäftszeiten Navigation aktivieren möchten, muss ein Menü Prompt benutzerdefinierte Audioaufnahme hinzufügen, aktivieren Sie das Kontrollkästchen **Aktivieren der Menünavigation Geschäftzeiten**, klicken Sie auf **Hinzufügen** , und legen Sie dann die Optionen auf der **Neue menünavigationseintrags**-Seite.

- **Geschäftzeiten Menünavigation:** Dies ist die Liste der Optionen, die Anrufer hören, während der Geschäftszeiten, die auf der Seite **Geschäftzeiten** definiert sind. Beispielsweise "für den technischen Support drücken oder 1 angenommen. Drücken Sie für Zweigstellen und Verwaltung die oder Angenommen Sie 2. Für den Verkauf drücken, oder 3 sagen."

Sie müssen die folgenden Schritte ausführen, um eine Menünavigation während der Geschäftszeit zu aktivieren:

1. **Menü Aufforderung:** Hiermit können Sie eine benutzerdefinierte Menü Prompt Audiodatei angeben. Um eine benutzerdefinierte oder zuvor aufgezeichnete Geschäftszeiten Menü Aufforderung zu verwenden, klicken Sie auf **Ändern**, und klicken Sie dann auf **Durchsuchen**, um im Menü Prompt Aufzeichnung zu suchen.
2. **Aktivieren der Menünavigation Geschäftzeiten:** Aktivieren Sie dieses Kontrollkästchen, um Optionen für die Menünavigation im zu aktivieren, die während der Geschäftszeiten verwendet wird. Wenn Sie Geschäftszeiten Menünavigation aktivieren, können Sie neue menünavigationseinträge für Geschäftszeiten hinzufügen.
3. Klicken Sie auf **Hinzufügen**  zum Erstellen einer neuen menünavigationseintrags. Verwenden Sie die folgenden Optionen auf der Seite **neue menünavigationseintrags** zum Erstellen einer neuen menünavigationseintrags:

- **Auffordern:** Verwenden Sie dieses Feld den Namen der im Navigationsmenü neu eingeben. Der Name des Navigation wird nur für die Anzeige verwendet. Dies ist ein erforderliches Feld.

Da Sie möglicherweise mehrere neue Navigationsmenüs festlegen möchten, sollten Sie für die Tastenzuordnungen aussagekräftige Namen verwenden. Die maximale Länge des Namens für eine Tastenzuordnung beträgt 64 Zeichen inklusive Leerzeichen. Die folgenden Zeichen dürfen jedoch nicht enthalten sein: "/\[]:;|=,+\*?<>.

- **Wenn diese Taste gedrückt wird:** mit dieser Liste können tastenzuordnung aktivieren. Die tastaturzuordnung ist die Taste, die ein Anrufer drückt der automatischen Telefonzentrale einen bestimmten Vorgang ausführen Weiterleiten des Anrufers an eine andere automatische Telefonzentrale oder an einen Operator. Standardmäßig sind keine Einträge definiert.

Verwenden Sie die Dropdownliste, um die Zifferntaste (1 bis 9) auszuwählen, die der Anrufer drücken muss. Null (0) ist für die Vermittlungsstelle der automatischen Telefonzentrale reserviert.

Wenn Sie in der Dropdownliste die Option **Timeout** auswählen, können Anrufer an eine Durchwahlnummer oder eine andere automatische Telefonzentrale weitergeleitet werden, vorausgesetzt, sie drücken keine Taste auf der Wähltastatur des Telefons. Zum Beispiel "Bitte legen Sie nicht auf. Ihr Anruf wird vom nächsten freien Mitarbeiter entgegengenommen." Die Standardeinstellung ist 5 Sekunden. Wenn Sie diese Option aktivieren, wird eine leere Tastenzuordnung erstellt.

- **Die folgende Audiodatei wiedergeben:** Verwenden Sie diese Option, um eine zuvor aufgezeichnete Audiodatei für Anrufer auszuwählen. Klicken Sie auf **Ändern**, und klicken Sie dann auf **Durchsuchen**, um die Audiodatei zu suchen. Wenn Sie die Audiodatei unverändert lassen <keine>, das Modul Unified Messaging TTS (Text-zu-Sprache) wird ein Geschäftszeiten hauptmenüänsage synthetisieren. Alternativ können Sie erstellen eine benutzerdefinierte Audiodatei, die für das Hauptmenü Geschäftszeiten verwendet werden kann Prompt für eine Sprachaktiviert automatische Telefonzentrale. Beispielsweise kann es sagen Sie "zu eine Sprachnachricht hinterlassen für den Vertrieb, sagen Sie 1., Sagen Sie 2, um eine Sprachnachricht für den technischen Support zu lassen. Um eine Sprachnachricht für die Administration lassen möchten, sagen Sie 3."
- **Diese zusätzliche Aktion ausführen:** Wählen Sie eine der folgenden Optionen, um die Aktion definieren, die Sie die automatische Telefonzentrale für den Anrufer durchführen möchten:
  - **None:** Verwenden Sie diese Option, wenn Sie nicht möchten, dass die automatische Telefonzentrale Weiterleiten des Anrufs an eine Erweiterung oder an eine andere automatische Telefonzentrale oder für einen Benutzer eine Nachricht hinterlassen.,
  - **Weiterleiten an diese Durchwahl:** Wählen Sie diese Option, um Anrufe in einer Durchwahlnummer übertragen werden können. Wenn Sie diese Option aktivieren, verwenden Sie das Feld die Erweiterung, in dem der Anruf weitergeleitet werden. In diesem Feld können nur numerische Zeichen. Es kann keine der folgenden Zeichen enthalten: "/ \ []; | = , + \* ? < >.
  - **Weiterleiten an diese automatische um-Telefonzentrale:** Wählen Sie diese Option, um den Anruf an eine automatische Telefonzentrale weiterleiten aus. Klicken Sie auf **Durchsuchen**, um die automatische Telefonzentrale zu suchen, die Sie verwenden möchten. Bevor Sie diese Option aktivieren, müssen Sie zuerst erstellen und konfigurieren die automatischen Telefonzentrale. Diese Option wird verwendet, wenn Sie eine hierarchische Struktur von automatischen UM-Telefonzentralen erstellen.
  - **Eine Sprachnachricht hinterlassen für diesen Benutzer:** Wählen Sie diese Option, um ein Anrufer eine Nachricht für einen Benutzer hinterlassen, die auf dem selben Wählplan wie die automatische Telefonzentrale ist, die Sie konfigurieren können. Wenn ein Anrufer diese Option aus einem Auto attendant Menü auswählt, werden sie aufgefordert, eine Sprachnachricht für den Benutzer hinterlassen, die ausgewählt wurde. Klicken Sie auf **Durchsuchen**, um den UM-aktivierten Benutzer zu suchen.
  - **Unternehmensstandort Announce:** Wählen Sie diese Option aktivieren Sie einen Anrufer wählen eine automatische Telefonzentrale Menüoption und zu hören den Speicherort des Unternehmens, die für die automatische Telefonzentrale konfiguriert ist. Hierzu ordnungsgemäß funktioniert müssen Sie zuerst den Unternehmensstandort im Feld **Business Speicherort** auf der Seite **Allgemein** auf die automatische Telefonzentrale eingeben.
  - **Geschäftszeiten Announce:** Wählen Sie diese Option aktivieren Sie einen Anrufer wählen eine automatische Telefonzentrale Menüoption und zu hören die Betriebszeiten für das Unternehmen, der für die automatische Telefonzentrale konfiguriert ist. Hierzu ordnungsgemäß funktioniert, müssen Sie zuerst der Geschäftszeiten auf der Seite **Geschäftszeiten** der automatischen UM-Telefonzentrale konfigurieren.
  - **Geschäftszeit Stunden Menünavigation:** Dies ist die Liste der Optionen, die Anrufer hören, während der Geschäftszeiten, die auf der Seite **Geschäftszeiten** definiert sind. Beispielsweise "wird der Anruf für uns sehr wichtig. Sie haben jedoch Woodgrove Bank Geschäftszeiten erreicht. Wenn Sie eine Nachricht hinterlassen möchten, wird Bitte drücken oder sagen 1 und wir den Anruf so bald wie möglich zurück."

Sie müssen die folgenden Schritte ausführen, um eine Menünavigation außerhalb der Geschäftszeit zu aktivieren:

  1. **Menü Aufforderung:** Hiermit können Sie eine benutzerdefiniertes Menü Prompt Audiodatei angeben. Klicken Sie für die Verwendung eine benutzerdefinierten oder zuvor aufgezeichnete außerhalb der Geschäftszeiten im Menü Ausführen auf **Durchsuchen**.

**2. Aktivieren der Menünavigation außerhalb der Geschäftszeiten:** Aktivieren Sie dieses Kontrollkästchen, um Optionen für die Menünavigation im zu aktivieren, die während der Geschäftszeiten verwendet wird. Wenn Sie außerhalb der Geschäftszeiten Menünavigation aktivieren, können Sie neue menünavigationseinträge für außerhalb der Geschäftszeiten hinzufügen.

3. Klicken Sie auf **Hinzufügen** zum Erstellen einer neuen menünavigationseintrags. Verwenden Sie die folgenden Optionen auf der Seite **neue menünavigationseintrags** zum Erstellen einer neuen menünavigationseintrags:

- **Auffordern:** Verwenden Sie dieses Feld den Namen der im Navigationsmenü neu eingeben. Der Name des Navigation wird nur für die Anzeige verwendet. Dies ist ein erforderliches Feld.

Da Sie möglicherweise mehrere neue Navigationsmenüs festlegen möchten, sollten Sie für die Tastenzuordnungen aussagekräftige Namen verwenden. Die maximale Länge des Namens für eine Tastenzuordnung beträgt 64 Zeichen inklusive Leerzeichen. Die folgenden Zeichen dürfen jedoch nicht enthalten sein: " / \ [ ] : ; | = , + \* ? < > .

- **Wenn diese Taste gedrückt wird:** mit dieser Liste können tastenzuordnung aktivieren. Die tastaturzuordnung ist die Taste, die ein Anrufer drückt der automatischen Telefonzentrale einen bestimmten Vorgang ausführen Weiterleiten des Anrufers an eine andere automatische Telefonzentrale oder an einen Operator. Standardmäßig sind keine Einträge definiert.

Verwenden Sie die Dropdownliste, um die Zifferntaste (1 bis 9) auszuwählen, die der Anrufer drücken muss. Null (0) ist für die Vermittlungsstelle der automatischen Telefonzentrale reserviert.

Wenn Sie in der Dropdownliste die Option **Timeout** auswählen, können Anrufer an eine Durchwahlnummer oder eine andere automatische Telefonzentrale weitergeleitet werden, vorausgesetzt, sie drücken keine Taste auf der Wähltafel des Telefons. Zum Beispiel "Bitte legen Sie nicht auf. Ihr Anruf wird vom nächsten freien Mitarbeiter entgegengenommen." Die Standardeinstellung ist 5 Sekunden. Wenn Sie diese Option aktivieren, wird eine leere Tastenzuordnung erstellt.

- **Die folgende Audiodatei wiedergeben:** Verwenden Sie diese Option, um eine zuvor aufgezeichnete Audiodatei für Anrufer auszuwählen. Klicken Sie auf **Ändern**, und klicken Sie dann auf **Durchsuchen**, um die Audiodatei zu suchen. Wenn Sie die Audiodatei unverändert lassen <keine>, das Modul Unified Messaging TTS (Text-zu-Sprache) wird eine Hauptmenüansage außerhalb der Geschäftszeiten synthetisieren. Alternativ können Sie eine benutzerdefinierte Audiodatei erstellen, die für die außerhalb der Geschäftszeiten Hauptmenüansage für eine Sprachaktivierte automatische Telefonzentrale verwendet werden kann, die, z. B. würde "Sie" Contoso "während der Geschäftszeiten erreicht haben. Um eine Sprachnachricht für den Verkauf lassen möchten, sagen Sie 1. Sagen Sie 2, um eine Sprachnachricht für den technischen Support zu lassen. Um eine Sprachnachricht für die Administration lassen möchten, sagen Sie 3. Zum Erreichen einer Geschäftszeiten Operator, drücken Sie 0 (null)."

- **Diese zusätzliche Aktion ausführen:** Wählen Sie eine der folgenden Optionen, um die Aktion definieren, die Sie die automatische Telefonzentrale für den Anrufer durchführen möchten:

- **None:** Verwenden Sie diese Option, wenn Sie nicht möchten, dass die automatische Telefonzentrale Weiterleiten des Anrufs an eine Erweiterung oder an eine andere automatische Telefonzentrale oder für einen Benutzer eine Nachricht hinterlassen.,

- **Weiterleiten an diese Durchwahl:** Wählen Sie diese Option, um Anrufe in einer Durchwahlnummer übertragen werden können. Wenn Sie diese Option aktivieren, verwenden Sie das Feld die Durchwahlnummer eingeben, in dem der Anruf weitergeleitet werden. In diesem Feld können nur numerische Zeichen. Es kann keine der folgenden Zeichen enthalten: " / \ [ ] : ; | = , + \* ? < > .

- **Weiterleiten an diese automatische um-Telefonzentrale:** Wählen Sie diese Option, um den Anruf an eine vorhandene automatische Telefonzentrale übertragen. Klicken Sie auf **Durchsuchen**, um die

automatische Telefonzentrale zu suchen, die Sie verwenden möchten. Bevor Sie diese Option aktivieren, müssen Sie zuerst erstellen und konfigurieren die automatischen Telefonzentrale. Diese Option wird verwendet, wenn Sie eine hierarchische Struktur von automatischen UM-Telefonzentralen erstellen.

- **Eine Sprachnachricht hinterlassen für diesen Benutzer:** Wählen Sie diese Option, um ein Anrufer eine Nachricht für einen Benutzer hinterlassen, die auf dem selben Wählplan wie die automatische Telefonzentrale ist, die Sie konfigurieren können. Wenn ein Anrufer diese Option aus einem Auto attendant Menü auswählt, werden sie aufgefordert, eine Sprachnachricht für den Benutzer hinterlassen, die ausgewählt wurde. Klicken Sie auf **Durchsuchen**, um den UM-aktivierten Benutzer zu suchen.
- **Unternehmensstandort Announce:** Wählen Sie diese Option aktivieren Sie einen Anrufer wählen eine automatische Telefonzentrale Menüoption und zu hören den Speicherort des Unternehmens, die für die automatische Telefonzentrale konfiguriert ist. Hierzu ordnungsgemäß funktioniert müssen Sie zuerst den Unternehmensstandort im Feld **Business Speicherort** auf der Seite **Allgemein** auf die automatische Telefonzentrale eingeben.
- **Geschäftszeiten Announce:** Wählen Sie diese Option aktivieren Sie einen Anrufer wählen eine automatische Telefonzentrale Menüoption und zu hören die Betriebszeiten für das Unternehmen, der für die automatische Telefonzentrale konfiguriert ist. Hierzu ordnungsgemäß funktioniert, müssen Sie zuerst der Geschäftszeiten auf der Seite **Geschäftszeiten** der automatischen UM-Telefonzentrale konfigurieren.

7. Verwenden Sie die Einstellung **Zugriff auf Adressbuch und Vermittlungsstelle**, um die Funktionen zu definieren, die Anrufern bei einem Anruf bei der automatischen Telefonzentrale zur Verfügung stehen. Sie können folgende Funktionen konfigurieren: die bei der Anwahl der automatischen Telefonzentrale zu verwendende Sprache sowie die Umleitung von Anrufern an die Durchwahlnummer der Vermittlungsstelle. Sie können Folgendes konfigurieren:

- **Optionen für die Kontaktaufnahme mit Benutzern:** Verwenden Sie diese Optionen, um zu bestimmen, wie Anrufer wenden können Benutzer mit Voicemail Wenn sie in einer automatischen UM-Telefonzentrale anrufen
- **Anrufer So wählen Sie Benutzer zulassen:** Aktivieren Sie dieses Kontrollkästchen, um Aufrufer zum Übertragen von Anrufen für Benutzer zu aktivieren. Standardmäßig ist diese Option ist aktiviert und kann Benutzer, die in der gleichen um-Wählplan der Dial Plan Übertragung Anrufe für Benutzer zugeordnet sind. Nachdem Sie dieses Kontrollkästchen aktivieren, können Sie festlegen, die Gruppe von Benutzern, die Anrufer übertragen werden können, indem Sie die entsprechende Option unter **Optionen für die Suche des Adressbuchs** auf dieser Seite auswählen.

Wenn Sie diese Option und die Option **Anrufer dürfen Sprachnachrichten für Benutzer hinterlassen** deaktivieren, stehen die Optionen unter **Optionen zum Durchsuchen des Adressbuchs** nicht zur Verfügung.

- **Anrufer zu belassen, Sprachnachrichten für Benutzer zulassen:** Aktivieren Sie dieses Kontrollkästchen, um Anrufer Sprachnachrichten an Benutzer senden aktivieren. Standardmäßig ist diese Option ist aktiviert und kann Benutzer, die in der gleichen um-Wählplan Dial Plan senden Sprachnachrichten für Benutzer zugeordnet sind. Nachdem Sie dieses Kontrollkästchen aktivieren, können Sie festlegen, die Gruppe von Benutzern, die Anrufer, indem Sie die entsprechende Option unter **Optionen für die Suche des Adressbuchs** auf dieser Seite auswählen Sprachnachrichten senden können.

Wenn Sie diese Option und die Option **Anrufer dürfen Benutzer wählen** deaktivieren, stehen die Optionen unter **Optionen zum Durchsuchen des Adressbuchs** nicht zur Verfügung.

Wenn Sie diese Option deaktivieren, stellt die automatische Telefonzentrale Anrufern während einer Systemansage nicht das Senden einer Sprachnachricht zur Wahl.

- **Optionen für die Suche im Adressbuchs:** Verwenden Sie diese Optionen, um eine Gruppierung von Benutzern zu bestimmen. Standardmäßig wird zusammen mit der Option **In diesen Wähleinstellungen**

**nur Zulassen Anrufer zum Suchen nach Benutzer nach Name oder Alias** ausgewählt. Sie können jedoch ändern die Gruppierung von Benutzern, ob Anrufer durchstellen von Anrufen oder Sprachnachrichten an Benutzer senden können, die in der globalen Adressliste (GAL) für eine Organisation befinden. Sie können aus den folgenden wählen:

- **Anrufer zulassen nach Benutzern nach Name oder Alias zu suchen:** Standardmäßig ist diese Option ausgewählt. Dabei können Anrufer diese automatische Telefonzentrale Aufrufen eine Verzeichnissuche für Benutzer nach Name oder nach ihren Alias ausführen. Ein Alias wird zu einem Benutzer zugewiesen, wenn ein Postfach für sie erstellt wird. Der Alias ist der erste Teil des SMTP-Adresses, beispielsweise [tonysmith@contoso.com](mailto:tonysmith@contoso.com). Die SMTP-Adresse ist [tonysmith@contoso.com](mailto:tonysmith@contoso.com), während der Alias "tonysmith". Wenn Sie diese Option wirkt sich nur auf Anrufer, die diese automatische Telefonzentrale und nicht die Benutzer Outlook Voice Access verwenden.
- **In diesen Wähleinstellungen nur:** Wählen Sie diese Option, um den Anrufer an die automatische Telefonzentrale zu suchen, und wenden Sie sich an Benutzer eine Verbindung zu ermöglichen, die in den gleichen Wähleinstellungen sind, die dieser automatischen UM-Telefonzentrale zugeordnet ist. Standardmäßig ist diese Option für den Wahlplan und für die automatische Telefonzentrale aktiviert. Dies bedeutet, dass Outlook Voice Access-Benutzer und Anrufer in der automatischen Telefonzentrale für Benutzer innerhalb desselben Wahlplans suchen können.
- **In der gesamten Organisation:** Wählen Sie diese Option, um können Anrufer, die Aufrufen in dieser automatischen um-Telefonzentrale suchen, und wenden Sie sich an alle Personen, die in der globalen Adressliste für die Organisation aufgelistet. Dies schließt nicht nur UM-aktivierte Benutzer, sondern alle Benutzer, die Postfach aktiviert werden. Mit dieser Option können Anrufer an Benutzer in mehrere Wahlpläne wenden. Es ist nicht standardmäßig aktiviert. Diese Einstellung ist auch auf einem Wahlplan für Outlook Voice Access-Benutzer verfügbar.
- **Für ähnliche Namen einzufügenden Informationen:** Verwenden Sie diese Dropdown-Liste auswählen die Option für die automatische Telefonzentrale verwendet werden, wenn Benutzer die gleichen oder ähnlichen Namen haben. Diese Einstellung wird verwendet, wenn mindestens zwei Benutzer mit dem gleichen Namen im Verzeichnis vorhanden sind. Dies ist auch einen übereinstimmenden Namen oder zur Klärung Feld bezeichnet. Sie können diese Einstellung konfigurieren, oder lassen Sie die Standardeinstellung für die automatische Telefonzentrale. Standardmäßig wird die automatische Telefonzentrale diese Einstellung aus der Einstellung für den Wahlplan erben, die mit der automatischen Telefonzentrale verknüpft ist. Es folgt ein Beispiel für eine Sprachaktivierte automatische Telefonzentrale:
  1. System: "Herzlich willkommen bei Contoso. Wenn Sie den Namen der Person kennen, die Sie erreichen möchten, sagen Sie bitte deren Namen."
  2. Anrufer sagt "Tony Smith."
  3. Es gibt mehrere Personen mit diesem Namen. Wählen Sie eine der folgenden Optionen: Für Tony Smith, Forschung, drücken Sie bitte die 1. Für Tony Smith, Verwaltung, drücken Sie bitte die 2. Für Tony Smith, technischer Support, drücken Sie bitte die 3."
  4. Der Anrufer drückt die entsprechende Taste auf der Tastatur, und der Anruf wird an den gewünschten Benutzer übergeben.

#### **NOTE**

Bei Verwendung einer automatischen Telefonzentrale ohne Sprachaktivierung weist das System den Anrufer an, den Namen des Benutzers (Nachname zuerst) über die Tastatur einzugeben und nach dem Benutzer zu suchen. Wenn mehrere Personen mit demselben Namen im Verzeichnis enthalten sind, wird der Anrufer angewiesen, die geeignete Taste zu drücken, um mit dem gewünschten Benutzer verbunden zu werden. Sie können optional eine automatische DTMF-Fallback-Telefonzentrale erstellen, die ausschließlich die Tastatur zur Eingabe eines Namens oder Alias verwendet.

Zur Verwendung dieser Einstellungen müssen Sie dem Benutzer die richtigen Informationen hinzufügen. Wenn Sie beispielsweise möchten, dass die automatische Telefonzentrale einen Titel zur Unterscheidung von zwei Benutzern mit demselben Namen verwendet, müssen Sie diese Informationen dem Benutzerkonto hinzufügen. Wählen Sie eine der folgenden Methoden aus, um dem Anrufer weitere Informationen bereitzustellen, die diesen bei der Auswahl des gewünschten Benutzers in der Organisation unterstützen:

- **Erben von Wähleinstellungen:** Wählen Sie diese Option, um die automatische Telefonzentrale Verwendung haben die Standardeinstellung aus dem Wählplan mit der automatischen Telefonzentrale verknüpft ist.
- **Titel:** Wählen Sie diese Option, damit die automatische Telefonzentrale Titel des Benutzers einschließen aus, wenn Übereinstimmungen auflisten.
- **Abteilung:** Wählen Sie diese Option, damit die automatische Telefonzentrale Abteilung des Benutzers einschließen aus, wenn der Auflistung entspricht.
- **Speicherort:** Wählen Sie diese Option, damit die automatische Telefonzentrale Standort des Benutzers einschließen aus, wenn der Auflistung entspricht.
- **None:** Wählen Sie diese Option, wenn keine weiteren Informationen beim Auflisten von Übereinstimmungen angegeben haben.
- **Aufforderung für Alias:** Wählen Sie diese Option, damit die automatische Telefonzentrale auffordern, den Anrufer in der Aliasname des Benutzers.

8. Unterhalb von **Vermittlungsstellenzugriff** können Sie folgende Vermittlungsstelleneinstellungen für die automatische Telefonzentrale festlegen:

- **Operator-Erweiterung:** in diesem Feld Geben Sie die Durchwahlnummer verwendet, um einen Operator aufrufen können. Diese Durchwahlnummer kann Anrufer Herstellen einer Verbindung mit einer human-Operator oder ein UM-aktivierten Postfach, oder rufen Sie eine externe Telefonnummer konfiguriert werden kann. Standardmäßig ist eine Erweiterung Operator in dieses Feld nicht enthalten.
- **Zulassen Übergabe an Vermittlungsstelle während der Geschäftszeit:** Aktivieren Sie dieses Kontrollkästchen aktivieren Anrufer übertragen werden an einen human Operator während der Geschäftszeit mithilfe von die Durchwahlnummer an, die Sie im Feld **Operator Erweiterung** konfigurieren. Diese Option ist standardmäßig deaktiviert.

Diese Option sollte aktiviert werden, damit Anrufer eine Sprachnachricht hinterlassen bzw. bei der Vermittlungsstelle anrufen können, falls Sie den gewünschten Teilnehmer während der Geschäftszeit weder über Menüansagen noch über die Verzeichnissuche erreichen können. Nach dem Aktivieren dieser Option können Sie die Durchwahlnummer für die Vermittlungsstelle festlegen, die in einem überwachten UM-fähigen Postfach konfiguriert ist. Der Anrufer kann eine Sprachnachricht hinterlassen oder die Hilfe eines Telefonisten in Anspruch nehmen, der die Durchwahlnummer kennt.

- **Zulassen Übergabe an Vermittlungsstelle während der Geschäftszeiten:** Aktivieren Sie dieses

Kontrollkästchen aktivieren Anrufer übertragen werden an einen Operator human Geschäftszeiten mithilfe von die Durchwahlnummer an, die Sie im Feld **Operator Erweiterung** konfigurieren. Diese Option ist standardmäßig deaktiviert.

Diese Option sollte aktiviert werden, damit Anrufer eine Sprachnachricht hinterlassen bzw. bei der Vermittlung anrufen können, falls Sie den gewünschten Teilnehmer außerhalb der Geschäftszeit weder über Menüansagen noch über die Verzeichnissuche erreichen können. Nach dem Aktivieren dieser Option können Sie die Durchwahlnummer für die Vermittlungsstelle festlegen, die in einem überwachten UM-fähigen Postfach konfiguriert ist. Der Anrufer kann eine Sprachnachricht hinterlassen oder die Hilfe eines Telefonisten in Anspruch nehmen, der die Durchwahlnummer kennt.

9. Verwenden Sie die Einstellung **Wählautorisierung**, um Wählregeln für Anrufer zu konfigurieren, die bei einer automatischen UM-Telefonzentrale anrufen. Mithilfe dieser Einstellungen können Sie die Durchwahlnummern steuern, die über eine automatische Telefonzentrale erreichbar sind, oder die Rufnummern, die von Anrufern gewählt werden können, die eine automatische Telefonzentrale angewählt haben. Sie können Folgendes konfigurieren:

- **Anrufe in die gleiche UM-Wählplan:** Aktivieren Sie dieses Kontrollkästchen, um Benutzern zu ermöglichen, die eine automatische Telefonzentrale, der getätigten oder durchstellen von Anrufen an einer Durchwahlnummer eines UM-aktivierten Benutzers anrufen, die die gleichen Wählplan wie die automatische Telefonzentrale zugeordnet ist. Diese Einstellung ist standardmäßig aktiviert.

Wenn Sie diese Einstellung deaktivieren, können Benutzer beim Anwählen einer automatischen Telefonzentrale Benutzer ohne UM-Aktivierung oder andere Durchwahlnummern anrufen, die keinem UM-aktivierten Benutzer zugeordnet sind, sowie Anrufe an diese weiterleiten. Benutzer können keine Anrufe an UM-aktivierte Benutzer weiterleiten, die denselben Wähleinstellungen wie die automatische Telefonzentrale zugeordnet sind. Der Grund dafür ist, dass die Einstellung **Anrufe an jede Durchwahl zulassen** standardmäßig aktiviert ist.

- **Zulassen von Anrufen an eine beliebige Erweiterung:** Wenn diese Einstellung deaktiviert ist, können keine Benutzer, die eine automatische Telefonzentrale anrufen platzieren Anrufe werden nicht UM-aktivierten Benutzern oder anderen Durchwahlnummern keinem UM-aktivierten Benutzer zugeordnet. Sie können jedoch anrufen und Weiterleiten von Anrufen an Durchwahlnummern UM-aktivierten Benutzer zugeordnet platzieren. Dies ist, da die **Anrufe in demselben UM-Wählplans** Einstellung standardmäßig aktiviert ist. Die Einstellung für **jede Erweiterung aufrufen zulassen** ist standardmäßig aktiviert.

Wenn diese Einstellung aktiviert ist, können Benutzer beim Anwählen einer automatischen Telefonzentrale Benutzer ohne UM-Aktivierung, andere Durchwahlnummern, die keinem UM-aktiviertem Benutzer zugeordnet sind, und UM-aktivierte Benutzer anrufen. Der Grund dafür ist, dass die Einstellung **Anrufe in denselben UM-Wähleinstellungen** standardmäßig aktiviert ist.

Diese Einstellung kann in einer Umgebung aktiviert werden, in der nicht alle Benutzer UM-aktiviert sind. Sie ist außerdem hilfreich, wenn Sie zulassen möchten, dass Benutzer, die bei einer in einer Telefonzentrale konfigurierten Rufnummer anrufen, Durchwahlnummern anrufen können, die keinem UM-aktivierten Benutzer zugeordnet sind.

- **Autorisierte nationale/regionale Wählregelgruppen:** Verwenden Sie diesen Abschnitt zum Hinzufügen oder Entfernen von nationale/regionale Wählregelgruppen zulässig. Standardmäßig gibt es keine nationale/regionale Wählregelgruppen auf automatische um-Telefonzentralen konfiguriert sind.

Mit nationalen/regionalen Wählregelgruppen können Sie den Zugriff auf Rufnummern in einem Land oder einer Region zulassen oder beschränken, die von Benutzern beim Anrufen der UM-Telefonzentrale gewählt werden können. Diese Maßnahme hilft dabei, unnötige bzw. nicht autorisierte Telefonate und Gebühren zu vermeiden.

Sie müssen zuerst die entsprechenden nationalen/regionalen Wählregelgruppen für die Wähleinstellungen

erstellen, die der UM-Telefonzentrale zugeordnet sind, um nationale/regionale Wählregelgruppen hinzufügen zu können. Anschließend müssen Sie die entsprechende Wählregelgruppe hinzufügen.

Nationale/regionsinterne Wählregelgruppen können von Unified Messaging verwendet werden, um den Zugriff auf Rufnummern in einem Land oder einer Region zuzulassen oder einzuschränken. Dies wird bei jedem Benutzer angewendet, der bei einer Telefonzentrale anruft. Weitere Informationen zum Wählen externer Nummern finden Sie unter [Autorisieren von Benutzern für Anrufe](#).

- **Internationale Wählregelgruppen autorisiert:** Verwenden Sie diesen Abschnitt zum Hinzufügen oder Entfernen von internationale Wählregelgruppen zulässig. Standardmäßig sind gibt es keine internationale Wählregelgruppen auf automatische um-Telefonzentralen konfiguriert.

Mit internationalen Wählregelgruppen können Sie den Zugriff auf Rufnummern außerhalb eines Landes oder einer Region zulassen oder beschränken, die von Benutzern beim Anrufen der UM-Telefonzentrale gewählt werden können. Diese Maßnahme hilft dabei, unnötige bzw. nicht autorisierte Telefonate und Gebühren zu vermeiden.

Zum Hinzufügen von internationalen Wählregelgruppen müssen Sie zunächst geeignete internationale Wählregelgruppen in dem Wählplan erstellen, der der automatischen UM-Telefonzentrale zugeordnet ist. Nachdem Sie die erforderlichen Wählregelgruppen im Wählplan erstellt haben, müssen Sie sie der Liste der autorisierten Wählregelgruppen in der automatischen UM-Telefonzentrale hinzufügen.

Mithilfe von internationalen Wählregelgruppen kann Unified Messaging den Zugriff auf Rufnummern außerhalb eines Lands oder einer Region zulassen oder einschränken. Dies wird bei jedem Benutzer angewendet, der bei einer Telefonzentrale anruft. Weitere Informationen zum Wählen externer Nummern finden Sie unter [Autorisieren von Benutzern für Anrufe](#).

10. Klicken Sie auf **OK**, um die neue Menünavigation zu erstellen.
11. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale** auf **Speichern**, um die Änderungen zu speichern.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie UM automatische Telefonzentrale-Eigenschaften

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert **MySpeechEnabledAA** zurückgreifen der **MyDTMFAA** -Telefonzentrale, wird der Operator Erweiterung auf 50100 und Übertragungen, diese Durchwahlnummer Geschäftszeiten ermöglicht.

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -DTMFFallbackAutoAttendant MyDTMFAA -OperatorExtension 50100 -AfterHoursTransferToOperatorEnabled $true
```

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert **MyUMAutoAttendant** , bei dem: Geschäftszeiten konfiguriert als 10:45 bis 13:15 (10:45 und 1:15 Uhr) an einem Sonntag 09:00 Uhr bis 17:00 (09:00 Uhr bis 17:00 Uhr) am Montag und 09:00 bis 16:30 (9:00 Uhr bis 4:30 Uhr) samstags; Feiertag Zeiten und ihre zugehörigen Ansage als "Neues Jahr" auf 2 Januar 2013 konfiguriert. und "Erstellen von geschlossen für Konstruktion" vom April 24 bis 28 April 2013 konfiguriert.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -BusinessHoursSchedule 0.10:45-0.13:15,1.09:00-1.17:00,6.09:00-6.16:30 -HolidaySchedule "New Year,newyrgrt.wav,1/2/2013","Building Closed for Construction,construction.wav,4/24/2013,4/28/2013"
```

## Verwenden Sie Exchange Online PowerShell, um Eigenschaften für

## Ansicht UM automatische Telefonzentrale

In diesem Beispiel wird eine formatierte Liste aller automatischen UM-Telefonzentralen zurückgegeben.

```
Get-UMAutoAttendant | Format-List
```

In diesem Beispiel werden die Eigenschaften einer automatischen UM-Telefonzentrale mit dem Namen "MyUMAutoAttendant" angezeigt.

```
Get-UMAutoAttendant -Identity MyUMAutoAttendant
```

# Konfigurieren Sie eine automatische DTMF-fallback-Telefonzentrale

18.12.2018 • 5 minutes to read

Sie können eine sprachaktivierte automatische UM-Telefonzentrale (Unified Messaging) konfigurieren, die über eine automatische DTMF-Fallback-Telefonzentrale (Dual Tone Multi-Frequency) verfügt. Eine automatische DTMF-Fallback-Telefonzentrale wird verwendet, wenn die sprachaktivierte automatische UM-Telefonzentrale die Spracheingaben des Anrufers nicht verstehen oder erkennen kann. Wenn eine automatische DTMF-Fallback-Telefonzentrale konfiguriert wurde, muss der Anrufer DTMF-Eingaben (auch als Tonwahleingaben bezeichnet) verwenden, um durch das Menüsystem der Telefonzentrale zu navigieren, den Namen eines Benutzers zu buchstabieren oder eine benutzerdefinierte Menüansage zu verwenden. Wenn keine automatische DTMF-Fallback-Telefonzentrale konfiguriert und die maximale Anzahl von Spracheingaben überschritten wurde, da das System den Anrufer nicht verstanden hat, antwortet das System mit folgender Ansage: "Leider kann ich Ihnen nicht helfen. Versuchen Sie es später noch einmal."

Eine automatische Telefonzentrale ist bei ihrer Erstellung standardmäßig nicht sprachaktiviert. Nachdem Sie die automatische Telefonzentrale sprachaktiviert haben, können die Anrufer nur Sprachbefehle und keine Tonwahleingaben verwenden, um durch das Menüsystem der automatischen Telefonzentrale zu navigieren. Obwohl es nicht erforderlich ist, wird empfohlen, dass Sie eine automatische DTMF-Fallback-Telefonzentrale für jede sprachaktivierte automatische Telefonzentrale konfigurieren, damit die Anrufer Tonwahleingaben verwenden können, falls die sprachaktivierte automatische Telefonzentrale die gesagten Worte nicht erkennt oder versteht. Außerdem wird empfohlen, dass Sie eine automatische DTMF-Fallback-Telefonzentrale nicht sprachaktivieren.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren einer sprachaktivierten automatischen Telefonzentrale

## **zur Verwendung einer automatischen DTMF-Fallback-Telefonzentrale mithilfe der Exchange-Verwaltungskonsole**

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. Wählen Sie in der Listenansicht den UM-Wählplan zu ändern, und klicken Sie auf **Bearbeiten**.
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen** UM-Telefonzentrale für die Sie eine automatische DTMF-fallback-Telefonzentrale erstellen möchten. Klicken Sie auf der Symbolleiste auf **Bearbeiten**.
3. Aktivieren Sie auf der Seite **Automatische UM-Telefonzentrale > Allgemein** das Kontrollkästchen neben **Verwenden Sie diese automatische Telefonzentrale, wenn Sprachbefehle nicht ordnungsgemäß funktionieren**, und klicken Sie anschließend auf **Durchsuchen**.
4. Wählen Sie auf der Seite **Automatische UM-Telefonzentrale auswählen** die automatische Telefonzentrale aus, die Sie als automatische DTMF-Fallback-Telefonzentrale verwenden möchten, und klicken Sie anschließend auf **Speichern**.

### **IMPORTANT**

Zuerst muss die automatische Telefonzentrale sprachaktiviert werden, bevor Sie nach einer von Ihnen eingerichteten automatischen DTMF-Fallback-Telefonzentrale suchen können.

## **Verwenden von Exchange Online PowerShell zum Konfigurieren einer Sprachaktivierte automatische Telefonzentrale mit einer DTMF-fallback-Telefonzentrale**

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen konfiguriert **MySpeechEnabledAA** verwenden eine DTMF-fallback-Telefonzentrale mit dem Namen **MyDTMFAA**.

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -DTMFFallbackAutoAttendant MyDTMFAA
```

# Aktivieren einer automatischen UM-Telefonzentrale

18.12.2018 • 2 minutes to read

Beim Erstellen einer automatischen UM-Telefonzentrale wird deren Status standardmäßig auf "Deaktiviert" festgelegt. Nach der Erstellung können Sie den Status der automatischen UM-Telefonzentrale ändern, damit eingehende Anrufe über die Telefonzentrale entgegengenommen werden können.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren einer automatischen UM-Telefonzentrale mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. Wählen Sie in der Listenansicht den UM-Wählplan zu ändern, und klicken Sie auf **Bearbeiten**.
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen** UM-Telefonzentrale, den, die Sie aktivieren möchten. Klicken Sie auf der Symbolleiste auf den **Pfeil nach oben ↑**.
3. Klicken Sie auf der Seite **Warnung** auf **Ja**.

## Verwenden Sie Exchange Online PowerShell, um eine automatische um-Telefonzentrale aktivieren

Dieses Beispiel aktiviert die automatische Telefonzentrale mit dem Namen `MyUMAutoAttendant`, die eingehende Anrufe entgegennehmen.

```
Enable-UMAutoAttendant -Identity MyUMAutoAttendant
```

# Deaktivieren einer automatischen UM-Telefonzentrale

18.12.2018 • 3 minutes to read

Beim Erstellen einer automatischen UM-Telefonzentrale wird deren Status standardmäßig auf "Deaktiviert" festgelegt. Nachdem Sie die automatische UM-Telefonzentrale erstellt haben, können Sie deren Status ändern, um zu steuern, ob sie eingehende Anrufe annehmen kann. Sie können beispielsweise die automatische UM-Telefonzentrale deaktivieren, um benutzerdefinierte Ansagen und Mitteilungen zum ersten Mal oder erneut aufzuzeichnen.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#). Vergewissern Sie sich außerdem, dass der Status der automatischen UM-Telefonzentrale auf "Aktiviert" festgelegt ist.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Deaktivieren einer automatischen UM-Telefonzentrale mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. Klicken Sie in der Listenansicht auswählen die Wähleinstellungen, die Sie ändern möchten, und klicken Sie auf der Symbolleiste auf **Bearbeiten**.
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen** UM-Telefonzentrale, den, die Sie deaktivieren möchten. Klicken Sie auf der Symbolleiste auf **Pfeil nach unten** ↓
3. Klicken Sie auf der Seite **Warnung** auf **Ja**.

Verwenden Sie Exchange Online PowerShell, um eine automatische um-Telefonzentrale deaktivieren

In diesem Beispiel wird eine automatische Telefonzentrale mit dem Namen `MyUMAutoAttendant`.

```
Disable-UMAutoAttendant -Identity MyUMAutoAttendant
```

# Löschen einer automatischen UM-Telefonzentrale

18.12.2018 • 2 minutes to read

Nach dem Löschen einer Telefonzentrale von Unified Messaging (UM) werden die eingehenden Anrufe, die von der automatischen UM-Telefonzentrale beantwortet wurden, von einem Mitarbeiter der Vermittlungsstelle beantwortet. Eine automatische UM-Telefonzentrale kann nicht gelöscht werden, wenn ihr als standardmäßige automatische UM-Telefonzentrale ein Satz UM-Wähleinstellungen zugeordnet wurde.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Löschen einer automatischen UM-Telefonzentrale mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen** UM-Telefonzentrale, den, die Sie löschen möchten. Klicken Sie auf der Symbolleiste auf **Löschen**. Klicken Sie auf der Seite **Warnung** auf **Ja**.

## Verwenden von Exchange Online PowerShell So löschen Sie eine automatische um-Telefonzentrale

Dieses Beispiel löscht eine UM-Telefonzentrale mit dem Namen `MyUMAutoAttendant`.

```
Remove-UMAutoAttendant -Identity MyUMAutoAttendant
```

# Aktivieren oder Deaktivieren der automatischen Spracherkennung

18.12.2018 • 4 minutes to read

Sie können die automatische Unified Messaging-Telefonzentrale (UM) für die automatische Spracherkennung aktivieren. Durch die Sprachaktivierung einer automatischen UM-Telefonanlage können Benutzer verbal auf die Ansagen der automatischen Telefonzentrale antworten bzw. durch das Menüsystem der automatischen Telefonzentrale navigieren. Eine automatische Telefonzentrale ist bei ihrer Erstellung standardmäßig nicht sprachaktiviert. Nachdem Sie die automatische Telefonzentrale sprachaktiviert haben, können die Anrufer nur Sprachbefehle und keine Tonwahleingaben verwenden, um durch das Menüsystem der automatischen Telefonzentrale zu navigieren.

Diese Vorgehensweise ist zwar nicht erforderlich, es wird jedoch empfohlen, eine automatische DTMF-Fallback-Telefonzentrale (Dual Tone Multi-Frequency) für jede sprachaktivierte automatische Telefonzentrale zu erstellen, damit Anrufer Tonwahleingaben verwenden können, wenn die sprachaktivierte automatische Telefonzentrale die von ihnen gesprochenen Wörter nicht erkennt oder versteht. Wenn eine automatische DTMF-Fallback-Telefonzentrale konfiguriert ist, können Benutzer die DTMF-Eingabe (auch als Tonwahleingabe bezeichnet) verwenden, um durch das Menüsystem der automatischen Telefonzentrale zu navigieren, den Namen eines Benutzers zu buchstabieren oder eine benutzerdefinierte Menüansage zu verwenden. Es wird empfohlen, die Spracherkennung für automatische DTMF-Fallback-Telefonzentralen nicht zu aktivieren.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Aktivieren der Spracherkennung einer automatischen UM-Telefonzentrale

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der

Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale Sie Speech aktivieren möchten, und klicken Sie dann auf **Bearbeiten**

3. Aktivieren Sie auf der Seite **Automatische UM-Telefonzentrale > Allgemein** das Kontrollkästchen **Automatische Telefonzentrale zum Beantworten von Sprachbefehlen festlegen**, um die Spracherkennung zu aktivieren. Deaktivieren Sie dieses Kontrollkästchen, um die automatische Spracherkennung zu deaktivieren.

4. Klicken Sie auf **Speichern**.

Verwenden Sie Exchange Online PowerShell, um eine automatische um-Telefonzentrale Speech aktivieren

Dieses Beispiel aktiviert die ASR auf einer automatischen um-Telefonzentrale mit dem Namen `MySpeechEnabled AA`

```
Set-UMAutoAttendant -Identity MySpeechEnabledAA -SpeechEnabled $true
```

# Ermöglichen oder verhindern, dass Weiterleiten von Anrufen von einer automatischen Telefonzentrale

18.12.2018 • 3 minutes to read

Sie können für Anrufer das Weiterleiten von Anrufen an Benutzer über eine automatische Telefonzentrale aktivieren oder deaktivieren. Diese Option ist standardmäßig aktiviert und ermöglicht die Weiterleitung von Anrufern an UM-aktivierte Benutzer im Unified Messaging-Wählplan (UM), der der automatischen UM-Telefonzentrale zugeordnet ist.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren oder Verhindern der Anrufweiterleitung an Benutzer von einer automatischen UM-Telefonzentrale mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** 
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie den Anruf weiterleiten konfigurieren möchten, und klicken Sie dann auf **Bearbeiten** 
3. Aktivieren Sie auf der Seite **Automatische UM-Telefonzentrale > Zugriff auf Adressbuch und Vermittlungsstelle** unter **Optionen für das Kontaktieren von Benutzern** das Kontrollkästchen neben **Anrufer dürfen Benutzer wählen**, um das Weiterleiten von Anrufen zu ermöglichen. Deaktivieren Sie das Kontrollkästchen, um die Anrufweiterleitung zu verhindern.

4. Klicken Sie auf **Speichern**.

**NOTE**

Wenn Sie dieses Kontrollkästchen und auch das Kontrollkästchen **Anrufer dürfen Sprachnachrichten für Benutzer hinterlassen** deaktivieren, stehen die Optionen unter **Optionen zum Durchsuchen des Adressbuchs** nicht zur Verfügung.

Verwenden von Exchange Online PowerShell zu aktivieren oder eine automatische um-Telefonzentrale Call gehandelt an Benutzer verhindern

In diesem Beispiel wird verhindert, dass Call gehandelt auf einer automatischen um-Telefonzentrale mit dem Namen `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AllowDialPlanSubscribers $false
```

Dieses Beispiel aktiviert die Call gehandelt auf einer automatischen um-Telefonzentrale mit dem Namen `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AllowDialPlanSubscribers $true
```

# Aktivieren oder Deaktivieren des Versands von Sprachnachrichten an Benutzer

18.12.2018 • 4 minutes to read

Sie können Anrufern das Senden von Sprachnachrichten an Benutzer von einer automatischen UM-Telefonzentrale ermöglichen oder das Senden solcher Sprachnachrichten verhindern. Diese Option ist standardmäßig aktiviert und ermöglicht Anrufern das Senden von Sprachnachrichten an Benutzer in einem Satz mit UM-Wähleinstellungen (Unified Messaging), der der automatischen UM-Telefonzentrale zugeordnet ist. Wenn Sie diese Option deaktivieren, stellt die automatische Telefonzentrale Anrufern während einer Systemansage nicht das Senden einer Sprachnachricht zur Wahl.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren oder Deaktivieren von Anrufern für das Senden von Sprachnachrichten mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  

2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten**  

3. Aktivieren Sie auf der Seite **Automatische UM-Telefonzentrale > Zugriff auf Adressbuch und Vermittlungsstelle** unter **Optionen für das Kontaktieren von Benutzern** das Kontrollkästchen **Anrufer dürfen Sprachnachrichten für Benutzer hinterlassen**, um Anrufern das Hinterlassen von Sprachnachrichten zu ermöglichen. Wenn Sie verhindern möchten, dass Anrufer Sprachnachrichten

hinterlassen, deaktivieren Sie das Kontrollkästchen.

4. Klicken Sie auf **Speichern**.

**NOTE**

Wenn Sie diese Option und die Option **Anrufer dürfen Benutzer wählen** deaktivieren, wird auch **Optionen zum Durchsuchen des Adressbuchs** deaktiviert.

## Verwenden von Exchange Online PowerShell um Anrufer senden Sprachnachrichten oder verhindern, dass sie auf diese Weise zu aktivieren

In diesem Beispiel wird verhindert, dass Anrufer, die mit dem Namen einer UM-Telefonzentrale anrufen `MyUMAutoAttendant` Sprachnachrichten zu senden.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -SendVoiceMsgEnabled $false
```

Dieses Beispiel aktiviert die Anrufer, die mit dem Namen einer UM-Telefonzentrale anrufen `MyUMAutoAttendant` Sprachnachrichten senden.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -SendVoiceMsgEnabled $true
```

# Aktivieren oder Deaktivieren der Verzeichnissuche

18.12.2018 • 3 minutes to read

Sie können Verzeichnissuchen aktivieren, damit Anrufer, die bei einer automatischen Unified Messaging-Telefonzentrale (UM) anrufen, über die Tastatur ihres Telefons Namen im Verzeichnis nachschlagen können, ohne das Verzeichnis mithilfe von Spracheingaben durchsuchen zu können. Diese Einstellung ist standardmäßig aktiviert. Wenn diese Einstellung deaktiviert wird, können Anrufer nicht mithilfe der Tonwahl oder mithilfe von Spracheingaben im Verzeichnis nach einer bestimmten Person suchen.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## NOTE

Outlook Voice Access-Benutzer automatische Spracherkennung Spracherkennung (ASR) oder Spracheingaben verwenden können, um Benutzer in das Verzeichnis zu suchen, können sie nur DTMF- oder Mehrfrequenzwahlverfahren verwenden.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren oder Deaktivieren der Verzeichnissuche mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie aktivieren oder Deaktivieren von Verzeichnissuchen möchten, und klicken Sie dann auf **Bearbeiten**
3. Aktivieren Sie auf der Seite **Automatische UM-Telefonzentrale > Zugriff auf Adressbuch und**

**Vermittlungsstelle** unter **Optionen zum Durchsuchen des Adressbuchs** das Kontrollkästchen neben **Anrufer dürfen Benutzer nach Name oder Alias suchen**, um Anrufern das Suchen nach Benutzern zu ermöglichen. Um Anrufern das Suchen nach Benutzern nicht zu ermöglichen, deaktivieren Sie dieses Kontrollkästchen.

4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren der Verzeichnissuche

Dieses Beispiel deaktiviert die Directory-Lookups auf einem UM-Telefonzentrale mit dem Namen `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -NameLookupEnabled $false
```

# Konfigurieren Sie die Gruppe von Benutzern, die kontaktiert werden können

18.12.2018 • 4 minutes to read

Sie können die Gruppe der Benutzer angeben, die Anrufer erreichen können, wenn sie eine Verbindung mit einer automatischen Unified Messaging-Telefonzentrale (UM) herstellen. Standardmäßig können Anrufer Benutzer innerhalb desselben Satzes Wähleinstellungen kontaktieren, der der automatischen UM-Telefonzentrale zugeordnet ist. Sie können die Gruppierung von Benutzern jedoch ändern, um Anrufern die Übergabe von Anrufen oder das Senden von Sprachnachrichten an Benutzer, die im Adressbuch der Organisation enthalten sind, bzw. an eine bestimmte Auswahl von Benutzern zu ermöglichen.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Verwalten einer automatischen UM-Telefonzentrale](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der Benutzergruppe, die von Anrufern kontaktiert werden kann, mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale, die Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**
3. Treffen Sie auf der Seite **Automatische UM-Telefonzentrale > Zugriff auf Adressbuch und Vermittlungsstelle** unter **Optionen zum Durchsuchen des Adressbuchs** eine Auswahl aus folgenden Optionen:

- **In diesen Wähleinstellungen nur:** Wählen Sie diese Option, um den Anrufer an die automatische Telefonzentrale zu suchen, und wenden Sie sich an Benutzer eine Verbindung zu ermöglichen, die in den Wähleinstellungen die UM-Telefonzentrale zugeordnet sind.
- **In der gesamten Organisation:** Wählen Sie diese Option, ob Anrufer können eine Verbindung herstellen, um die automatische Telefonzentrale zu suchen, und wenden Sie sich an alle Benutzer im Adressbuch der Organisation aufgelistet. Dazu gehören alle Benutzer, die Postfach aktiviert werden.

4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie die Gruppe von Benutzern, die Anrufer wenden können

In diesem Beispiel wird den Bereich der Benutzer, die Anrufer wenden können für alle Benutzer in der Organisation des Adressbuchs auf einer automatischen um-Telefonzentrale mit dem Namen `MyUMAutoAttendant`.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -ContactScope GlobalAddressList
```

# Konfigurieren einer automatischen Telefonzentrale für Benutzer mit ähnlichen Namen

18.12.2018 • 5 minutes to read

In den Optionen **Zugriff auf Adressbuch und Vermittlungsstelle** der automatischen Telefonzentrale können Sie die Methode konfigurieren, die für Benutzer mit ähnlichen Namen verwendet wird, oder Sie können die Standardeinstellung der automatischen Telefonzentrale beibehalten und diese Einstellung in dem Wählplan konfigurieren, der der automatischen Telefonzentrale zugeordnet ist. Standardmäßig kann eine automatische Telefonzentrale zwischen mehreren Benutzern mit demselben oder ähnlichen Namen unterscheiden, weil die Standardeinstellung der automatischen Telefonzentrale **Vererbung von Wählplan** lautet.

## NOTE

Damit die Informationen für Benutzer mit ähnlichen Namen ordnungsgemäß verwendet werden können, müssen Sie den Titel, die Abteilung und Standortinformationen für die Empfänger in Ihrer Microsoft Exchange-Organisation bereitstellen.

Zusätzliche Verwaltungstasks im Zusammenhang mit automatischen UM-Telefonzentralen finden Sie unter [Automatische UM-Telefonzentrale - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren einer automatischen UM-Telefonzentrale für Benutzer mit ähnlichen Namen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  

2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-

Telefonzentrale, die Sie konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**

3. Klicken Sie auf der Seite **Automatische UM-Telefonzentrale** auf **Zugriff auf Adressbuch und Vermittlungsstelle**, und wählen Sie unter **Informationen, die für Benutzer mit demselben Namen eingeschlossen werden** eine der folgenden Optionen aus:

- **Titel:** berücksichtigt die automatische Telefonzentrale Titel des Benutzers, wenn Übereinstimmungen aufgelistet.
- **Abteilung:** berücksichtigt die automatische Telefonzentrale Abteilung des Benutzers, wenn Übereinstimmungen aufgelistet.
- **Speicherort:** berücksichtigt die automatische Telefonzentrale Standort des Benutzers, wenn Übereinstimmungen aufgelistet.
- **None:** die automatischen Telefonzentrale zusätzliche Informationen werden nicht einschließen aus, wenn es Übereinstimmungen enthält.
- **Aufforderung für Alias:** die automatische Telefonzentrale fordert den Anrufer in der Aliasname des Benutzers.
- **Erben aus dem Wählplan:** Verwenden Sie die automatische Telefonzentrale wird die Standardeinstellung aus den Wähleinstellungen die automatische Telefonzentrale zugeordnet.

4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell zum Konfigurieren einer automatischen um-Telefonzentrale für Benutzer mit ähnlichen Namen

In diesem Beispiel wird die Informationen zum Lieferumfang von Benutzern mit ähnlichen Namen zu Prompt für Alias für einen UM-Telefonzentrale mit dem Namen werden .

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -MatchedNameSelectionMethod PromptForAlias
```

In diesem Beispiel wird die Informationen zum Lieferumfang von Benutzern mit ähnlichen Namen an den Titel der Benutzer werden festgelegt, Namenssuche aktiviert und können Anrufer, die wählen in der automatischen Telefonzentrale, drücken \* mit die Begrüßung für Outlook Voice Access für präsentiert werden ein Automatische um-Telefonzentrale mit dem Namen .

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -MatchedNameSelectionMethod Title -NameLookupEnabled $true -StarOutToDialPlanEnabled $true
```

# Einrichten von Voicemail für Benutzer

18.12.2018 • 2 minutes to read

Nachdem Sie Ihr Telefonienetz verbunden oder Microsoft Lync Server in Exchange Unified Messaging (UM) integriert und die erforderlichen UM-Komponenten erstellt und konfiguriert haben, müssen Sie die Voicemailfunktion für Ihre Benutzer einrichten.

Wenn Sie Benutzer für Voicemails aktivieren, müssen Sie die Benutzer mit einer UM-Postfachrichtlinie verknüpfen. UM-Postfachrichtlinien werden verwendet, um gängige Einstellungen auf eine Gruppe von UM-aktivierten Benutzern anzuwenden. Zu diesen Einstellungen gehören PIN-Richtlinien, Beschränkungen für ausgehende Anrufe, mit Nachrichten gesendeter Text und weitere Einstellungen. Sie können entweder die standardmäßige UM-Postfachrichtlinie verwenden oder eine UM-Postfachrichtlinie erstellen und diese gemäß den Anforderungen Ihrer Organisation anpassen.

## Einrichten der Voicemailfunktion für Benutzer

Bevor Sie Benutzer für UM aktivieren, müssen Sie die zu verwendenden Wählplantypen und Durchwahlnummern berücksichtigen und festlegen, welche PIN-Richtlinien, Outlook Web Access-Funktionen und weiteren Funktionen Sie für den Benutzerzugriff konfigurieren möchten. Weitere Informationen finden Sie unter [Voicemail für Benutzer](#).

# UM-Postfachrichtlinien

18.12.2018 • 2 minutes to read

Unified Messaging-Postfachrichtlinien (UM) sind erforderlich, wenn Sie Benutzer für Unified Messaging aktivieren. Sie erstellen UM-Postfachrichtlinien, um einen gemeinsamen Satz an Richtlinien oder Sicherheitseinstellungen auf eine Sammlung von Postfächern von Voicemailbenutzern anzuwenden. UM-Postfachrichtlinien werden wie folgt zum Angeben von UM-Einstellungen verwendet:

- PIN-Richtlinien
- Wähleinschränkungen
- Andere allgemeine Eigenschaften von UM-Postfachrichtlinien

Sie können beispielsweise eine UM-Postfachrichtlinie zum Erhöhen der PIN-Sicherheit erstellen, indem Sie die maximale Anzahl von Anmeldefehlversuchen für eine bestimmte Gruppe von UM-aktivierten Benutzern, z. B. von Führungskräften, verringern.

## UM-Postfachrichtlinien

Mindestens eine UM-Postfachrichtlinie muss erstellt worden sein, ehe Sie Benutzer für Unified Messaging aktivieren können. Sie können zusätzliche UM-Postfachrichtlinien erstellen, um eine gemeinsame Gruppe von Einstellungen auf Benutzergruppen anzuwenden.

Erstellen Sie UM-Postfachrichtlinien mithilfe von Exchange Online PowerShell oder der Exchange-Verwaltungskonsole (EAC). Standardmäßig wird eine einzelne um-Postfachrichtlinie erstellt jedes Mal, wenn Sie einen um-Wählplan erstellen. Neue UM-Postfachrichtlinie automatisch dem um-Wählplan zugeordnet ist, und in den Anzeigenamen des UM-Postfachrichtlinie ist Teil der Wählplanname enthalten. Sie können dieses Standard-UM-Postfachrichtlinie bearbeiten.

Mehrere UM-aktivierte Benutzer können einer einzelnen UM-Postfachrichtlinie zugeordnet sein. Das Postfach jedes UM-aktivierten Benutzers muss jedoch mit einer einzelnen UM-Postfachrichtlinie verknüpft sein. Dadurch können Sie PIN-Sicherheitseinstellungen steuern, z. B. die Mindestanzahl an Stellen einer PIN oder die Höchstanzahl von Anmeldeversuchen für UM-aktivierte Benutzer, die der UM-Postfachrichtlinie zugeordnet sind. Sie können außerdem Nachrichtentexteinstellungen oder Wähleinschränkungen für dieselben UM-aktivierten Postfächer steuern.

# UM-Postfachrichtlinien - Verfahren

18.12.2018 • 2 minutes to read

[Erstellen einer UM-Postfachrichtlinie](#)

[Verwalten einer UM-Postfachrichtlinie](#)

[Löschen einer um-Postfachrichtlinie](#)

# Erstellen einer UM-Postfachrichtlinie

18.12.2018 • 5 minutes to read

Sie können eine Unified Messaging-Postfachrichtlinie (UM) erstellen, um einen allgemeinen Satz von UM-Richtlinieneinstellungen, z. B. PIN-Richtlinieneinstellungen oder Wähleinschränkungen, auf eine Sammlung von UM-aktivierten Postfächern anzuwenden. UM-Postfachrichtlinien verknüpfen einen UM-aktivierten Benutzer mit einer UM-Wähleinstellung und wenden einen allgemeinen Satz von Richtlinien oder Sicherheitseinstellungen auf eine Sammlung von UM-aktivierten Postfächern an. UM-Postfachrichtlinien sind hilfreich beim Anwenden und Standardisieren von Unified Messaging-Konfigurationseinstellungen für UM-aktivierte Benutzer.

Beim Erstellen einer UM-Wähleinstellung wird standardmäßig gleichzeitig eine UM-Postfachrichtlinie erstellt. Nachdem Sie Unified Messaging in Ihrer Organisation bereitgestellt haben, müssen Sie ggf. weitere UM-Postfachrichtlinien erstellen und konfigurieren oder vorhandene UM-Postfachrichtlinien ändern.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Erstellen einer UM-Postfachrichtlinie

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien, neu**.
3. Geben Sie auf der Seite **Neue UM-Postfachrichtlinie** im Feld **Name** den Namen der neuen UM-Postfachrichtlinie ein.

Geben Sie in dieses Feld einen eindeutigen Namen für die UM-Postfachrichtlinie ein. Hierbei handelt es sich um den Anzeigenamen, der in der Exchange-Verwaltungskonsole angezeigt wird. Wenn Sie den Anzeigenamen der UM-Postfachrichtlinie nach dem Erstellen ändern müssen, muss zuerst die vorhandene UM-Postfachrichtlinie gelöscht und dann eine andere UM-Postfachrichtlinie mit dem entsprechenden Namen erstellt werden. Sie können eine UM-Postfachrichtlinie nur löschen, wenn dieser keine UM-aktivierten Benutzer zugeordnet sind.

Der UM-Postfachrichtlinienname ist erforderlich, wird jedoch nur zur Anzeige verwendet. Wenn in Ihrer Organisation mehrere UM-Postfachrichtlinien verwendet werden, empfiehlt sich die Verwendung sinnvoller Namen für die UM-Postfachrichtlinien. Die maximale Länge eines UM-Postfachrichtlinienamens beträgt 64 Zeichen, wobei Leerzeichen enthalten sein dürfen. Er darf jedoch keines der folgenden Zeichen enthalten: "/\[]:;|=,+\*?<>.

4. Klicken Sie auf **Speichern**, um die neue UM-Postfachrichtlinie zu speichern. Wenn Sie die UM-Postfachrichtlinie speichern, werden alle Standardeinstellungen einschließlich PIN-Richtlinien, Voicemailfeatures und Einstellungen für geschützte Voicemail aktiviert. Wenn Sie Standardeinstellungen anpassen oder ändern möchten, verwenden Sie das Cmdlet **Set-UMMailbox**, um die Einstellungen für die UM-Postfachrichtlinie zu ändern, die Sie gerade erstellt haben.

## Verwenden Sie Exchange Online PowerShell, um eine um-Postfachrichtlinie zu erstellen

Dieses Beispiel erstellt eine UM-Postfachrichtlinie mit der Bezeichnung `MyUMMailboxPolicy` Zusammenhang mit einem um-Wählplan mit dem Namen `MyUMDialPlan`.

```
New-UMMailboxPolicy -Name MyUMMailboxPolicy -UMDialPlan MyUMDialPlan
```

# Verwalten einer UM-Postfachrichtlinie

18.12.2018 • 42 minutes to read

Nachdem Sie eine Unified Messaging-Postfachrichtlinie (UM) erstellt haben, können Sie verschiedene Einstellungen anzeigen und konfigurieren. Beispielsweise können Sie UM-Funktionen wie "Voicemailvorschau" oder "Wiedergabe über Telefon" sowie andere, sicherheitsbezogene Optionen wie Einstellungen für geschützte Voicemail und PIN-Richtlinien konfigurieren.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwalten einer UM-Postfachrichtlinie mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** 
  2. Klicken Sie auf der Seite **UM-Wähleinstellungen** klicken Sie unter **UM-Postfachrichtlinien**, klicken Sie auf der Symbolleiste auf **Bearbeiten** 
- Unter **Allgemein** können Sie die Einstellungen für eine UM-Postfachrichtlinie anzeigen und konfigurieren. Beispielsweise können Sie die der UM-Postfachrichtlinie zugeordneten Wähleinstellungen anzeigen oder Benachrichtigungen über verpasste Anrufe für Benutzer, die einer bestimmten UM-Postfachrichtlinie zugeordnet sind, deaktivieren. Wenn Sie die Einstellungen für eine UM-Postfachrichtlinie ändern, gelten die geänderten Einstellungen für alle Benutzer, die der UM-Postfachrichtlinie zugeordnet sind. Sie können folgende Informationen anzeigen oder konfigurieren:
  - **UM-Wähleinstellungen:** Zeigt den Namen des Wählplans UM-Postfachrichtlinie zugeordnet. Dies ist

der Name des Wählplans in Exchange Online PowerShell angezeigt.

Wenn eine neue um-Postfachrichtlinie erstellt wird, müssen sie einen Wählplan zugeordnet werden. Nachdem die um-Postfachrichtlinie erstellt und einem Wählplan zugeordnet ist, gelten die Einstellungen für die Postfachrichtlinie definiert für die Benutzer, die den Wählplan zugeordnet sind. Standardmäßig beim Erstellen eines UM-Wählplans von Exchange Online PowerShell, wird sie auch eine um-Postfachrichtlinie zu erstellen.

- **Name:** Geben Sie den Namen des Wählplans. Ein UM-Wählplanname ist erforderlich und muss eindeutig sein. Es wird jedoch nur für die Anzeige in der Exchange-Verwaltungskonsole und Exchange Online PowerShell verwendet. Wenn Sie den Anzeigenamen des Wählplans ändern haben, nachdem es erstellt wurde, müssen Sie zunächst Löschen der vorhandenen um-Wählplan und erstellen Sie eine andere Wählplan mit dem entsprechenden Namen. Wenn Ihre Organisation mehrere um-Wählpläne verwendet, wird empfohlen, für die Verwendung von aussagekräftigen Names für die um-Wählpläne. Die maximale Länge einer UM-Wählplanname beträgt 64 Zeichen und Leerzeichen enthalten. (Wenn Sie eine mit Microsoft Office Communications Server 2007 R2 Integration haben oder Microsoft Lync Server nicht empfohlen, verwenden Sie Leerzeichen.) Es kann keine jedoch enthalten die folgenden Zeichen: "/\[];|=, + \* ? < >.
- **Grenzwert für persönliche Begrüßung (Minuten):** Verwenden Sie dieses Textfeld, geben Sie die maximale Anzahl von Minuten, die Benutzer, die die um-Postfachrichtlinie zugeordnet sind verwenden können, wenn sie ihre Voicemail-Ansage aufzeichnen. Sie können diese Einstellung ändern, nachdem die um-Postfachrichtlinie erstellt wird. Nur numerische Zeichen sind zulässig. Der gültige Bereich für die Begrüßung ist von 1 bis 10 Minuten. Die Standardeinstellung beträgt 5 Minuten.
- **Voicemailvorschau zulassen:** Aktivieren oder deaktivieren Sie dieses Kontrollkästchen zum Aktivieren oder deaktivieren das Feature Voicemailvorschau für Benutzer, die um-Postfachrichtlinie zugeordnet. Durch Aktivieren dieser Einstellung kann Benutzer den Text einer Voicemailnachricht im Textkörper Nachricht, einer e-Mail oder Textnachricht empfangen. Die Standardeinstellung ist aktiviert.
- **Konfigurieren der Aufruf von mailboxansageregeln durch Benutzer zulassen:** Aktivieren Sie dieses Kontrollkästchen, um zuzulassen, mailboxansageregeln für Benutzer, die zum Erstellen der UM-Postfachrichtlinie zugeordnet sind. Wenn diese Option auf dem um-Wählplan deaktiviert ist, wird nicht dieses Feature für die um-Postfachrichtlinie zugeordnet UM-aktivierten Benutzer verfügbar sein. Die Standardeinstellung ist aktiviert.
- **Zulassen Nachricht wartet Indikator:** Aktivieren oder deaktivieren Sie dieses Kontrollkästchen zum Aktivieren oder Deaktivieren von Message Waiting Indicator für Benutzer, die um-Postfachrichtlinie zugeordnet. Message Waiting Indicator ist ein Feature in die meisten älteren Voicemail-Systemen gefunden. Der am häufigsten verwendeten Form arbeitet er eine Lamp auf das Voice Mail Telefon des Benutzers an, dass das Vorhandensein einer neuen Sprachnachricht. Message Waiting Indicator können auch eine Textnachricht an das Mobiltelefon des UM-aktivierten Benutzers senden. Die Standardeinstellung ist aktiviert.
- **Zulassen von Outlook Voice Access:** Aktivieren oder deaktivieren Sie dieses Kontrollkästchen, um zu aktivieren oder Deaktivieren des Zugriffs auf Outlook Voice Access für UM-aktivierten Benutzer, die dieser UM-Postfachrichtlinie zugeordnet sind. Outlook Voice Access ist ein Feature von UM-aktivierte Benutzer auf ihre Postfächer zugreifen, über ein Telefon verwendet. Diese Einstellung ist standardmäßig aktiviert.
- **Benachrichtigungen über zulassen verpasste Anrufe:** Aktivieren oder deaktivieren Sie dieses Kontrollkästchen zum Aktivieren oder Deaktivieren von Benachrichtigungen über verpasste Anrufe für Benutzer, die um-Postfachrichtlinie zugeordnet. Benachrichtigung über eine verpasste Anrufe ist eine e-Mail-Nachricht an dem Postfach eines Benutzers gesendet, wenn der Benutzer einen eingehenden Anruf nicht beantworten. Dies ist eine andere e-Mail-Nachricht als e-Mail-Nachricht, die die Sprachnachricht Links für einen Benutzer enthält.

**NOTE**

Wenn Sie Unified Messaging und Lync Server lokal integrieren, stehen Benachrichtigungen über verpasste Anrufe nicht für Benutzer zur Verfügung, die über ein Postfach auf einem Exchange 2007- oder Exchange 2010-Postfachserver verfügen. Es wird eine Benachrichtigung über einen verpassten Anruf generiert, wenn ein Benutzer sich abmeldet, bevor der Anruf an Unified Messaging gesendet wurde.

Normalerweise bekommt ein Benutzer zwei E-Mail-Nachrichten, wenn er einen eingehenden Anruf verpasst: eine Nachricht, die die Sprachnachricht enthält, und eine Nachricht, die den Benutzer über den verpassten Anruf informiert. Standardmäßig wird beim Erstellen einer UM-Postfachrichtlinie die Benachrichtigung über verpasste Anrufe aktiviert.

- **Zulassen Wiedergabe über Telefon für Voicemail:** Aktivieren oder deaktivieren Sie dieses Kontrollkästchen zum Aktivieren oder deaktivieren den am Telefon-Feature für Benutzer, die um-Postfachrichtlinie zugeordnet wiedergeben. Diese Option ist standardmäßig aktiviert und ermöglicht es Benutzern, deren Sprachnachrichten über ein beliebiges Telefon, einschließlich eines Büros oder eines Mobiltelefons wiedergegeben werden sollen.
- **Eingehende Faxe zulassen:** Aktivieren oder deaktivieren Sie dieses Kontrollkästchen zum Aktivieren oder deaktivieren eingehende Faxe für Benutzer, die um-Postfachrichtlinie zugeordnet sind. Wenn Sie Benutzer für UM aktivieren, ist ihr Postfach in der Standardeinstellung Faxe empfangen. Jedoch ist diese Option auf dem um-Wählplan deaktiviert, werden UM-aktivierten Benutzer, die die um-Postfachrichtlinie zugeordnet sind, nicht Faxe empfangen. Die Standardeinstellung für die um-Postfachrichtlinie ist deaktiviert.

Nachdem Sie die Einstellung **Eingehende Faxe zulassen** aktiviert haben, müssen Sie den URI des Partnerfaxservers angeben. Falls die UM-Postfachrichtlinie mit einem Wählplan verknüpft ist, der TCP und TLS verwenden kann, müssen Sie URIs sowohl für TCP als auch für TLS eingeben.

- **Microsoft-Hilfe zu verbessern, voicemailvorschau:** mit diesen Optionen können Sie Microsoft, um die Qualität der Voicemailvorschau zu verbessern. Sie können die folgenden Einstellungen aktivieren:
- **Zulassen Analyse der Sprachnachrichten links BSSID:** Verwenden Sie diese Option, um die Qualität der Voicemailvorschau in zukünftigen Versionen von Microsoft Exchange zu verbessern, indem Sie Kopien von Sprachnachrichten an Microsoft zur Analyse weiterleiten. Diese Option kann nicht festgelegt werden, wenn alle Sprachnachrichten geschützt sind.
- **Teilen Sie Anrufer, dass Sprachnachrichten analysiert werden können:** mit dieser Option können Anrufer feststellen, dass die verlassenen Nachrichten von Microsoft zur Verbesserung der Qualität der Voicemailvorschau und ermöglichen es ihnen, die Bestätigung aufgehoben werden analysiert werden können.
- Unter **Nachrichtentext** können Sie die Nachrichtentexteinstellungen für Benutzer konfigurieren, die einer UM-Postfachrichtlinie zugeordnet sind. Sie können beispielsweise den Text der E-Mail-Nachricht festlegen, die an Benutzer gesendet wird, nachdem sie ihre UM-PIN zurückgesetzt haben. Sie können Folgendes konfigurieren:
- **Wenn ein Benutzer für Unified Messaging aktiviert ist:** der Text in das Textfeld eingegeben wird in der E-Mail-Nachricht an Benutzer gesendet, wenn sie für UM aktiviert sind. Wenn das Postfach des Empfängers für UM aktiviert ist und sie für Voicemail aktiviert sind, wird eine E-Mail-Nachricht, die der Benutzer zu Unified Messaging legt, großen Wert auf an den Benutzer gesendet. Dieses Textfeld wird auf 512 Zeichen beschränkt und kann einfache HTML-Formatierung enthalten. Standardmäßig ist kein Text in das Textfeld definiert.

Diese Nachricht enthält Begrüßungstext und die PIN-Informationen, die der Benutzer für den Zugriff auf das Unified Messaging- oder Voicemailsystem verwendet. Der in dieses Textfeld eingegebene Text wird

unten in dieser Begrüßungsnachricht angezeigt. Sie können dieses Textfeld für Informationen wie z. B. die Rufnummern des technischen Supports für Voicemail oder Outlook Voice Access-Nummern verwenden.

Wenn in dieses Textfeld kein Text eingegeben wird, enthält die E-Mail-Nachricht den vom UM- oder Voicemailsysten generierten Standardtext.

In dieses Textfeld eingegebener Text darf unformatiert sein. Er darf auch einfache HTML-Formatierungstags enthalten, wenn Sie Text hervorheben oder Hyperlinks hinzufügen möchten.

**Beispiel 1:** Wenn Sie Fragen oder Vorschläge zu Voice Mail-Dienst verfügen, wenden Sie sich beim Helpdesk zur Erweiterung 4200.

**Beispiel 2:** Wenn Sie Fragen oder Vorschläge zu haben <b>voice Mail-Dienst</b>, wenden Sie sich beim Helpdesk Erweiterung 4200 Rufnummer oder auf unserer Website unter <ein Href = "http://emp.contoso.com/itinfo/vmail"></a>.

- **Wenn Outlook Voice Access-PIN eines Benutzers zurücksetzen ist:** der Text in das Textfeld eingegeben ist enthalten, in der e-Mail-Nachricht an UM-aktivierte Benutzer gesendet, wenn die um-PIN zurückgesetzt wird.

Eine PIN wird vom UM- oder Voicemailsysten zurückgesetzt, falls mehr als 10 (Standardeinstellung) gescheiterte Anmeldeversuche unternommen wurden oder Benutzer ihre PIN mithilfe der UM-Funktionen von Microsoft Outlook, Outlook Web App oder Outlook Voice Access per Telefon selbst zurücksetzen. Sie können dieses Textfeld verwenden, um Informationen wie z. B. Sicherheitshinweise oder andere sicherheitsbezogene Informationen in die E-Mail-Nachricht aufzunehmen.

Wenn in dieses Textfeld kein Text eingegeben wird, enthält die E-Mail-Nachricht den vom UM-System generierten Standardtext.

Die Länge dieses Textfelds ist auf 512 Zeichen begrenzt. In der Standardeinstellung ist in diesem Textfeld kein Text vorhanden.

In dieses Textfeld eingegebener Text darf unformatiert sein. Er darf auch einfache HTML-Formatierungstags enthalten, wenn Sie Text hervorheben oder Hyperlinks hinzufügen möchten.

- **Wenn ein Benutzer eine Sprachnachricht erhält:** der Text in das Textfeld eingegeben ist in der e-Mail-Nachricht an Benutzer gesendet, wenn sie eine Sprachnachricht vom ein Anrufer erhalten enthalten. Dieser Text kann beispielsweise Haftungsausschlüsse enthalten, die Informationen zum Weiterleiten von Sprachnachrichten oder System Sicherheitsrichtlinien, die beschreiben die richtige Methode zum Verarbeiten von Sprachnachrichten in Ihrer Organisation enthalten.

Wenn in dieses Textfeld kein Text eingegeben wird, enthält die E-Mail-Nachricht den vom System generierten Standardtext. Die Länge dieses Textfelds ist auf 512 Zeichen begrenzt. In der Standardeinstellung ist in diesem Textfeld kein Text vorhanden.

In dieses Textfeld eingegebener Text darf unformatiert sein. Er darf auch einfache HTML-Formatierungstags enthalten, wenn Sie Text hervorheben oder Hyperlinks hinzufügen möchten.

- **Wenn ein Benutzer eine Faxnachricht erhält:** der Text in das Textfeld eingegeben ist in der e-Mail-Nachricht an Benutzer gesendet wird, wenn sie eine eingehende Faxnachricht in ihren Posteingang erhalten enthalten. Dieses Textfeld können Sie Haftungsausschlüsse einzubeziehen, die Informationen zum Weiterleiten von Faxnachrichten oder anderen Sicherheitsrichtlinien System über die richtige Methode zum Verarbeiten von Faxnachrichten in Ihrer Organisation enthalten.

Wenn in dieses Textfeld kein Text eingegeben wird, enthält die E-Mail-Nachricht den vom System generierten Standardtext. Die Länge dieses Textfelds ist auf 512 Zeichen begrenzt. In der Standardeinstellung ist in diesem Textfeld kein Text vorhanden.

- Unter **PIN-Richtlinien** können Sie die PIN-Einstellungen für Benutzer konfigurieren, die einer UM-

Postfachrichtlinie zugeordnet sind. UM-PINs ermöglichen es Benutzern, per Telefon auf ihren Posteingang zuzugreifen. Beim Konfigurieren der Einstellungen auf dieser Seite können Sie die Mindestanzahl von Ziffern für eine UM-PIN festlegen und angeben, wie viele Anmeldeversuche scheitern dürfen, bevor das Postfach eines Benutzers gesperrt wird.

Planen Sie die UM-PIN-Richtlinien, die Sie in Ihrer Umgebung implementieren, sehr sorgfältig. Falls Sie keine geeigneten UM-PIN-Richtlinien planen und implementieren, kann dies Sicherheitsbedrohungen zur Folge haben und versehentlich nicht autorisierten Zugriff auf Ihr Netzwerk ermöglichen. Sie können Folgendes konfigurieren:

- **Minimale PIN-Länge (Ziffern):** Verwenden Sie dieses Textfeld die minimale Anzahl von Ziffern angeben, UM der PIN eines Benutzers enthalten kann. Die Standardeinstellung ist sechs Ziffern. Der Bereich liegt zwischen 4 bis 24 Ziffern. Diese Einstellung kann nicht deaktiviert werden.

Wenn Sie die Anzahl der Ziffern erhöhen, die für eine PIN erforderlich ist, steigt auch der Sicherheitsgrad für Ihr UM-System. Wenn Sie die Anzahl der Ziffern verringern, die für eine PIN erforderlich ist, wird der Sicherheitsgrad für Ihr Netzwerk gesenkt. Je weniger Ziffern für eine PIN erforderlich sind, desto einfacher ist es für einen möglichen Angreifer, die PIN eines Benutzers zu erraten.

Wenn die Einstellung zu hoch gewählt wird, können die Benutzer Probleme haben, sich ihre PIN zu merken. Wenn die Einstellung jedoch zu niedrig ist, riskieren Sie nicht autorisierte Zugriffe auf das UM-System.

- **PIN recycle Count:** Verwenden Sie diese Einstellung, um die Anzahl der eindeutigen PINs, die Benutzer festlegen muss verwenden, bevor ein alte PIN wiederverwendet werden kann. In den meisten Unternehmen sollte dieser Wert auf den Standardwert 5, die Anzahl der PINs festgelegt werden, die das System merken wird. PIN-Verlauf kann nicht deaktiviert werden.

Sie können für diese Einstellung einen Wert zwischen 1 und 20 festlegen. Wenn Sie diesen Wert zu niedrig festlegen, kann dies die Benutzer verärgern, weil es schwierig ist, sich so viele PINs zu merken. Wird er zu niedrig festgelegt, kann dies eine Sicherheitsbedrohung für Ihr Netzwerk bedeuten.

- **Zulassen gängiger PIN Muster:** mit dieser Einstellung können Komplexitätsanforderungen für um-PIN festlegen. PIN geändert wird oder neue PINs erstellt werden, werden diese Komplexitätsanforderungen erzwungen.

Wenn diese Option deaktiviert ist, werden Zahlenfolgen, wiederholte Zahlen und das Suffix der Postfachdurchwahl zurückgewiesen. Wenn diese Option aktiviert ist, wird nur das Suffix der Postfachdurchwahl zurückgewiesen.

Als bewährte Sicherheitsmethode wird empfohlen, diese Einstellung zu deaktivieren. Bei Aktivierung dieser Einstellung dürfen Benutzer-PINs Folgendes nicht enthalten:

Zahlenfolgen wie 123456 oder 456789.

Wiederholte Zahlen wie z. B. 111111 oder 8888888.

Suffix der Postfachdurchwahl.

- **Erzwingen PIN-Gültigkeitsdauer (Tage):** Verwenden Sie dieses Textfeld so konfigurieren Sie die Anzahl der Tage, bis die UM-aktivierten Benutzer-PIN läuft ab. Nachdem die PIN läuft ab, muss der Benutzer eine neue um-PIN erstellen. In den meisten Unternehmen sollte dieser Wert auf den Standardwert von 60 Tage festgelegt werden.

Der Wert dieser Einstellung kann zwischen 0 und 999 liegen. Bei der Einstellung 0 sind PINs unbegrenzt gültig. Wenn Sie diesen Wert zu niedrig festlegen, kann dies die Benutzer verärgern, weil sie zu häufig neue PINs erstellen und sich merken müssen.

- **Anzahl der Anmeldung Fehler vor dem PIN zurücksetzen:** Verwenden Sie dieses Textfeld, um die

Nummer des sequenziellen nicht erfolgreichen oder fehlgeschlagenen Anmeldeversuche eingeben, die auftreten können, bevor der UM-Systems automatisch PIN eines Benutzers zurückgesetzt. In den meisten Unternehmen sollte dieser Wert auf den Standardwert 5 Versuche festgelegt werden.

Der Wert dieser Einstellung kann zwischen 0 und 999 liegen. Beim Wert 0 ist die Einstellung deaktiviert, und das System setzt die PINs von Benutzern nicht automatisch zurück. Wird der Wert zu niedrig gewählt, kann dies Verärgerung bei den Benutzern auslösen. Bei einem zu hohen Wert erhalten böswillige Benutzer größere Chancen, die PIN zu ermitteln.

Der Wert dieser Einstellung muss niedriger sein als der Wert der Einstellung **Anzahl der Anmeldefehler vor dem Sperren**. Diese Einstellung kann dazu beitragen, Brute-Force-Angriffe auf Benutzer-PINs abzuwehren.

- **Anzahl der Anmeldung Fehler vor der Sperrung:** Verwenden Sie dieses Textfeld, geben die maximale Anzahl von sequenziellen nicht erfolgreichen oder fehlgeschlagenen Anmeldeversuchen, bevor der Benutzer von ihren Postfächern gesperrt sind.

Wenn ein Benutzer z. B. fünfmal erfolglos versucht, sich bei seinem Postfach anzumelden, setzt das System die PIN des Benutzers basierend auf der Einstellung **Anzahl der Anmeldefehler vor dem Zurücksetzen der PIN** zurück. Versucht der Benutzer wiederum mehr als fünfmal erfolglos, seine neue PIN zu verwenden, setzt das System die PIN erneut zurück. Wenn der Benutzer anschließend nochmals fünfmal erfolglos versucht, seinen neuen PIN zu verwenden, wird das Postfach des Benutzers gesperrt. Nachdem das Postfach des Benutzers gesperrt wurde, muss ein Administrator das Postfach für den Benutzer manuell zurücksetzen oder die Sperre aufheben.

Die Einstellung kann auf einen Wert zwischen 1 und 999 festgelegt werden. Wird der Wert zu niedrig gewählt, kann dies Verärgerung bei den Benutzern auslösen. Bei einem zu hohen Wert erhalten böswillige Benutzer größere Chancen, die PIN zu ermitteln. Bei den meisten Organisationen sollte dieser Wert auf die Standardeinstellung von 15 Versuchen festgelegt werden.

Der angegebene Wert muss größer sein als der Wert der Einstellung **Anzahl der Anmeldefehler vor dem Zurücksetzen der PIN**. Diese Einstellung kann dazu beitragen, Brute-Force-Angriffe auf Benutzer-PINs abzuwehren.

- Unter **Wählautorisierung** können Sie die Wählregeln für UM-aktivierte Benutzer konfigurieren, die dieser UM-Postfachrichtlinie zugeordnet sind.

Mit diesen Einstellungen können Sie die Durchwahlnummern, die erreichbar sind, oder die Telefonnummern steuern, die von UM-aktivierten Benutzern, die der UM-Postfachrichtlinie zugeordnet sind, gewählt werden können. Sie können Folgendes konfigurieren:

- **Anrufe in die gleiche UM-Wählplan:** Aktivieren Sie dieses Kontrollkästchen, um zuzulassen, UM-aktivierten Benutzer, die ein-Abonenten Zugriffsnummer für einen Wählplan konfiguriert und erfolgreich melden Sie sich mit ihrem Postfach zum Tätigen von Anrufen oder Weiterleiten an UM-aktivierten Benutzer, die Erweiterung Zahlen in der gleichen Wählplan. Diese Einstellung ist standardmäßig aktiviert.

Wenn Sie diese Einstellung deaktivieren, können UM-aktivierte Benutzer, die eine in einem Wählplan konfigurierte Abonentenzugriffsnummer anrufen und sich erfolgreich bei ihrem Postfach anmelden, nicht-UM-aktivierte Benutzer oder andere Durchwahlnummern, die keinem UM-aktivierten Benutzer zugeordnet sind, anrufen oder Anrufe an diese weiterleiten. Sie können jedoch keine Anrufe an UM-aktivierte Benutzer weiterleiten, die in der gleichen Wähleinstellung aufgeführt sind. Der Grund dafür ist, dass die Einstellung **Anrufe an jede Durchwahl** standardmäßig aktiviert ist.

- **Anrufe an eine beliebige Erweiterung:** Wenn diese Einstellung aktiviert ist, können Benutzer, rufen Sie eine Teilnehmerzugriffsnummer auf einem Wählplan konfiguriert und erfolgreich melden Sie sich mit ihrem Postfach, Anrufe für Benutzer, die UM-aktivierten, auf andere nicht zugeordnete

Durchwahlnummern sind nicht platzieren mit einem UM-aktivierten Benutzer und für UM-aktivierten Benutzer innerhalb desselben Wählplans. Dies ist, da die **Anrufe in demselben UM-Wählplans** Einstellung standardmäßig aktiviert ist.

Wenn diese Einstellung deaktiviert ist, können Benutzer, die eine in einem Wählplan konfigurierte Outlook Voice Access-Nummer anrufen und sich erfolgreich bei ihrem Postfach anmelden, weder nicht-UM-aktivierte Benutzer noch andere Durchwahlnummern anrufen, die keinem UM-aktivierten Benutzer zugeordnet sind. Sie sind jedoch in der Lage, Anrufe zu tätigen oder Anrufe an Durchwahlnummern, die UM-aktivierten Benutzern zugewiesen sind, weiterzuleiten. Der Grund dafür ist, dass die Einstellung **Anrufe im gleichen UM-Wählplan** standardmäßig aktiviert ist. Die Einstellung **Anrufe an jede Durchwahl** ist standardmäßig aktiviert.

Diese Einstellung kann in einer Umgebung aktiviert werden, in der nicht alle Benutzer UM-aktiviert sind. Sie ist außerdem hilfreich, wenn Sie zulassen möchten, dass Benutzer, die eine in einer Wähleinstellung konfigurierte Outlook Voice Access-Nummer anrufen, Durchwahlnummern anrufen können, die keinem UM-aktivierten Benutzer zugeordnet sind.

- **Autorisierte nationale/regionale Wählregelgruppen:** Verwenden Sie diesen Abschnitt zum Hinzufügen oder Entfernen von nationale/regionale Wählregelgruppen zulässig. Standardmäßig gibt es keine nationale/regionale Wählregelgruppen auf UM-Postfachrichtlinien konfiguriert sind.

Nationale/regionale Wählregelgruppen werden verwendet, um die Rufnummern innerhalb eines Landes oder einer Region, die Benutzer von Outlook Voice Access anrufen können, zuzulassen oder einzuschränken. Diese Maßnahme hilft dabei, unnötige bzw. nicht autorisierte Telefonate und Gebühren zu vermeiden.

Zum Hinzufügen von nationalen/regionalen Wählregelgruppen müssen Sie zunächst die entsprechenden nationalen/regionalen Wählregelgruppen in der Wähleinstellung erstellen, die der UM-Postfachrichtlinie zugeordnet ist, und anschließend der Wählregelgruppe die entsprechenden Wählregeleinträge hinzufügen. Wenn Sie die erforderlichen Wählregelgruppen für den Wählplan erstellt haben, müssen Sie die Wählregelgruppen zur Liste der Wähleinschränkungen unter **Wählautorisierung** für die UM-Postfachrichtlinie hinzufügen.

Mithilfe von nationalen Wählregelgruppen können Sie Unified Messaging in die Lage versetzen, den Zugriff auf Rufnummern in einem Land zuzulassen oder einzuschränken. Dies gilt für Outlook Voice Access-Benutzer, die eine Outlook Voice Access-Nummer angerufen haben.

- **Internationale Wählregelgruppen autorisiert:** Verwenden Sie diesen Abschnitt zum Hinzufügen oder Entfernen von internationale Wählregelgruppen zulässig. Standardmäßig sind gibt es keine internationale Wählregelgruppen auf UM-Postfachrichtlinien konfiguriert.

Zum Hinzufügen von internationalen Wählregelgruppen müssen Sie zunächst die entsprechenden internationalen Wählregelgruppen in der Wähleinstellung erstellen, die der UM-Postfachrichtlinie zugeordnet ist, und anschließend der Wählregelgruppe die entsprechenden Wählregeleinträge hinzufügen. Wenn Sie die erforderlichen Wählregelgruppen erstellt haben, müssen Sie diese den Wähleinschränkungen für die UM-Postfachrichtlinie hinzufügen.

Mithilfe von internationalen Wählregelgruppen können Sie Unified Messaging in die Lage versetzen, den Zugriff auf Rufnummern außerhalb eines Lands oder einer Region zuzulassen oder einzuschränken. Dies findet Anwendung bei Outlook Voice Access-Benutzern, die eine Outlook Voice Access-Nummer angerufen haben.

Internationale Wählregelgruppen werden verwendet, um die Rufnummern außerhalb eines Landes oder einer Region, die Benutzer von Outlook Voice Access anrufen können, zuzulassen oder einzuschränken. Diese Maßnahme hilft dabei, unnötige bzw. nicht autorisierte Telefonate und Gebühren zu vermeiden.

- Unter **Geschützte Voicemail** können Sie die folgenden Einstellungen konfigurieren:

- **Protect Sprachnachrichten von nicht authentifizierten Anrufern zu erfassen:** Wählen Sie eine der folgenden Optionen aus der Dropdownliste, um festzustellen, ob ein eingehender Anruf beantwortet mit Unified Messaging Sprachnachrichten geschützt sind. Diese Einstellung gilt für Sprachnachrichten an UM-aktivierte Benutzer gesendet, wenn sie das Telefon nicht beantwortet. Diese Einstellung gilt auch für VoIP-Nachrichten direkt an UM-aktivierte Benutzer gesendet, wenn der Aufrufer eine automatische um-Telefonzentrale verwendet. Sie können die folgenden konfigurieren:

**None:** mit dieser Einstellung können Sie keinen angewendeten Dokumentschutztyp an alle Sprachnachrichten an UM-aktivierte Benutzer gesendet.

**Privat:** Verwenden Sie diese Einstellung, wenn Sie Schutz nur Sprachnachrichten zuweisen möchten, die vom Anrufer als privat gekennzeichnet wurden.

**Alle:** Verwenden Sie diese Einstellung, wenn Sie auf alle VoIP-Nachrichten, einschließlich der nicht als privat gekennzeichnet Schutz anwenden möchten.

- **Protect Sprachnachrichten von authentifizierten Anrufern zu erfassen:** Wählen Sie eine der folgenden Optionen aus der Dropdownliste, um festzustellen, ob ein eingehender Anruf beantwortet mit Unified Messaging Sprachnachrichten geschützt sind. Diese Einstellung gilt für Sprachnachrichten an UM-aktivierte Benutzer gesendet, wenn sie das Telefon nicht beantwortet. Diese Einstellung gilt auch, wenn Anrufer melden Sie sich mit ihrem Postfach mithilfe von Outlook Voice Access, und klicken Sie dann erstellen und einer Sprachnachricht senden. Sie können die folgenden konfigurieren:

**None:** mit dieser Einstellung können Sie keinen angewendeten Dokumentschutztyp an alle Sprachnachrichten an UM-aktivierte Benutzer gesendet.

**Privat:** Verwenden Sie diese Einstellung, wenn Sie Schutz nur Sprachnachrichten zuweisen möchten, die vom Anrufer als privat gekennzeichnet wurden.

**Alle:** Verwenden Sie diese Einstellung, wenn Sie auf alle VoIP-Nachrichten, einschließlich der nicht als privat gekennzeichnet Schutz anwenden möchten.

- **Erfordern Wiedergabe über Telefon für geschützte Sprachnachrichten:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie Benutzer zu zwingen, die erhalten geschützte Sprachnachrichten wiedergeben Phone-Feature verwenden möchten. Oder, wenn die Clientsoftware Verwaltung von Informationsrechten nicht unterstützt, müssen Benutzer Outlook Voice Access verwenden. Am Telefon wiedergeben gilt nur für Clients, die mit einer Version von Outlook, die Verwaltung von Informationsrechten unterstützt. Für Outlook 2007 und früheren Versionen, die Verwaltung von Informationsrechten nicht unterstützen, und für Outlook Web App-Clients, ist Outlook Voice Access die einzige Möglichkeit, die Benutzer auf geschützte Voicemail überwachen können.

In der Standardeinstellung müssen alle Benutzer, die der UM-Postfachrichtlinie zugeordnet sind, zum Abhören von geschützten Sprachnachrichten die Funktion "Wiedergabe über Telefon" verwenden. Damit wird verhindert, dass die Sprachnachricht mit einem Media Players über Computerlautsprecher oder auf einem Mobiltelefon wiedergegeben wird und dabei von anderen Personen gehört werden kann. Auch wenn diese Option aktiviert ist, können UM-aktivierte Benutzer weiterhin Outlook Voice Access zum Abhören der geschützten Sprachnachricht verwenden.

Dies ist insbesondere dann sinnvoll, wenn UM-aktivierte Benutzer öffentliche Computer, Laptops an öffentlich zugänglichen Orten oder die Medienwiedergabe ihres Mobiltelefons zum Abhören von Sprachnachrichten verwenden, die private Informationen enthalten können.

- **VoIP-Antworten auf e-Mails und Kalender Elemente zulassen:** mit dieser Option können Sie UM-aktivierten Benutzer VoIP Antworten auf geschützte Voicemail-Nachrichten senden können. Der Standardwert ist aktiviert. Wenn Sie deaktivieren, wenn ein UM-aktivierten Benutzer eine geschützte Voicemail-Nachricht empfängt, sie ist nicht möglich, Outlook Voice Access verwenden, um e-Mail-und Kalenderelemente Antworten.

- **Nachricht an Benutzer senden, die nicht über Windows Rights Management unterstützen**

**verfügen:** geschützter Voicemail von e-Mail-Clients, die Information Rights Management (IRM) unterstützen nur zugegriffen werden kann oder wenn ein UM-aktivierten Benutzer Outlook Voice Access verwendet für den Zugriff auf die geschützte Voicemail-Nachricht.

Wird eine geschützte Voicemailnachricht an einen E-Mail-Client ohne IRM-Unterstützung gesendet, erhält der Benutzer eine E-Mail-Nachricht mit dem Text, den Sie in dieses Feld eingeben. Dieser Text sollte erläutern, was der Benutzer tun muss, um die geschützte Voicemailnachricht empfangen zu können.

## Verwenden von Exchange Online PowerShell zum Verwalten einer um-Postfachrichtlinie

In diesem Beispiel wird die PIN-Einstellungen für Benutzer, die mit dem Namen einer UM-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 8 -MaxLogonAttempts 12 -MinPINLength 8 -PINHistoryCount 10 -PINLifetime 60 -ResetPINText "The PIN that is used to allow you access to your mailbox using Outlook Voice Access has been reset."
```

In diesem Beispiel werden die nationalen/regionalen und internationalen Gruppen aus den Gruppen ausgewählt, die für die UM-Wähleinstellungen der UM-Postfachrichtlinie konfiguriert sind. UM-aktivierte Benutzer, die dieser UM-Postfachrichtlinie zugeordnet sind, können ausgehende Anrufe entsprechend den für diese Gruppen definierten Regeln ausführen.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowDialPlanSubscribers $true -AllowedInCountryOrRegionGroups InCountry/RegionGroup1,InCountry/RegionGroup2 -AllowedInternationalGroups InternationalGroup1,InternationalGroup2 -AllowExtensions $true
```

In diesem Beispiel wird der Text von Sprachnachrichten, die an UM-aktivierte Benutzer gesendet werden, sowie der Text der E-Mail-Nachricht konfiguriert, die ein Benutzer nach der UM-Aktivierung erhält.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -UMEnabledText "You have been enabled for Unified Messaging." -VoiceMailText "You have received a voice message from Microsoft Exchange Unified Messaging."
```

## Verwenden Sie Exchange Online PowerShell, um Eigenschaften der Ansicht UM-Postfachrichtlinie

In diesem Beispiel wird eine formatierte Liste aller UM-Postfachrichtlinien in der Active Directory-Gesamtstruktur zurückgegeben.

```
Get-UMMailboxPolicy | Format-List
```

Dieses Beispiel gibt die Eigenschaften und Werte für eine um-Postfachrichtlinie mit der Bezeichnung `MyUMMailboxPolicy`.

```
Get-UMMailboxPolicy -Identity MyUMMailboxPolicy
```

# Löschen einer um-Postfachrichtlinie

18.12.2018 • 2 minutes to read

Wenn eine Unified Messaging-Postfachrichtlinie (UM) gelöscht wird, kann diese UM-Postfachrichtlinie nicht mehr Empfängern zugeordnet werden, die für UM aktiviert sind. Sie können keine UM-Postfachrichtlinie löschen, auf die von UM-aktivierten Postfächern verwiesen wird. Und Sie können einen UM-Wählplan nicht löschen, wenn diesem eine UM-Postfachrichtlinie zugeordnet ist.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

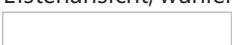
## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Löschen einer UM-Postfachrichtlinie mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** 
2. Klicken Sie auf der Seite **UM-Wähleinstellungen** klicken Sie unter **UM-Postfachrichtlinien**, klicken Sie auf der Symbolleiste auf **Löschen** 

## Verwenden von Exchange Online PowerShell So löschen Sie eine um-Postfachrichtlinie

Dieses Beispiel löscht eine um-Postfachrichtlinie mit der Bezeichnung `MyUMMailboxPolicy`.

```
Remove-UMMailboxPolicy -Identity MyUMMailboxPolicy
```

# Voicemail für Benutzer

18.12.2018 • 15 minutes to read

Mit Unified Messaging (UM) können Benutzer in einer Exchange-Organisation ihre gesamten E-Mail- und Sprachnachrichten in einem einzigen Postfach empfangen. Die Unified Messaging- und Voicemailfunktionen steigern die Benutzerproduktivität erheblich und ermöglichen ein flexibleres Messaging in der gesamten Organisation.

Wenn Sie einen Benutzer in Ihrer Organisation hinzufügen, erhalten Sie die Möglichkeit, erstellen ein Postfach oder ein vorhandenes Postfach den Benutzer verbinden den. Nachdem das Postfach für den Benutzer erstellt oder der Benutzer auf ein vorhandenes Postfach verbunden ist, können Sie das Postfach für Unified Messaging aktivieren, damit der Benutzer das Voicemailsysteem und Voicemail enthaltenen Features verwenden kann. Nachdem der Benutzer für Unified Messaging, alle e-Mail, Voicemail, aktiviert ist und Faxnachrichten an das Postfach des Benutzers übermittelt werden. Mithilfe von Microsoft Office Outlook 2007 oder höher, Outlook Web App, ein Mobiltelefon für Microsoft Exchange ActiveSync oder ein reguläres aktiviert oder Mobiltelefon, können Benutzer ihre e-Mail, Sprachnachrichten, persönliche Kontakte und Kalenderinformationen zugreifen.

## Eigenschaften für Voicemailbenutzer

Ein Benutzer muss ein Postfach verfügen, bevor sie für Unified Messaging aktiviert werden können. Aber standardmäßig ein Benutzer mit einem Postfach ist nicht für Unified Messaging aktiviert. Nachdem der Benutzer UM-aktiviert ist, können verwalten, zu ändern, und konfigurieren Sie die UM-Eigenschaften und voice Mail-Features für diese. Sie können einen Benutzer für Unified Messaging mit der Exchange-Verwaltungskonsole oder Exchange Online PowerShell aktivieren. Weitere Informationen hierzu finden Sie unter [Aktivieren eines Benutzers für Voicemail](#). Um mehrere UM-Benutzer zu aktivieren, verwenden Sie die Exchange-Verwaltungskonsole oder das Cmdlet **Enable-UMMailbox** im Exchange Online PowerShell.

## Beziehung zwischen einem Voicemailbenutzer und anderen UM-Komponenten

Wenn Sie einen Benutzer für Unified Messaging aktivieren, muss der Benutzer zugeordnet oder mit einer vorhandenen UM-Postfachrichtlinie verknüpft werden, und geben Sie für diese eine Durchwahlnummer ein. Sie können einen Benutzer mit einer um-Postfachrichtlinie zuordnen, über das Cmdlet **Enable-UMMailbox** im Exchange Online PowerShell oder, indem Sie die um-Postfachrichtlinie auswählen, wenn Sie den Benutzer für Unified Messaging aktivieren. Standardmäßig wird beim Erstellen eines UM-Wählplans eine neue UM-Postfachrichtlinie erstellt. Diese Richtlinie kann geändert werden, oder eine andere Richtlinie erstellt und zu den Wähleinstellungen, um zu bestimmen, welche Features oder Einstellungen auf einen Benutzer oder eine Gruppe von Benutzern angewendet werden verknüpft werden kann.

Eine um-Postfachrichtlinie enthält Einstellungen für die Einwahl Einschränkungen und PIN-Richtlinien für einen Benutzer. Wenn eine um-Postfachrichtlinie erstellt wird, müssen sie nur ein UM-Wählplan zugeordnet werden. Alle Exchange-Server können eingehende Anrufe entgegennehmen und Bereitstellung von voicemaildiensten für UM-aktivierten Benutzer verknüpft sind mit dem um-Wählplan für VoIP. Nachdem der Benutzer für Unified Messaging aktiviert ist, werden die Einstellungen aus einer um-Postfachrichtlinie für den UM-aktivierten Benutzer angewendet.

## Durchwahlnummern und SIP-Adressen

Wenn Sie einen Benutzer für Unified Messaging aktivieren, müssen Sie mindestens eine Durchwahlnummer

definieren, die von Unified Messaging verwendet wird, wenn Voicemailnachrichten an das Benutzerpostfach übermittelt werden. Nachdem Sie den Benutzer für Unified Messaging aktiviert haben, können Sie dem Benutzerpostfach sekundäre Durchwahlnummern hinzufügen, diese ändern oder entfernen, indem Sie die Exchange Unified Messaging-Proxyadresse (EUM-Proxyadresse) für das Benutzerpostfach konfigurieren oder zusätzliche oder sekundäre Durchwahlnummern für die Benutzer in der Exchange-Verwaltungskonsole hinzufügen oder entfernen. Sie können die primäre Durchwahlnummer in der Exchange-Verwaltungskonsole entfernen, indem Sie die EUM-Proxyadresse entfernen. Es wird jedoch empfohlen, diese Adresse nicht zu entfernen. Das Entfernen der primären Durchwahlnummer führt dazu, dass Anrufe nicht ordnungsgemäß an das Benutzerpostfach weitergeleitet werden können.

#### NOTE

Für die Anzahl von sekundären Durchwahlnummern, die Sie für einen UM-aktivierten Benutzer hinzufügen können, gilt keine Einschränkung, pro Benutzer kann jedoch nur eine primäre Durchwahlnummer angegeben werden.

Das Postfach eines UM-aktivierten Benutzers kann nur einem einzigen Satz UM-Wähleinstellungen zugeordnet werden. Einem UM-aktivierten Benutzer können folgende Elemente zugewiesen werden:

- Eine einzelne primäre Durchwahlnummer, eine SIP-Adresse (Session Initiation Protocol) oder eine E.164-Adresse in einem einzelnen Wählplan.
- Mehrere sekundäre Durchwahlnummern, SIP-Adressen oder E.164-Adressen in einem einzelnen Wählplan.
- Mehrere primäre Durchwahlnummern, SIP-Adressen oder E.164-Adressen in zwei getrennten Wählplänen.

#### NOTE

Jede Durchwahlnummer, SIP-Adresse und E.164-Nummer muss innerhalb eines Wählplans identisch sein, und die Anzahl von Stellen im Wählplan werden für alle Benutzer verwendet, die dem Wählplan zugeordnet sind.

Angenommen, ein UM-aktivierter Benutzer reist häufig von New York nach Tokio. Das Postfach des Benutzers ist dem Satz Wähleinstellungen "New York" zugeordnet, und für das Postfach des Benutzers ist eine einzige Durchwahlnummer konfiguriert. Eine zweite Durchwahlnummer ist für das Postfach des Benutzers für den Satz Wähleinstellungen "Tokio" konfiguriert. Wenn ein Anrufer nun eine dieser Durchwahlnummern wählt und eine Sprachnachricht für den Benutzer hinterlässt, wird diese Sprachnachricht an das gleiche UM-aktivierte Postfach übermittelt.

## Aktivieren eines Benutzers für UM und Voicemail mithilfe der Exchange-Verwaltungskonsole

Nachdem Sie ein Exchange-Postfach für den Benutzer erstellt haben, können Sie die UM-Postfacheinstellungen über **Details anzeigen** unterhalb von **Unified Messaging** in der Exchange-Verwaltungskonsole konfigurieren. Wenn Sie einen Benutzer aktivieren, müssen Sie verschiedene Einstellungen konfigurieren:

1. **SIP-Adresse:** Dies ist die SIP-Adresse für den Benutzer. Diese Einstellung wird angezeigt, wenn der Benutzer, den Sie für UM Aktivieren einer um-Postfachrichtlinie zugeordnet ist, die mit einem SIP-URI-Wählplan verknüpft ist. SIP-URI-Wählpläne werden verwendet, bei der Integration von Office Communications Server 2007 R2 oder Microsoft Lync Server. Wenn Sie den Benutzer zuweisen einer um-Postfachrichtlinie, die mit einem SIP-URI verknüpft ist oder e. 164-Wählplan, müssen Sie auch weiterhin eine Durchwahlnummer für den Benutzer eingeben. Die primäre Durchwahlnummer wird vom Benutzer Zugriff auf Outlook Voice Access verwendet.
2. **Durchwahlnummer:** manuell Geben Sie die Durchwahlnummer für den Benutzer, die Sie für UM aktiviert

sind.

Sie müssen eine gültige Durchwahlnummer für den Benutzer angeben, die mit der in den Wähleinstellungen angegebenen Anzahl von Stellen übereinstimmt. Sie können nur Zahlenwerte von 1 bis 20 eingeben. Eine typische Durchwahlnummer umfasst 3 bis 7 Ziffern und wird in dem Wählplan konfiguriert, der die UM-Postfachrichtlinie zugeordnet ist, die dem Benutzer zugewiesen ist.

### 3. PIN-Einstellungen für den Benutzer:

- **PIN automatisch generieren:** Diese Einstellung automatisch generiert eine PIN für den UM-aktivierten Benutzer für Voice Mail Access über Outlook Voice Access verwenden. Dies ist die Standardeinstellung. Wenn Sie auf diese Schaltfläche klicken, wird automatisch eine PIN generiert basierend auf PIN-Richtlinien auf dem Benutzer zugewiesene UM-Postfachrichtlinie konfiguriert ist. Es wird empfohlen, dass Sie diese Einstellung verwenden, um die PIN des Benutzers zu schützen. Die PIN wird in die Willkommensnachricht an den Benutzer gesendet, die sie erhalten, nachdem sie für UM aktiviert sind. In der Standardeinstellung müssen sie diese PIN ändern, wenn Sie zunächst ihr Postfach Anmeldung ihre Voicemail abrufen.
- **Eine PIN eingeben:** mit dieser Einstellung können Sie manuell eine PIN-Nummer angeben, mit denen Benutzer Zugriff auf das Voice Mail-System.

Die PIN muss den PIN-Richtlinieneinstellungen entsprechen, die in der diesem UM-aktivierten Benutzer zugeordneten UM-Postfachrichtlinie konfiguriert sind. Wenn die UM-Postfachrichtlinie beispielsweise so konfiguriert wurde, dass ausschließlich PINs mit sieben oder mehr Ziffern akzeptiert werden, muss die in diesem Feld eingegebene PIN mindestens sieben Ziffern umfassen.

- **Muss der Benutzer ihre PIN-Nummer der ersten Anmeldung zurückzusetzen:** Diese Einstellung erzwingt, dass den Benutzer ihre Voicemail-PIN zurücksetzen, beim Zugriff auf das Voicemailsyste über ein Telefon mit Outlook Voice Access zum ersten Mal. Sie werden aufgefordert, eine PIN einzugeben, die mehr vertraut ist. Es ist eine bewährte Sicherheitsmethode zu erzwingen, dass UM-aktivierten Benutzer ihre PIN zu ändern, wenn sie zum ersten Mal anmelden zum Schutz gegen unbefugten Zugriff auf ihre Daten und Posteingang. Dieses Kontrollkästchen ist standardmäßig aktiviert.

## Verwenden von Exchange Online PowerShell zum Aktivieren eines Benutzers für UM und Voicemail

In diesem Beispiel wird Unified Messaging und Voice Mail für das Postfach für tony smith@contoso.com ermöglicht, legt die Erweiterung fest und die PIN für den Benutzer manuell festgelegt und dann eine um-Postfachrichtlinie mit dem Namen den Benutzer zugewiesen `MyUMMailboxPolicy`.

```
Enable-UMMailbox -Identity tony smith@contoso.com -UMMailboxPolicy MyUMMailboxPolicy -Extensions 51234 -PIN 5643892 -PINExpired $true
```

In diesem Beispiel wird Unified Messaging und Voice Mail für ein Postfach für tony smith@contoso.com ermöglicht, weist den Benutzer einer um-Postfachrichtlinie mit der Bezeichnung `MyUMMailboxPolicy`, und legt die Durchwahlnummer, SIP-Adresse und manuell die PIN für den Benutzer.

```
Enable-UMMailbox -Identity tony smith@contoso.com -UMMailboxPolicy MyUMMailboxPolicy -Extensions 51234 -PIN 5643892 -SIPResourceIdentifier "tony smith@contoso.com" -PINExpired $true
```

## Deaktivieren von Unified Messaging für einen Benutzer

Wenn Sie Unified Messaging für einen Benutzer deaktivieren, kann das Benutzerkonto immer noch angezeigt werden, wenn ein Anrufer eine Verzeichnissuche über ein Menü der automatischen UM-Telefonzentrale oder unter Verwendung von Outlook Voice Access durchführt. Anrufern ist es eventuell möglich, einen Benutzer im

Verzeichnis zu ermitteln; beim Versuch der Kontaktaufnahme werden sie jedoch zurück zum Hauptmenü in Unified Messaging geleitet. Dies kann Verwirrung stiften und dazu führen, dass Anrufer sich über das System ärgern. Sie können verhindern, dass Anrufer über eine Verzeichnissuche Kontakt zu einem für Unified Messaging deaktivierten Benutzer aufnehmen, indem der Benutzer mit einem anderen Voicemailsysteem verbunden oder aus der Verzeichnissuche der automatischen UM-Telefonzentrale entfernt wird, oder indem das Benutzerkonto entfernt wird.

Nachdem das Konto eines UM-aktivierten Benutzers für Unified Messaging deaktiviert wurde, kann dieser möglicherweise weiterhin mithilfe von Outlook Voice Access oder Microsoft Outlook auf sein persönliches UM-aktiviertes Postfach zugreifen. Dies kann passieren, wenn die Änderungen im Verzeichnis nicht konsistent sind. Um das Risiko zu verringern, dass ein Benutzer Zugriff auf das Postfach erhält, obwohl das Konto für Unified Messaging deaktiviert wurde, können Sie die Replikation manuell erzwingen oder alle Unified Messaging-Informationen aus dem Postfach des Benutzers entfernen, sobald der Benutzer für Unified Messaging deaktiviert ist.

# Voicemail-aktivierter Benutzer – Verfahren

18.12.2018 • 2 minutes to read

[Aktivieren eines Benutzers für Voicemail](#)

[Einschließen von Text mit der e-Mail-Nachricht gesendet, wenn ein Benutzer für Voicemail aktiviert ist](#)

[Verwalten von Voicemail-Einstellungen für einen Benutzer](#)

[Zuweisen einer um-Postfachrichtlinie](#)

[Ändern des um-Wählplans](#)

[Aktivieren von Anrufen nicht UM-aktivierter Benutzer](#)

[Deaktivieren von Anrufen nicht UM-aktivierter Benutzer](#)

[Zulassen einer Sprachnachricht bei Anrufern ohne Anrufer-ID](#)

[Enthalten Sie mit der e-Mail-Nachricht gesendet, wenn eine VoIP-Nachricht empfangen wird text](#)

[Verhindern Sie, dass Anrufer ohne eine Anrufer-ID eine Sprachnachricht hinterlassen](#)

[Deaktivieren von Voicemail für einen Benutzer](#)

[Ändern einer SIP-Adresse](#)

[Ändern einer Durchwahlnummer](#)

[Hinzufügen einer SIP-Adresse](#)

[Entfernen einer SIP-Adresse](#)

[Hinzufügen einer Durchwahlnummer](#)

[Entfernen einer Durchwahlnummer](#)

[Ändern Sie eine e. 164-Nummer](#)

[Hinzufügen einer E.164-Nummer](#)

[Entfernen einer e. 164-Nummer](#)

# Aktivieren eines Benutzers für Voicemail

18.12.2018 • 10 minutes to read

Wenn Sie einen Benutzer für Unified Messaging (UM) aktivieren, wird eine Standardgruppe von Eigenschaften auf den Benutzer angewendet, und der Benutzer ist in der Lage, die Voicemailfunktionen von Unified Messaging zu nutzen. Nachdem Sie einen Benutzer für Voicemail aktiviert haben, können Sie für den Benutzer eine SIP-Adresse (Session Initiation Protocol) hinzufügen, wenn er einem UM-Postfach zugewiesen ist, das mit einem SIP-URI-Wählplan verknüpft ist. Alternativ können Sie eine E.164-Nummer für den Benutzer hinzufügen, wenn er einer UM-Postfachrichtlinie zugewiesen ist, die mit einem E.164-Wählplan verknüpft ist. In beiden Fällen muss für den Benutzer weiterhin eine Durchwahlnummer konfiguriert sein.

Eine Durchwahlnummer ist für jeden Benutzer erforderlich, der einer Telefondurchwahl, einem SIP-URI oder einem E.164-Wählplan zugewiesen ist. Die Durchwahlnummer muss mit der Anzahl der Ziffern übereinstimmen, die in den UM-Wähleinstellungen für die UM-Postfachrichtlinie festgelegt sind.

## NOTE

Sie müssen hinzufügen, entfernen oder Ändern von Durchwahlnummern für alle UM-aktivierten Benutzer mithilfe der Exchange-Verwaltungskonsole oder Exchange Online PowerShell, auch wenn sie einen SIP-URI verknüpft sind oder e. 164-Wählplan. Hinzufügen, entfernen oder Ändern von SIP-Adresse oder e. 164-Rufnummern für Benutzer, müssen Sie Exchange Online PowerShell verwendet werden, da diese Optionen nicht in der Exchange-Verwaltungskonsole verfügbar sind.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren eines Benutzers für Voicemail mithilfe der Exchange-

# Verwaltungskonsole

1. Klicken Sie in der Exchange-Verwaltungskonsole auf **Empfänger**.
2. Wählen Sie in der Listenansicht den Benutzer aus, den Sie für Unified Messaging aktivieren möchten.
3. Klicken Sie im Detailbereich unter **Telefon- und Sprachfunktionen** auf **Aktivieren**.
4. Klicken Sie auf der Seite **UM-Postfach aktivieren** neben **UM-Postfachrichtlinie** auf die Schaltfläche **Durchsuchen**, navigieren Sie zu der UM-Postfachrichtlinie, der Sie den Benutzer aus der Liste zuweisen möchten, und klicken Sie dann auf **OK**.
5. Füllen Sie auf der Seite **UM-Postfach aktivieren** die folgenden Felder aus:
  - **SIP-Adresse oder die e. 164-Nummer:** Geben Sie In das Textfeld **SIP-Adresse** oder die **e. 164-Nummer** der SIP-Adresse oder die e. 164-Nummer für den Benutzer. Diese Optionen sind verfügbar, wenn der Benutzer, den Sie für Unified Messaging aktivieren einer um-Postfachrichtlinie zugeordnet ist, die mit einem SIP-URI oder eine e. 164-Wählplan verknüpft ist. Sie können eine SIP-Adresse oder die e. 164-Nummer für einen Benutzer hinzufügen, wenn der Benutzer eine Telefondurchwahl-Wähleinstellungen zugeordnet ist.

Wenn Sie den Benutzer einer UM-Postfachrichtlinie zuweisen, die mit einem SIP-URI oder E.164-Wählplan verknüpft ist, müssen Sie eine Durchwahlnummer für den Benutzer eingeben. Der Benutzer nutzt diese Durchwahlnummer für den Zugriff auf sein Postfach über Outlook Voice Access. Die Anzahl der in diesem Feld konfigurierten Ziffern muss der Anzahl von Ziffern entsprechen, die für die SIP-URI- oder E.164-Wähleinstellungen konfiguriert ist.
  - **Durchwahlnummer:** Verwenden Sie dieses Textfeld, um manuell die Durchwahlnummer für den Benutzer geben Sie für UM aktiviert sind.

Sie müssen für den Benutzer angeben eine gültige Durchwahlnummer, die mit der im Wählplan angegebenen Anzahl von Ziffern übereinstimmt. Sie können nur Ziffern von 1 bis 20 eingeben. Eine typische Durchwahlnummer hat 3 bis 7 Ziffern. Die Anzahl von Ziffern der Durchwahl ist für den Wählplan festgelegt, der mit dem UM-Postfach verknüpft ist, das dem Benutzer zugewiesen ist.
  - Führen Sie unter **PIN-Einstellungen** folgende Schritte aus:
    - **PIN automatisch generieren:** Klicken Sie auf diese Schaltfläche, um eine PIN für den UM-aktivierten Benutzer für Voice Mail Access über Outlook Voice Access verwendet automatisch generieren. Dies ist die Standardeinstellung. Die PIN wird automatisch generiert basierend auf PIN-Richtlinien auf dem Benutzer zugewiesene UM-Postfachrichtlinie konfiguriert ist. Mit dieser Einstellung hilft bei der der PIN eines Benutzers zu schützen. Die PIN wird in die Willkommensnachricht an den Benutzer gesendet, die sie erhalten, nachdem sie für UM aktiviert sind. In der Standardeinstellung müssen sie diese PIN ändern, wenn Sie zunächst ihr Postfach Anmeldung ihre Voicemail abrufen.
    - **Eine PIN eingeben:** Klicken Sie auf diese Schaltfläche, um eine PIN einzugeben, mit denen Benutzer Zugriff auf das Voice Mail-System. Die PIN-Nummer muss die PIN-Richtlinieneinstellungen auf die um-Postfachrichtlinie dieses UM-aktivierten Benutzer zugeordnet konfiguriert entsprechen. Beispielsweise muss nur PINs akzeptieren, die sieben oder mehr Ziffern enthalten die um-Postfachrichtlinie konfiguriert ist, die PIN, die Sie in dieses Feld eingeben mindestens sieben Ziffern lang sein.
    - **Muss der Benutzer ihre PIN-Nummer der ersten Anmeldung zurückzusetzen:** Aktivieren Sie dieses Kontrollkästchen, um dem Benutzer ihre Voicemail-PIN zurücksetzen, beim Zugriff auf

das Voicemailsystem über ein Telefon mit Outlook Voice Access zum ersten Mal zu erzwingen. Sie werden aufgefordert, eine PIN einzugeben, die mehr vertraut ist. Es ist eine bewährte Sicherheitsmethode zu erzwingen, dass UM-aktivierten Benutzer ihre PIN zu ändern, wenn sie zum ersten Mal anmelden zum Schutz gegen unbefugten Zugriff auf ihre Daten und Posteingang. Dieses Kontrollkästchen ist standardmäßig aktiviert.

6. Überprüfen Sie auf der Seite **UM-Postfach aktivieren** Ihre Einstellungen. Klicken Sie auf **Fertig stellen**, um den Benutzer für Voicemail zu aktivieren. Klicken Sie auf **Zurück**, um Konfigurationsänderungen vorzunehmen.

## Verwenden von Exchange Online PowerShell zum Aktivieren eines Benutzers für Voicemail

In diesem Beispiel wird Unified Messaging für das Postfach von `tonysmith@contoso.com` ermöglicht, die Durchwahlnummer auf 51234 festgelegt, wird die PIN für den Benutzer zu 5643892 und weist den Benutzer einer um-Postfachrichtlinie mit der Bezeichnung `MyUMMailboxPolicy`.

```
Enable-UMMailbox -Identity tonysmith@contoso.com -UMMailboxPolicy MyUMMailboxPolicy -Extensions 51234  
-PIN 5643892 -PINExpired $true
```

In diesem Beispiel wird Unified Messaging für das Postfach von `tonysmith@contoso.com` ermöglicht, weist den Benutzer einer um-Postfachrichtlinie mit der Bezeichnung `MyUMMailboxPolicy`, und die Durchwahlnummer, die SIP-Adresse und die PIN für den Benutzer festgelegt.

```
Enable-UMMailbox -Identity tonysmith@contoso.com -UMMailboxPolicy MyUMMailboxPolicy -Extensions 51234  
-PIN 5643892 -SIPResourceIdentifier "tonysmith@contoso.com" -PINExpired $true
```

# Einschließen von Text mit der e-Mail-Nachricht gesendet, wenn ein Benutzer für Voicemail aktiviert ist

18.12.2018 • 4 minutes to read

Wenn das Postfach eines Benutzers für UM-Voicemail (Unified Messaging) aktiviert wird, wird eine E-Mail-Nachricht gesendet, die den Benutzer bei Unified Messaging begrüßt. Diese Nachricht enthält die PIN-Informationen, die der Benutzer für den ersten Zugriff auf das Voicemailssystem verwendet.

Sie können den Text anpassen, der in der Begrüßungs-E-Mail gesendet wird, indem Sie Text im Textfeld **Wenn ein Benutzer für Unified Messaging aktiviert ist** für eine UM-Postfachrichtlinie eingeben. Sie können Informationen wie z. B. die Rufnummern des technischen Supports für Unified Messaging oder zusätzliche Outlook Voice Access-Nummern einschließen. Nachdem Sie den Text hinzugefügt haben, wird er in jede E-Mail-Nachricht eingefügt, die gesendet wird, wenn der UM-Postfachrichtlinie zugeordnete Benutzer für Unified Messaging aktiviert werden.

## NOTE

Der benutzerdefinierte Text, den Sie der Begrüßungsnachricht hinzufügen, ist auf 512 Zeichen beschränkt und kann einfache HTML-Text umfassen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

Anpassen des beim Aktivieren eines Postfachs für Unified Messaging gesendeten Texts mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  
[redacted]
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten** [redacted].
3. Geben Sie auf der Seite **UM-Postfachrichtlinie > Nachrichtentext** im Textfeld für **Wenn ein Benutzer für Unified Messaging aktiviert ist** den Text ein, der in der E-Mail-Nachricht enthalten sein soll, die beim Aktivieren von Benutzern für Unified Messaging gesendet wird.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell, passen Sie den Text gesendet, wenn ein Postfach für Unified Messaging aktiviert ist

In diesem Beispiel erhalten UM-aktivierte, mit einer UM-Postfachrichtlinie verknüpfte Benutzer die Möglichkeit, weitere Anleitungen zu Unified Messaging und der Rufnummer von Outlook Voice Access, mit der sie per Telefon auf ihre Postfächer zugreifen können, abzurufen.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -UMEEnabledText "You've been enabled for Unified Messaging voice mail. To access your Exchange mailbox, call your internal telephone extension number. From outside your office, call 425-555-1234."
```

# Verwalten von Voicemail-Einstellungen für einen Benutzer

18.12.2018 • 8 minutes to read

Sie können Unified Messaging- und Voicemailfunktionen sowie Konfigurationseinstellungen für einen Benutzer anzeigen und festlegen, der für UM und Voicemail aktiviert wurde. Sie können beispielsweise folgende Aufgaben ausführen:

- Die Outlook Voice Access-PIN eines Benutzers zurücksetzen.
- Die Durchwahlnummer für eine persönliche Vermittlungsstelle hinzufügen.
- Andere Durchwahlnummern hinzufügen.
- Die automatische Spracherkennung (Automatic Speech Recognition, ASR) aktivieren oder deaktivieren.
- Mailboxansagergeln aktivieren oder deaktivieren.
- Den Zugriff auf E-Mails oder Kalender aktivieren oder deaktivieren.

## NOTE

Einige der Features und Einstellungen können nur mithilfe von Exchange Online PowerShell konfiguriert werden.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass der vorhandene Benutzer für Unified Messaging aktiviert ist. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Konfigurieren oder Anzeigen der Eigenschaften eines UM-aktivierten Benutzers mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Wählen Sie in der Listenansicht das Postfach aus, dessen UM-Postfachrichtlinie Sie ändern möchten.
3. Klicken Sie im Detailbereich unter **Telefon- und Sprachfunktionen > Unified Messaging** auf **Details anzeigen**.
4. Klicken Sie auf der Seite **UM-Postfach** auf **UM-Postfacheinstellungen**, um folgende UM-Eigenschaften für einen vorhandenen UM-aktivierten Benutzer anzuzeigen oder zu ändern:
  - **PIN-Status:** dieses reine Anzeigefeld zeigt den Status des Postfach des Benutzers. Wenn ein Benutzer UM-aktiviert wird der PIN-Status wird standardmäßig als **nicht gesperrt**, aufgelistet. Wenn der Benutzer eine falsche Outlook Voice Access-PIN mehrfach eingeben, wird der Status als **Gesperrt** aufgeführt.
  - **UM-Postfachrichtlinie:** Dieses Feld zeigt den Namen des UM-Postfachrichtlinie dem UM-aktivierten Benutzer zugeordnet. Sie können klicken Sie auf **Durchsuchen**, um zu suchen, und geben Sie die um-Postfachrichtlinie dieses UM-Postfach zugeordnet werden soll.
  - **Durchwahl für persönliche Vermittlungsstelle:** in diesem Feld können Sie die Durchwahlnummer Operator für den Benutzer angeben. Standardmäßig ist keine Durchwahlnummer konfiguriert. Die Länge des die Durchwahlnummer kann von 1 bis 20 Zeichen sein. Daher können für eingehende Anrufe für den UM-aktivierten Benutzer an die Durchwahlnummer weitergeleitet werden, die Sie in dieses Feld angeben.  
Für Wähleinstellungen und automatische Telefonzentralen können weitere Typen von Durchwahlnummern für Vermittlungsstellen angegeben werden. Diese Durchwahlnummern gelten jedoch in der Regel für unternehmensweite Telefonvermittlungen. Die Einstellung Durchwahl für persönliche Vermittlungsstelle kann verwendet werden, wenn ein administrativer oder persönlicher Assistent eingehende Anrufe beantwortet, bevor diese für einen bestimmten Benutzer beantwortet werden.
5. Auf der Seite **UM-Postfach** können Sie unter **Andere Durchwahlen** Durchwahlnummern für den Benutzer anzeigen, hinzufügen und ändern.
  - Klicken Sie auf **Hinzufügen**, um eine Durchwahlnummer ein hinzuzufügen,  . Klicken Sie auf der Seite **Fügen Sie eine andere Erweiterung** verwenden Sie **Durchsuchen**, um-Wählplan auszuwählen, und geben Sie die Durchwahlnummer im Feld **Durchwahlnummer ein** .
  - Zum Entfernen einer Durchwahlnummer wählen Sie die Durchwahlnummer an, die Sie entfernen möchten, und klicken Sie dann auf **Entfernen**  .
6. Wenn Sie Änderungen vorgenommen haben, klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell zum Konfigurieren von Features für einen UM-aktivierten Benutzer

In diesem Beispiel werden die Wiedergabe über Telefon und Benachrichtigungen über verpasste Anrufe deaktiviert, Textnachrichten (SMS) werden jedoch aktiviert.

### NOTE

Wenn Sie bei lokalen und Hybridbereitstellungen Unified Messaging und Lync Server integrieren, stehen Benachrichtigungen über verpasste Anrufe nicht für Benutzer zur Verfügung, die über ein Postfach auf einem Exchange 2007- oder Exchange 2010-Postfachserver verfügen. Es wird eine Benachrichtigung über einen verpassten Anruf generiert, wenn ein Benutzer sich abmeldet, bevor der Anruf an einen Postfachserver gesendet wurde.

```
Set-UMMailbox -Identity tony@contoso.com -UMEnabled $true -UMMailboxPolicy AdminPolicy -MissedCallNotificationEnabled $false -PlayOnPhoneEnabled $false -SMSMessageWaitingNotificationEnabled $true
```

In diesem Beispiel wird ein Benutzer am Zugriff auf den Kalender gehindert, es wird jedoch der E-Mail-Zugriff aktiviert, wenn der Benutzer Outlook Voice Access verwendet.

```
Set-UMMailbox -Identity tony@contoso.com -UMEnabled $true -UMMailboxPolicy AdminPolicy -Extension 523456 -FAXEnabled $true -TUIAccessToCal $false -TUIAccessToEmail True
```

In diesem Beispiel wird ein Benutzer am Zugriff auf Kalender und E-Mail gehindert, wenn der Benutzer Outlook Voice Access verwendet.

```
Set-UMMailbox -Identity tony@contoso.com -TUIAccessToCalendarEnabled $false -TUIAccessToEmailEnabled $false
```

In diesem Beispiel wird der Benutzer daran gehindert, Mailboxansageregeln zu erstellen, eingehende Faxe zu empfangen und Outlook Voice Access zu verwenden, die automatische Spracherkennung wird jedoch aktiviert.

```
Set-UMMailbox -Identity tony@contoso.com -AutomaticSpeechRecognitionEnabled $true -CallAnsweringRulesEnabled $false -FaxEnabled $false -SubscriberAccessEnabled $false
```

## Verwenden von Exchange Online PowerShell zum Anzeigen der Eigenschaften eines UM-aktivierten Benutzers

In diesem Beispiel wird eine Liste aller UM-aktivierten Postfächer in der Gesamtstruktur in einer formatierten Liste angezeigt.

```
Get-UMMailbox | Format-List
```

In diesem Beispiel werden die UM-Postfacheigenschaften für "tonysmith@contoso.com" angezeigt.

```
Get-UMMailbox -Identity tonysmith@contoso.com
```

### IMPORTANT

Wenn Sie Exchange 2007 und Exchange 2013 ausführen und das Postfach des Benutzers auf einem Exchange 2007-Postfachserver gespeichert ist, funktioniert das Cmdlet **Get-UMMailbox** nicht ordnungsgemäß. Zur Lösung dieses Problems führen Sie das Cmdlet **Get-UMMailbox** auf einem Exchange 2007-Server oder einem Computer mit den Exchange 2007-Verwaltungstools aus.

# Zuweisen einer um-Postfachrichtlinie

18.12.2018 • 4 minutes to read

Wenn Sie einen Benutzer für Unified Messaging (UM) und Voicemail aktivieren, müssen Sie die UM-Postfachrichtlinie auswählen, die dem Postfach des Benutzers zugeordnet wird. Sie können die UM-Postfachrichtlinie ändern, die dem Postfach des Benutzers zugeordnet ist, nachdem der Benutzer für Unified Messaging aktiviert wurde.

UM-Postfachrichtlinien werden erstellt, um eine allgemeine Zusammenstellung von Richtlinien und Sicherheitseinstellungen auf eine Gruppe von Postfächern UM-aktivierter Benutzer anzuwenden. Mithilfe von UM-Postfachrichtlinien können Sie beispielsweise die folgenden Einstellungen anwenden:

- PIN-Richtlinien
- Wähleinschränkungen
- Andere allgemeine Eigenschaften von UM-Postfachrichtlinien

## NOTE

Standardmäßig wird jedes Mal, wenn Sie einen Satz mit UM-Wähleinstellungen erstellen, eine UM-Postfachrichtlinie erstellt. Abhängig von den Anforderungen Ihrer Organisation können Sie die standardmäßigen UM-Postfachrichtlinien löschen oder zusätzliche UM-Postfachrichtlinien erstellen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass der Benutzer für Unified Messaging aktiviert ist. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern der einem UM-aktivierten Benutzer zugeordneten UM-Postfachrichtlinie mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Wählen Sie in der Listenansicht das Postfach aus, dessen UM-Postfachrichtlinie Sie ändern möchten.
3. Klicken Sie im Detailbereich unter **Telefon- und Sprachfunktionen > Unified Messaging** auf **Details anzeigen**.
4. Klicken Sie auf der Seite **UM-Postfach**, klicken Sie auf **UM-postfacheinstellungen**, und klicken Sie dann auf **Bearbeiten**.
5. Klicken Sie auf der Seite **UM-Postfach** > neben **UM-Postfachrichtlinie**, klicken Sie auf **Durchsuchen**, um die um-Postfachrichtlinie für den Benutzer zu suchen.
6. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so ändern Sie die um-Postfachrichtlinie zu einem UM-aktivierten Benutzer zugewiesen

In diesem Beispiel wird einen UM-aktivierten Benutzer "Tony Smith" mit einer um-Postfachrichtlinie mit der Bezeichnung ordnet **MyUMMailboxPolicy**.

```
Set-UMMailbox -Identity tony.smith@contoso.com -UMMailboxPolicy MyUMMailboxPolicy
```

# Ändern des um-Wählplans

18.12.2018 • 4 minutes to read

Es kann notwendig sein, einen Benutzer, der für Unified Messaging (UM) aktiviert wurde, in einen anderen UM-Wählplan zu verschieben oder die Wähleinstellungen zu ändern, die dem zugeordnet sind. Beispielsweise könnten Sie einen UM-aktivierten Benutzer aus einem Wählerplan mit Telefondurchwählen in einen SIP-URI-Wählplan verschieben.

Zum Ändern des UM-Wählplans müssen Sie den Benutzer für UM deaktivieren und den Benutzer anschließend im neuen UM-Wählplan wieder für UM aktivieren. Dies ist erforderlich, da für verschiedene Wähleinstellungen verschiedene Einstellungen und Anforderungen gelten können, z. B. unterschiedliche Durchwahlängen oder verschiedene URI-Typen. Bei SIP-URI-Wählplänen ist es beispielsweise erforderlich, dass jedem UM-aktivierten Postfach eine SIP-Ressourcen-ID zugewiesen ist, bei Telefondurchwahl-Wähleinstellungen jedoch nicht. Darüber hinaus enthält jedes UM-Postfach Verweise sowohl auf die UM-Wähleinstellungen als auch auf die UM-Postfachrichtlinie. Die UM-Postfachrichtlinie enthält wiederum Verweise auf den UM-Wählplan. Wenn Sie die primäre Proxyadresse für einen UM-aktivierten Benutzer ändern, sodass sie auf andere Wähleinstellungen zeigt, weist das UM-Postfach anschließend einen inkonsistenten Zustand auf.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 10 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass der vorhandene Exchange-Empfänger für Unified Messaging aktiviert ist. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Schritt 1: Erstellen des neuen UM-Wählplans

**IMPORTANT**

Wenn Sie UM-aktivierte Benutzer zu Microsoft Office Communications Server 2007 R2 oder Microsoft Lync Server migrieren, müssen Sie zunächst einen SIP-URI-Wählplan erstellen.

Ausführliche Anweisungen finden Sie unter [Erstellen eines UM-Wählplans](#).

## Schritt 2: Deaktivieren des Benutzers für Unified Messaging

Ausführliche Anweisungen finden Sie unter [Deaktivieren von Voicemail für einen Benutzer](#).

## Schritt 3: Aktivieren des Benutzers für Unified Messaging im neuen UM-Wählplan

**IMPORTANT**

Wenn Sie Benutzer in eine Umgebung mit Office Communications Server 2007 R2 oder Lync Server verschieben, müssen Sie außerdem eine SIP-Ressourcen-ID für den Benutzer angeben, wenn Sie ihn für UM aktivieren. Darüber hinaus müssen Sie die UM-Postfachrichtlinie auswählen, die den SIP-Wähleinstellungen zugeordnet ist.

Ausführliche Anweisungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).

# Aktivieren Sie Anrufe von Benutzern, die UM-aktivierten sind nicht

18.12.2018 • 3 minutes to read

Sie können Anrufe von Benutzern aktivieren bzw. deaktivieren, die nicht für Unified Messaging (UM) aktiviert sind. Standardmäßig erlaubt Unified Messaging eingehende Anrufe von nicht authentifizierten Anrufern über eine automatische Telefonzentrale für UM-aktivierte Benutzer. Wenn diese Option aktiviert ist, können Benutzer außerhalb einer Organisation Anrufe an UM-aktivierte Benutzer weiterleiten.

Wenn diese Einstellung für einen UM-aktivierten Benutzer deaktiviert wurde, kann das Postfach des Benutzers mithilfe einer Verzeichnissuche dennoch ermittelt werden. Wenn ein externer Anrufer jedoch eine Weiterleitung an den Benutzer versucht, gibt das System die automatische Benachrichtigung aus, dass der Anruf nicht an diesen Benutzer weitergeleitet werden kann. Der Anrufer wird dann an die Vermittlungsstelle weitergeleitet, wenn eine solche für die automatische Telefonzentrale konfiguriert ist. Wenn keine Vermittlungsstelle für die automatische Telefonzentrale konfiguriert wurde, wird der Anruf an eine Vermittlungsstelle der Wähleinstellungen umgeleitet, wenn eine solche konfiguriert wurde. Wenn keine Vermittlungsstellendurchwahl für die sprachaktivierte automatische Telefonzentrale, die automatische DTMF-Fallback-Telefonzentrale oder die Wähleinstellungen konfiguriert wurde, gibt das System die automatische Benachrichtigung aus, dass weder die Vermittlungsstelle noch der Tonwahldienst verfügbar sind.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass das Postfach des Benutzers UM-aktiviert wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

Verwenden Sie Exchange Online PowerShell, um Anrufe von Benutzern zu aktivieren, die nicht UM-aktivierten sind

In diesem Beispiel wird Tony Smith gestattet, Anrufe von nicht UM-aktivierten Benutzern zu empfangen.

```
Set UMMailbox -Identity tony@contoso.com -AllowUMCallsFromNonUsers SearchEnabled
```

# Deaktivieren Sie Anrufe von Benutzern, die UM-aktivierten sind nicht

18.12.2018 • 3 minutes to read

Sie können Anrufe von Benutzern aktivieren bzw. deaktivieren, die nicht für Unified Messaging (UM) aktiviert sind. Standardmäßig erlaubt Unified Messaging eingehende Anrufe von nicht authentifizierten Anrufern über eine automatische Telefonzentrale für UM-aktivierte Benutzer. Wenn diese Einstellung aktiviert ist, können Benutzer außerhalb einer Organisation Anrufe an UM-aktivierte Benutzer weiterleiten.

Wenn diese Einstellung für einen UM-aktivierten Benutzer deaktiviert wurde, kann das Postfach des Benutzers mithilfe einer Verzeichnissuche dennoch ermittelt werden. Wenn ein externer Anrufer jedoch eine Weiterleitung an den Benutzer versucht, gibt das System die automatische Benachrichtigung aus, dass der Anruf nicht an diesen Benutzer weitergeleitet werden kann. Der Anrufer wird dann an die Vermittlungsstelle weitergeleitet, wenn eine solche für die automatische Telefonzentrale konfiguriert ist. Wenn keine Vermittlungsstelle für die automatische Telefonzentrale konfiguriert wurde, wird der Anruf an eine Vermittlungsstelle der Wähleinstellungen umgeleitet, wenn eine solche konfiguriert wurde. Wenn keine Vermittlungsstellendurchwahl für die sprachaktivierte automatische Telefonzentrale, die automatische DTMF-Fallback-Telefonzentrale oder die Wähleinstellungen konfiguriert wurde, gibt das System die automatische Benachrichtigung aus, dass weder die Vermittlungsstelle noch der Tonwahldienst verfügbar sind.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass das Postfach des Benutzers UM-aktiviert wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

Verwenden Sie Exchange Online PowerShell, um Anrufe von Benutzern zu deaktivieren, die nicht UM-aktivierten sind

In diesem Beispiel wird Tony Smith daran gehindert, Anrufe von nicht UM-aktivierten Benutzern zu empfangen.

```
Set UMMailbox -Identity tony@contoso.com -AllowUMCallsFromNonUsers None
```

# Zulassen einer Sprachnachricht bei Anrufern ohne Anrufer-ID

18.12.2018 • 3 minutes to read

Sie können es zulassen oder unterbinden, dass UM-aktivierte Benutzer Voicemailnachrichten von anonymen Anrufern empfangen. Wenn Benutzer für Unified Messaging (UM) und Voicemail aktiviert sind, können sie standardmäßig Anrufe empfangen, die anonym sind und keine Anrufer-ID-Informationen enthalten.

In den meisten Fällen enthalten Anrufe, die von Unified Messaging empfangen werden, eine Anrufer-ID, anhand der die Quelle des eingehenden Anrufs bestimmt werden kann. Aus folgenden Gründen ist es jedoch möglich, dass eingehende Anrufe keine Anrufer-ID-Informationen enthalten:

- Die Telefonieausrüstung Ihrer Organisation ist so konfiguriert, dass Anrufer-ID-Informationen nicht eingeschlossen werden.
- Der eingehende Anruf stammt von einem mobilen oder externen Telefon.
- Der Anrufer hat die Anrufer-ID auf seinem Telefon deaktiviert.

Da der Parameter *AnonymousCallersCanLeaveMessages* standardmäßig aktiviert ist, kann ein UM-aktivierten Benutzer eine Sprachnachricht empfangen, auch wenn Anrufer-ID-Informationen nicht enthalten ist. Wenn die Option *AnonymousCallersCanLeaveMessages* ist deaktiviert, und der UM-aktivierten Benutzer erhält einen Anruf, der eine Anrufer-ID umfasst, wird der Anruf als anonyme identifiziert werden, und der UM-aktivierten Benutzer wird keine Sprachnachricht erhalten.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass das Postfach des Benutzers UM-aktiviert wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell, Sprachnachrichten von anonymen Anrufern empfangen werden können

In diesem Beispiel wird es dem UM-aktivierten Benutzer "tonysmith@contoso.com" ermöglicht, Sprachnachrichten von eingehenden Anrufen zu empfangen, die keine Anrufer-ID-Informationen einschließen.

```
Set-UMMailbox -Identity tony.smith@contoso.com -AnonymousCallersCanLeaveMessages $true
```

# Enthalten Sie mit der e-Mail-Nachricht gesendet, wenn eine VoIP-Nachricht empfangen wird text

18.12.2018 • 4 minutes to read

Sie können zur E-Mail-Nachricht, die beim Empfang einer Voicemailnachricht durch für Unified Messaging (UM) aktivierte Benutzer gesendet wird, zusätzlichen Text hinzufügen. Standardmäßig gibt der E-Mail-Nachrichtentext beim Empfang einer Sprachnachricht nur an, dass der Benutzer eine Sprachnachricht empfangen hat. Sie können jedoch auch eine benutzerdefinierte Nachricht durch Hinzufügen von Text im Textfeld **Wenn ein Benutzer eine Sprachnachricht empfängt** für eine UM-Postfachrichtlinie erstellen. Dieser Text kann z. B. Informationen zu Systemsicherheitsrichtlinien enthalten und das ordnungsgemäße Verfahren für den Umgang mit Sprachnachrichten in Ihrer Organisation beschreiben. Nachdem Sie den Text hinzugefügt haben, wird dieser jeder E-Mail-Nachricht hinzugefügt, die gesendet wird, wenn der UM-Postfachrichtlinie zugeordnete UM-aktivierte Benutzer eine Sprachnachricht empfangen.

## NOTE

Der benutzerdefinierte Text, der eine Sprachnachricht begleitet, darf maximal 512 Zeichen lang sein und kann einfache HTML-Text enthalten.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern des E-Mail-Nachrichtentexts beim Empfang einer Sprachnachricht mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

- [ ]
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-  
Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten** [ ].
  3. Geben Sie auf der Seite **UM-Postfachrichtlinie > Nachrichtentext** in das Textfeld **Wenn ein Benutzer  
eine Sprachnachricht empfängt** den Text der E-Mail-Nachricht ein, die gesendet wird, wenn Benutzer  
eine Sprachnachricht empfangen.
  4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so ändern Sie den in einer Sprachnachricht eingeschlossen text

In diesem Beispiel wird den zusätzlichen Text enthält, die an Benutzer, die mit dem Namen der UM-  
Postfachrichtlinie zugeordnet sind gesendet "Nicht Sprachnachrichten für Benutzer außerhalb der Organisation,  
mit Sprachnachrichten weiterleiten" [ **MyUMMailboxPolicy** ].

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -VoiceMailText "Do not forward voice messages to users outside  
this organization."
```

# Verhindern Sie, dass Anrufer ohne eine Anrufer-ID eine Sprachnachricht hinterlassen

18.12.2018 • 3 minutes to read

Sie können es zulassen oder unterbinden, dass UM-aktivierte Benutzer Sprachnachrichten von anonymen Anrufern empfangen. Wenn Benutzer für Unified Messaging (UM) und Voicemail aktiviert sind, können sie standardmäßig Anrufe empfangen, die anonym sind und keine Anrufer-ID-Informationen enthalten.

In den meisten Fällen enthalten Anrufe, die von Exchange-Servern empfangen werden, eine Anrufer-ID, anhand der die Quelle des eingehenden Anrufs bestimmt werden kann. Aus folgenden Gründen ist es jedoch möglich, dass eingehende Anrufe keine Anrufer-ID-Informationen enthalten:

- Die Telefonieausrüstung Ihrer Organisation ist so konfiguriert, dass Anrufer-ID-Informationen nicht eingeschlossen werden.
- Der eingehende Anruf stammt von einem mobilen oder externen Telefon.
- Der Anrufer hat die Anrufer-ID auf seinem Telefon deaktiviert.

Da der Parameter *AnonymousCallersCanLeaveMessages* standardmäßig aktiviert ist, kann ein UM-aktivierten Benutzer eine Sprachnachricht empfangen, auch wenn Anrufer-ID-Informationen nicht enthalten ist. Wenn die Option *AnonymousCallersCanLeaveMessages* ist deaktiviert, und der UM-aktivierten Benutzer erhält einen Anruf, der eine Anrufer-ID umfasst, wird der Anruf als anonyme identifiziert werden, und der UM-aktivierten Benutzer wird keine Sprachnachricht erhalten.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass das Postfach des Benutzers UM-aktiviert wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um zu verhindern, dass von anonymen Anrufern Sprachnachrichten empfangen werden

In diesem Beispiel wird unterbunden, dass der UM-aktivierte Benutzer "tonysmith@contoso.com" Sprachnachrichten von Anrufen empfängt, die keine Anrufer-ID-Informationen einschließen.

```
Set-UMMailbox -Identity tonysmith@contoso.com -AnonymousCallersCanLeaveMessages $false
```

# Deaktivieren von Voicemail für einen Benutzer

18.12.2018 • 3 minutes to read

Sie können die Unified Messaging (UM) für einen UM-aktivierten Benutzer deaktivieren. Wenn Sie dies tun, kann der Benutzer die Voicemailfunktionen in Unified Messaging nicht mehr verwenden. Wenn Sie bevorzugen, wenn Sie, UM für einen Benutzer deaktivieren, können Sie die UM-Einstellungen für den Benutzer belassen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass der vorhandene Benutzer für Unified Messaging aktiviert ist. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Deaktivieren von Unified Messaging und Voicemail für einen Benutzer mithilfe der Exchange-Verwaltungskonsole

1. Klicken Sie in der Exchange-Verwaltungskonsole auf **Empfänger**.
2. Wählen Sie in der Listenansicht den Benutzer aus, dessen Postfach für Unified Messaging deaktiviert werden soll.
3. Klicken Sie im Detailbereich unter **Telefon- und Sprachfunktionen** unter **Unified Messaging** auf **Deaktivieren**.
4. Klicken Sie im Dialogfeld mit der Warnung\*\*\*\* auf **Ja**, um zu bestätigen, dass Unified Messaging für diesen Benutzer deaktiviert wird.

Verwenden Sie Exchange Online PowerShell, um Unified Messaging und Voice Mail für einen Benutzer zu deaktivieren

In diesem Beispiel werden Unified Messaging und Voicemail für "tonysmith@contoso.com" deaktiviert, die UM-Postfacheinstellungen werden jedoch beibehalten.

```
Disable-UMMailbox -Identity tonysmith@contoso.com -KeepProperties $True
```

# Ändern einer SIP-Adresse

18.12.2018 • 6 minutes to read

Wenn Sie einen Benutzer für UM aktivieren und ihn mit einem SIP-URI-Wählplan verknüpfen, werden zwei EUM-Proxyadressen erstellt. Eine enthält die Durchwahlnummer des Benutzers, und die andere enthält die SIP-Adresse für den Benutzer. Die Durchwahlnummer wird verwendet, wenn der Benutzer eine Outlook Voice Access-Nummer anruft.

SIP-URI-Wählpläne und SIP-Adressen werden verwendet, wenn Sie UM und Office Communications Server 2007 R2 oder Microsoft Lync Server integrieren. Die SIP-Adresse wird von Communications Server oder Lync Server zum Weiterleiten eingehender Anrufe und zum Senden von Voicemail an den Benutzer verwendet. Die von UM verwendete SIP-Adresse ist standardmäßig die von Communications Server oder Lync Server verwendete SIP-Adresse.

Sie können die primäre SIP-Adresse, die beim Aktivieren des Benutzers für UM hinzugefügt wurde, oder eine sekundäre SIP-Adresse, die später zusammen mit der EUM-Proxyadresse für den Benutzer hinzugefügt wurde, ändern. Die primäre SIP-Adresse, die Sie beim Aktivieren des Benutzers für UM hinzugefügt haben, wird als primäre EUM-Proxyadresse aufgeführt. Weitere von Ihnen hinzugefügte sekundäre SIP-Adressen werden als sekundäre EUM-Proxyadressen aufgeführt. Wenn sekundäre SIP-Adressen geändert werden, können Anrufer an allen SIP-Endpunkten, bei denen der Benutzer angemeldet ist, über die neuen SIP-Adressen eine Voicemail für den Benutzer hinterlassen. Alle Sprachnachrichten werden an das Postfach des gleichen Benutzers zugestellt.

Der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell können Sie um einen primären oder sekundären SIP-Adresse zu ändern. Die Seite **E-Mail-Adresse** können für das Postfach des Benutzers in der Exchange-Verwaltungskonsole Sie einem primären oder sekundären SIP-Adresse ändern. Die Seite **UM-Postfach** können in der Exchange-Verwaltungskonsole Sie um eine primäre oder sekundäre SIP-Adresse zu ändern.

Sie können die primäre und sekundäre SIP-Adresse für einen Benutzer über das Cmdlet **Get-UMMailbox** oder das Cmdlet **Get-Mailbox** in Exchange Online PowerShell anzeigen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein SIP-URI-UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass der vorhandene Benutzer für UM aktiviert wurde und mit einem SIP-URI-Wählplan verknüpft ist. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass die SIP-Adresse, die dem Benutzer zugewiesen werden soll, gültig und richtig formatiert ist.

- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern der primären oder einer sekundären SIP-Adresse mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Listenansicht, wählen Sie das Postfach, für die Sie eine SIP-Adresse ändern möchten, und klicken Sie dann auf **Bearbeiten** .
3. Auf der Seite **Benutzerpostfach** unter **E-Mail-Adresse**, wählen Sie die SIP-Adresse, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** . Die primäre SIP-Adresse ist in **fett** und **Zahlen** aufgeführt.
4. Geben Sie auf der Seite **E-Mail-Adresse** im Feld **Adresse/Durchwahl** die neue SIP-Adresse für den Benutzer ein, und klicken Sie dann auf **OK**. Wenn Sie einen neuen UM-Wählplan auswählen müssen, können Sie auf **Durchsuchen** klicken.
5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so ändern Sie die primäre und sekundäre SIP-Adresse

In diesem Beispiel wird eine SIP-Adresse für Tony Smith geändert.

#### NOTE

Bevor Sie eine SIP-Adresse von Exchange Online PowerShell ändern, müssen Sie die Position der EUM Proxy-Adresse zu ermitteln, die Sie ändern möchten. Verwenden Sie zum Bestimmen der Position der **\$mbx. EmailAddresses** Befehl. Die erste EUM Proxyadresse ist die Standardeinstellung (primären) SIP-Adresse, und es werden 0 in der Liste.

```
$mbx=Get-Mailbox tony.smith  
$mbx.EmailAddresses.Item(1)="eum:tsmith@contoso.com;phone-context=MySIPDialPlan.contoso.com"  
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

# Ändern einer Durchwahlnummer

18.12.2018 • 6 minutes to read

Wenn Sie einen Benutzer für UM aktivieren und mit einem Wählplan vom Typ "Telefondurchwahl" verknüpfen, wird für den Benutzer eine Exchange Unified Messaging-Proxyadresse (EUM) erstellt, die die Durchwahlnummer des Benutzers enthält. Sie müssen mindestens eine Durchwahlnummer für UM definieren, damit Voicemail an das Postfach des Benutzers gesendet werden kann. Die Durchwahlnummer wird auch verwendet, wenn der Benutzer eine Outlook Voice Access-Nummer anruft.

Sie können die primäre Durchwahlnummer ändern, die hinzugefügt wurde, als der Benutzer für UM aktiviert wurde. Oder Sie können die sekundäre Durchwahlnummer, die später hinzugefügt wurde, zusammen mit den EUM-Proxyadressen des Benutzers entfernen. Die primäre Durchwahlnummer, die hinzugefügt wurde, als der Benutzer für UM aktiviert wurde, wird als primäre EUM-Proxyadresse aufgelistet. Weitere hinzugefügte sekundäre Durchwahlnummern werden als sekundäre EUM-Proxyadressen aufgelistet. Nachdem weitere Durchwahlnummern hinzugefügt wurden, können Anrufer Voicemail für den Benutzer an allen neu eingerichteten Durchwahlnummern hinterlassen. Alle Sprachnachrichten werden an dasselbe Postfach des Empfängers zugestellt.

Der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell können Sie eine primäre oder eine sekundäre Durchwahlnummer für einen Benutzer ändern. Die Seite **E-Mail-Adresse** können für das Postfach des Benutzers in der Exchange-Verwaltungskonsole Sie einen primären oder sekundären Durchwahlnummer ändern. Sie können die Seite **UM-Postfach** in der Exchange-Verwaltungskonsole eine primäre Durchwahlnummer ändern, jedoch können Sie sie so ändern Sie einen sekundären Durchwahlnummer ein. Wenn Sie einen sekundären Durchwahlnummer ändern möchten, müssen Sie zuerst die vorhandenen sekundären Durchwahlnummer entfernt und fügen Sie die richtigen sekundären Durchwahlnummer für den Benutzer.

Sie können die primäre und sekundäre Durchwahlnummern für einen Benutzer mit dem Cmdlet **Get-UMMailbox**, oder das Cmdlet **Get-Mailbox** in Exchange Online PowerShell anzeigen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-Wählplan für Telefondurchwahlnummern erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass das Postfach des Benutzers UM-aktiviert und mit einem Wählplan vom Typ "Telefondurchwahl" verknüpft wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass die Durchwahlnummer, die dem Benutzer zugewiesen wird, die richtige, im UM-Wählplan festgelegte Anzahl von Ziffern aufweist.

- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern der primären oder sekundären Durchwahlnummer über die Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Listenansicht, wählen Sie das Postfach, für die Sie eine Durchwahlnummer ändern möchten, und klicken Sie dann auf **Bearbeiten** [ ].
3. Auf der Seite **Benutzerpostfach** unter **E-Mail-Adresse**, wählen Sie die Durchwahlnummer an, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** [ ]. Die primäre Durchwahlnummer wird in fett und Zahlen aufgeführt.
4. Wählen Sie auf der Seite **E-Mail-Adresse** die Option **Adresse/Erweiterung** aus, und geben Sie die neue Durchwahlnummer für den Benutzer ein. Wenn Sie einen neuen UM-Wählplan auswählen müssen, klicken Sie auf **Durchsuchen**.
5. Klicken Sie auf **Speichern**.

## Verwenden Sie Exchange Online PowerShell, um den primären oder sekundären Durchwahlnummer ändern

In diesem Beispiel wird die Durchwahlnummer 22222 für den UM-aktivierten Benutzer Tony Smith geändert.

#### NOTE

Bevor Sie eine Durchwahlnummer von Exchange Online PowerShell ändern, müssen Sie die Position der EUM Proxy-Adresse zu ermitteln, die Sie ändern möchten. Verwenden Sie zum Bestimmen der Position der **\$mbx. EmailAddresses** Befehl. Die erste EUM Proxyadresse ist die Standardnummer (primäre) Erweiterung, und es werden 0 in der Liste.

```
$mbx=Get-Mailbox tony.smith  
$mbx.EmailAddresses.Item(0)="eum:22222;phone-context=MyDialPlan.contoso.com"  
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

# Hinzufügen einer SIP-Adresse

18.12.2018 • 6 minutes to read

Wenn Sie einen Benutzer für UM aktivieren und ihn mit einem SIP-URI-Wählplan verknüpfen, werden zwei EUM-Proxyadressen erstellt. Eine enthält die Durchwahlnummer des Benutzers, und die andere enthält die SIP-Adresse für den Benutzer. Die Durchwahlnummer wird verwendet, wenn der Benutzer eine Outlook Voice Access-Nummer anruft.

SIP-URI-Wählpläne und SIP-Adressen werden verwendet, wenn Sie UM und Office Communications Server 2007 R2 oder Microsoft Lync Server integrieren. Die SIP-Adresse wird von Communications Server oder Lync Server zum Weiterleiten eingehender Anrufe und zum Senden von Voicemail an den Benutzer verwendet. Die von UM verwendete SIP-Adresse ist standardmäßig die von Communications Server oder Lync Server verwendete SIP-Adresse.

Die primäre SIP-Adresse, die Sie beim Aktivieren des Benutzers für UM hinzugefügt haben, wird als primäre EUM-Proxyadresse aufgeführt. Wenn die primäre SIP-Adresse entfernt wurde, wird die erste von Ihnen hinzugefügte EUM-Proxyadresse, die die SIP-Adresse des Benutzers enthält, als primäre EUM-Proxyadresse aufgeführt. Weitere von Ihnen hinzugefügte SIP-Adressen werden als sekundäre EUM-Proxyadressen aufgeführt. Wenn sekundäre SIP-Adressen hinzugefügt werden, können Anrufer an SIP-Endpunkten, bei denen der Benutzer angemeldet ist, über die SIP-Adressen eine Voicemail für den Benutzer hinterlassen. Alle Sprachnachrichten werden an das Postfach des gleichen Benutzers zugestellt.

Der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell können Sie einen primären oder sekundären SIP-Adresse für einen Benutzer hinzufügen. Die Seite **E-Mail-Adresse** können auf das Postfach des Benutzers in der Exchange-Verwaltungskonsole Sie eine primäre oder sekundäre SIP-Adresse hinzufügen. Sie können nicht die Seite **UM-Postfach** in der Exchange-Verwaltungskonsole zum Hinzufügen einer primären oder sekundären SIP-Adresse verwenden.

Sie können die primäre und sekundäre SIP-Adresse für einen Benutzer über das Cmdlet **Get-UMMailbox** oder das Cmdlet **Get-Mailbox** in Exchange Online PowerShell anzeigen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein SIP-URI-UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass der vorhandene Benutzer für UM aktiviert wurde und mit einem SIP-URI-Wählplan verknüpft ist. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass die SIP-Adresse, die dem Benutzer

zugewiesen werden soll, gültig und richtig formatiert ist.

- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Hinzufügen einer primären oder sekundären SIP-Adresse mit der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Listenansicht, wählen Sie das Postfach, für die Sie eine SIP-Adresse hinzufügen möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Benutzerpostfach** unter **E-Mail-Adresse Hinzufügen**.
4. Wählen Sie auf der Seite **Neue E-Mail-Adresse** die Option **EUM** aus, und geben Sie im Feld **Adresse/Durchwahl** die neue SIP-Adresse für den Benutzer ein.
5. Klicken Sie auf der Seite **Neue E-Mail-Adresse** unter **Wählplan** auf **Durchsuchen**, um einen SIP-URI-Wählplan auszuwählen, und klicken Sie dann auf **OK**.
6. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell, eine SIP-Adresse hinzufügen

In diesem Beispiel wird eine SIP-Adresse für den UM-aktivierten Benutzer Thorsten Scholl hinzugefügt.

#### NOTE

Bevor Sie eine SIP-Adresse von Exchange Online PowerShell hinzufügen, müssen Sie die Position der EUM Proxy-Adresse zu ermitteln, die Sie hinzufügen möchten. Verwenden Sie zum Bestimmen der Position der \$mbx. **EmailAddresses** Befehl. Die erste Proxyadresse in der Liste wird 0 sein.

```
$mbx=Get-Mailbox tony.smith  
$mbx.EmailAddresses +="eum:tsmit@contoso.com;phone-context=MyDialPlan.contoso.com"  
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

# Entfernen einer SIP-Adresse

18.12.2018 • 7 minutes to read

Wenn Sie einen Benutzer für UM aktivieren und ihn einem SIP-URI-Wählplan zuweisen, werden zwei Exchange Unified Messaging-Proxyadressen (EUM) erstellt. Eine enthält die Durchwahlnummer des Benutzers, die andere seine SIP-Adresse. Die Durchwahlnummer wird verwendet, wenn der Benutzer eine Outlook Voice Access-Nummer anruft.

SIP-URI-Wählpläne und SIP-Adressen werden verwendet, wenn Sie UM und Office Communications Server 2007 R2 oder Microsoft Lync Server integrieren. Die SIP-Adresse wird von Communications Server oder Lync Server zum Weiterleiten eingehender Anrufe und zum Senden von Voicemail an den Benutzer verwendet. Die von UM verwendete SIP-Adresse ist standardmäßig die von Communications Server oder Lync Server verwendete SIP-Adresse.

Sie können die primäre SIP-Adresse entfernen, die hinzugefügt wurde, als der Benutzer für UM aktiviert wurde. Oder Sie können die sekundäre SIP-Adresse, die später hinzugefügt wurde, zusammen mit den EUM-Proxyadressen des Benutzers entfernen. Die primäre SIP-Adresse, die hinzugefügt wurde, als der Benutzer für UM aktiviert wurde, wird als primäre EUM-Proxyadresse aufgelistet. Weitere hinzugefügte SIP-Adressen werden als sekundäre EUM-Proxyadressen aufgelistet. Wenn eine SIP-Adresse entfernt wird, können Anrufer keine Voicemail mehr für den Benutzer an der SIP-Adresse hinterlassen, die entfernt wurde, auch wenn der Benutzer mit der SIP-Adresse angemeldet ist, die dem Benutzer Communications Server oder Lync Server zugewiesen wurde.

Wenn Sie die primäre SIP-Adresse entfernen möchten, werden nicht UM zum Senden von Voicemail Postfach des Benutzers und das Anrufen, die antwortende Regeln werden nicht verarbeitet werden. Nachdem die primäre SIP-Adresse entfernt wurde, wird die EUM-Proxy-Adresse für den Benutzer als **Null** auf das Postfach des Benutzers in der Exchange-Verwaltungskonsole und wenn Sie das Cmdlet **Get-Mailbox** in Exchange Online PowerShell führen aufgeführt. Auch, wenn Sie das Cmdlet **Get-UMMailbox** ausführen, werden die Parameter *Extensions*, *\_PhoneNumber* und *CallAnsweringRulesExtensions* leer oder null sein.

Der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell können Sie um einem primären oder sekundären SIP-Adresse zu entfernen. Die Seite **E-Mail-Adresse** können für das Postfach des Benutzers in der Exchange-Verwaltungskonsole Sie um einem primären oder sekundären SIP-Adresse zu entfernen. Sie können nicht die Seite **UM-Postfach** in der Exchange-Verwaltungskonsole verwenden, um einen primären oder sekundären SIP-Adresse zu entfernen.

Sie können die primäre und sekundäre SIP-Adresse für einen Benutzer über das Cmdlet **Get-UMMailbox** oder das Cmdlet **Get-Mailbox** in Exchange Online PowerShell anzeigen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass das Postfach des Benutzers UM-aktiviert

und mit einem Wählplan vom Typ "SIP-URI" verknüpft wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).

- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass die primäre oder sekundäre SIP-Adresse für den Benutzer konfiguriert sind.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Entfernen der primären oder sekundären SIP-Adresse mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Listenansicht, wählen Sie das Postfach aus der Sie eine SIP-Adresse entfernen möchten, und klicken Sie dann auf **Bearbeiten**
3. Klicken Sie auf der Seite **Postfach des Benutzers**, klicken Sie unter **E-Mail-Adresse**, wählen Sie die SIP-Adresse, die Sie aus der Liste entfernen möchten, und klicken Sie dann auf **Löschen** . Die primäre EUM Proxy-Adresse oder SIP-Adresse ist in fett und Zahlen aufgeführt.
4. Klicken Sie auf **Speichern**.

## Verwenden Sie Exchange Online PowerShell, um den primären oder sekundären SIP-Adresse zu entfernen.

In diesem Beispiel wird die SIP-Adresse "tsmith@contoso" aus dem Postfach des UM-aktivierten Benutzers Tony Smith entfernt.

#### NOTE

Bevor Sie eine SIP-Adresse von Exchange Online PowerShell entfernen, müssen Sie die Position der EUM Proxy-Adresse zu ermitteln, die Sie ändern möchten. Verwenden Sie zum Bestimmen der Position der **\$mbx. EmailAddresses** Befehl. Die erste EUM-Proxy-Adresse in der Liste wird 0 sein.

```
$mbx = Get-Mailbox tony.smith
$mbx.EmailAddresses.Item(1) -="eum:tsmith@contoso.com;phone-context=MyDialPlan.contoso.com"
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

# Hinzufügen einer Durchwahlnummer

18.12.2018 • 7 minutes to read

Wenn Sie einen Benutzer für UM aktivieren und mit einem Telefondurchwahl-Wählplan verknüpfen, wird eine EUM-Proxyadresse für den Benutzer erstellt, die die Durchwahlnummer des Benutzers enthält. Sie müssen mindestens eine Durchwahlnummer für UM erstellen, damit Voicemail an das Postfach des Benutzers gesendet werden kann. Die Durchwahlnummer wird auch verwendet, wenn der Benutzer eine Outlook Voice Access-Nummer anruft.

Die primäre Durchwahlnummer, die Sie beim Aktivieren des Benutzers für UM hinzugefügt haben, wird als primäre EUM-Proxyadresse aufgeführt. Wenn die primäre Durchwahlnummer entfernt wurde, wird die erste von Ihnen hinzugefügte EUM-Proxyadresse, die die Durchwahlnummer des Benutzers enthält, zur primären EUM-Proxyadresse. Weitere von Ihnen hinzugefügte Durchwahlnummern werden als sekundäre EUM-Proxyadressen aufgeführt. Wenn zusätzliche sekundäre Durchwahlnummern hinzugefügt werden, können Anrufer an allen festgelegten Durchwahlnummern Voicemail für den Benutzer hinterlassen. Alle Sprachnachrichten werden an das Postfach des gleichen Benutzers zugestellt.

Der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell können Sie eine primäre oder eine sekundäre Durchwahlnummer für einen Benutzer hinzufügen. Die Seite **E-Mail-Adresse** können auf das Postfach des Benutzers in der Exchange-Verwaltungskonsole Sie einen primären oder sekundären Durchwahlnummer hinzufügen. Sie können die Seite **UM-Postfach** in der Exchange-Verwaltungskonsole eine primäre Erweiterungsnummer hinzufügen, aber Sie können diese Seite zum Hinzufügen von sekundären Durchwahlnummern verwenden.

Sie können die primäre und sekundäre Durchwahlnummern für einen Benutzer mit dem Cmdlet **Get-UMMailbox**, oder das Cmdlet **Get-Mailbox** in Exchange Online PowerShell anzeigen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-Wählplan für Telefondurchwahlnummern erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass das Postfach des Benutzers UM-aktiviert und mit einem Wählplan vom Typ "Telefondurchwahl" verknüpft wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass die Durchwahlnummer, die dem Benutzer zugewiesen wird, die richtige, im UM-Wählplan festgelegte Anzahl von Ziffern aufweist.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen](#).

Tastenkombinationen für die Exchange-Verwaltungskonsole.

**TIP**

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Hinzufügen einer sekundären Durchwahlnummer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Wählen Sie in der Listenansicht das Postfach aus, dem eine Durchwahlnummer hinzugefügt werden soll.
3. Klicken Sie im Detailbereich **Telefon- und Sprachfunktionen** unter **Unified Messaging** auf **Details anzeigen**.
4. Klicken Sie auf der Seite **UM-Postfach** klicken Sie auf **Andere Extensions**, und klicken Sie dann auf **Hinzufügen**
5. Klicken Sie auf der Seite **Andere Durchwahlen** neben **UM-Wählplan** auf **Durchsuchen**, und suchen Sie nach dem Wählerplan für den Benutzer.
6. Geben Sie auf der Seite **Andere Durchwahlen** im Feld **Durchwahlnummer** die Durchwahlnummer ein, und klicken Sie dann auf **OK**.
7. Klicken Sie auf **Speichern**.

## Hinzufügen einer primären oder sekundären Durchwahlnummer mit der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Listenansicht, wählen Sie das Postfach, dem Sie eine Durchwahlnummer ein hinzufügen möchten, und klicken Sie dann auf **Bearbeiten**
3. Klicken Sie auf der Seite **Benutzerpostfach** unter **E-Mail-Adresse Hinzufügen**
4. Wählen Sie auf der Seite **Neue E-Mail-Adresse** die Option **EUM** aus, und geben Sie im Feld **Adresse/Durchwahl** die Durchwahlnummer für den Benutzer ein.
5. Klicken Sie auf der Seite **Neue E-Mail-Adresse** unter **Wählplan** auf **Durchsuchen**, um einen Telefondurchwahl-Wählerplan auszuwählen, und klicken Sie dann auf **OK**.
6. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell, eine Durchwahlnummer ein hinzuzufügen

In diesem Beispiel wird die Durchwahlnummer 22222 für Tony Smith, einem UM-aktivierten Benutzer, hinzugefügt.

#### **NOTE**

Bevor Sie eine Durchwahlnummer von Exchange Online PowerShell hinzufügen, müssen Sie die Position der EUM Proxy-Adresse zu ermitteln, die Sie hinzufügen möchten. Verwenden Sie zum Bestimmen der Position der **\$mbx. EmailAddresses** Befehl. Die erste Proxyadresse in der Liste wird 0 sein.

```
$mbx=Get-Mailbox tony.smith  
$mbx.EmailAddresses +="eum:22222;phone-context=MyDialPlan.contoso.com"  
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

# Entfernen einer Durchwahlnummer

18.12.2018 • 7 minutes to read

Wenn Sie einen Benutzer für UM aktivieren und mit einem Wählplan vom Typ "Telefondurchwahl" verknüpfen, wird für den Benutzer eine Exchange Unified Messaging-Proxyadresse (EUM) erstellt, die die Durchwahlnummer des Benutzers enthält. Sie müssen mindestens eine Durchwahlnummer für UM definieren, damit Voicemail an das Postfach des Benutzers gesendet werden kann. Die Durchwahlnummer wird auch verwendet, wenn der Benutzer eine Outlook Voice Access-Nummer anruft.

Sie können die primäre Durchwahlnummer entfernen, die hinzugefügt wurde, als der Benutzer für UM aktiviert wurde. Oder Sie können die sekundäre Durchwahlnummer, die später hinzugefügt wurde, zusammen mit den EUM-Proxyadressen des Benutzers entfernen. Die primäre Durchwahlnummer, die hinzugefügt wurde, als der Benutzer für UM aktiviert wurde, wird als primäre EUM-Proxyadresse aufgelistet. Weitere hinzugefügte Durchwahlnummern werden als sekundäre EUM-Proxyadressen aufgelistet. Nach dem Entfernen einer Durchwahlnummer können Anrufer keine Voicemail mehr für den Benutzer an dieser Durchwahlnummern hinterlassen.

Wenn Sie die primäre Durchwahlnummer entfernen möchten, werden nicht UM zum Senden von Voicemail Postfach des Benutzers und das Anrufen, die antwortende Regeln werden nicht verarbeitet werden. Nachdem die primäre Durchwahlnummer entfernt wurde, wird die EUM-Proxy-Adresse für den Benutzer als **Null** auf das Postfach des Benutzers in der Exchange-Verwaltungskonsole und wenn Sie das Cmdlet **Get-Mailbox** in Exchange Online PowerShell führen aufgeführt. Auch, wenn Sie das Cmdlet **Get-UMMailbox** ausführen, werden die Parameter *Extensions*, *\_PhoneNumber* und *CallAnsweringRulesExtensions* leer oder null sein.

Der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell können Sie eine primäre oder eine sekundäre Durchwahlnummer entfernen. Die Seite **E-Mail-Adresse** können für das Postfach des Benutzers in der Exchange-Verwaltungskonsole Sie eine primäre oder eine sekundäre Durchwahlnummer entfernen. Sie können die Seite **UM-Postfach** in der Exchange-Verwaltungskonsole eine primäre Durchwahlnummer entfernen, aber Sie können es verwenden, um eine sekundäre Durchwahlnummer entfernen.

Sie können die primäre und sekundäre Durchwahlnummern für einen Benutzer mit dem Cmdlet **Get-UMMailbox**, oder das Cmdlet **Get-Mailbox** in Exchange Online PowerShell anzeigen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass das Postfach des Benutzers UM-aktiviert und mit einem Wählplan vom Typ "Telefondurchwahl" verknüpft wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).

- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass die primäre oder sekundäre Durchwahlnummer für den Benutzer konfiguriert sind.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Entfernen der primären oder sekundären Durchwahlnummer über die Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Listenansicht, wählen Sie das Postfach aus der Sie eine Durchwahlnummer ein entfernen möchten, und klicken Sie dann auf **Bearbeiten** .
3. Auf der Seite **Benutzerpostfach** unter **E-Mail-Adresse**, wählen Sie die Durchwahlnummer an, die Sie aus der Liste entfernen möchten, und klicken Sie dann auf **Löschen** . Die primäre EUM Proxy-Adresse oder die Erweiterung Nummer wird in fett und Zahlen aufgeführt.
4. Klicken Sie auf **Speichern**.

## Entfernen einer sekundären Durchwahlnummer über die Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Wählen Sie in der Listenansicht den Benutzer aus, aus dessen Postfach eine Durchwahlnummer entfernt werden soll.
3. Klicken Sie im Detailbereich unter **Telefon- und Sprachfunktionen > Unified Messaging** auf **Details anzeigen**.
4. Auf der Seite **andere Durchwahlen** in das Feld **Durchwahlnummer** wählen Sie die Durchwahlnummer an, die Sie entfernen möchten, und klicken Sie dann auf **Löschen** .
5. Klicken Sie auf **Speichern**.

## Verwenden Sie zum Entfernen einer Durchwahlnummer Exchange Online PowerShell

In diesem Beispiel wird die Durchwahlnummer 12345 aus dem Postfach des UM-aktivierten Benutzers Tony Smith entfernt.

#### NOTE

Bevor Sie eine Durchwahlnummer von Exchange Online PowerShell entfernen, müssen Sie die Position der EUM Proxy-Adresse zu ermitteln, die Sie ändern möchten. Verwenden Sie zum Bestimmen der Position der **\$mbx. EmailAddresses** Befehl. Die erste EUM-Proxy-Adresse in der Liste wird 0 sein.

```
$mbx = Get-Mailbox tony.smith
$mbx.EmailAddresses.remove("eum:22222;phone-context=MyDialPlan.contoso.com")
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

# 164-Nummer

18.12.2018 • 6 minutes to read

Wenn Sie einen Benutzer für UM aktivieren und ihn einem E.164-Wählplan zuweisen, werden zwei Exchange Unified Messaging-Proxyadressen (EUM) erstellt. Eine enthält die Durchwahlnummer des Benutzers, die andere seine E.164-Adresse. Die Durchwahlnummer wird verwendet, wenn der Benutzer eine Outlook Voice Access-Nummer anruft.

Sie können die primäre e. 164-Nummer, die hinzugefügt wurde, wenn der Benutzer für UM aktiviert wurde oder eine sekundäre e. 164-Nummer, die später, zusammen mit den EUM Proxyadressen für den Benutzer hinzugefügt wurde, ändern. Die primäre e. 164-Nummer, die Sie hinzugefügt haben, wenn der Benutzer für UM aktiviert wurde, wird als primäre EUM Proxy-Adresse aufgeführt. Eine beliebige zusätzlichen sekundären e. 164-Nummern, die Sie hinzugefügt werden als sekundäre EUM Proxyadressen aufgelistet. Bei e. 164-Nummern geändert wurden, können Anrufer Voicemail für den Benutzer in allen die neuen e. 164-Nummern lassen, die festgelegt wurden. Alle Sprachnachrichten werden auf das gleiche Postfach des Benutzers zugestellt.

Der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell können Sie um die primären und sekundären e. 164-Rufnummern für einen Benutzer zu ändern. Die Seite **E-Mail-Adresse** können für das Postfach des Benutzers Sie um einen primären oder sekundären e. 164-Nummer zu ändern. Jedoch können Sie zum Ändern einer primären oder sekundären e. 164-Nummer die Seite **UM-Postfach** in der Exchange-Verwaltungskonsole verwenden.

Sie können die primären und sekundären e. 164-Rufnummern für einen Benutzer mit dem Cmdlet **Get-UMMailbox**, oder das Cmdlet **Get-Mailbox** in Exchange Online PowerShell anzeigen.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass E.164-UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass das Postfach des Benutzers UM-aktiviert und mit einem Wählplan vom Typ "E.164" verknüpft wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass die E.164-Nummer, die dem UM-aktivierten Benutzer zugewiesen werden soll, gültig ist.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern der primären oder einer sekundären E.164-Nummer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Listenansicht, wählen Sie das Postfach, für die Sie eine e. 164-Nummer ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Benutzerpostfach** unter **E-Mail-Adresse**, wählen Sie die e. 164-Nummer, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**. Die primäre e. 164-Nummer wird in fett und Zahlen aufgeführt.
4. Geben Sie auf der Seite **E-Mail-Adresse** im Feld **Adresse/Durchwahl** die neue E.164-Nummer für den Benutzer ein, und klicken Sie dann auf **OK**. Wenn Sie einen neuen UM-Wählplan auswählen müssen, können Sie auf **Durchsuchen** klicken.
5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so ändern Sie die primäre oder eine sekundäre e. 164-Nummer

In diesem Beispiel wird eine E.164-Nummer für den UM-aktivierten Benutzer Tony Smith geändert.

#### NOTE

Bevor Sie eine e. 164-Nummer von Exchange Online PowerShell ändern, müssen Sie die Position der EUM Proxy-Adresse zu ermitteln, die Sie ändern möchten. Verwenden Sie zum Bestimmen der Position der **\$mbx. EmailAddresses** Befehl. Die erste EUM Proxyadresse ist der Standard (primäre) e. 164-Nummer, und es werden 0 in der Liste.

```
$mbx=Get-Mailbox tony.smith
$mbx.EmailAddresses.Item(1)="eum:+14255550123;phone-context=MyE.164DialPlan.contoso.com"
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

# Hinzufügen einer E.164-Nummer

18.12.2018 • 5 minutes to read

Wenn Sie einen Benutzer für UM aktivieren und ihn einem E.164-Wählplan zuweisen, werden zwei Exchange Unified Messaging-Proxyadressen (EUM) erstellt. Eine enthält die Durchwahlnummer des Benutzers, die andere seine E.164-Adresse. Die Durchwahlnummer wird verwendet, wenn der Benutzer eine Outlook Voice Access-Nummer anruft.

Die primäre E.164-Nummer, die hinzugefügt wurde, als der Benutzer für UM aktiviert wurde, wird als primäre EUM-Proxyadresse aufgelistet. Nachdem die primäre E.164-Nummer entfernt wurde, wird die erste EUM-Proxyadresse, die Sie hinzufügen und die E.164-Nummer des Benutzers enthält, als primäre EUM-Proxyadresse aufgelistet. Weitere hinzugefügte E.164-Nummern werden als sekundäre EUM-Proxyadressen aufgelistet. Nachdem weitere E.164-Nummern hinzugefügt wurden, können Anrufer Voicemail für den Benutzer an allen eingerichteten E.164-Nummern hinterlassen. Alle Sprachnachrichten werden an dasselbe Postfach des Empfängers zugestellt.

Der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell können Sie eine primäre oder eine sekundäre e. 164-Nummer für einen Benutzer hinzufügen. Die Seite **E-Mail-Adresse** können auf das Postfach des Benutzers in der Exchange-Verwaltungskonsole Sie einen primären oder sekundären e. 164-Nummer hinzufügen. Die Seite **UM-Postfach** können in der Exchange-Verwaltungskonsole Sie einen primären oder sekundären e. 164-Nummer hinzufügen.

Sie können die primären und sekundären e. 164-Rufnummern für einen Benutzer mit dem Cmdlet **Get-UMMailbox**, oder das Cmdlet **Get-Mailbox** in Exchange Online PowerShell anzeigen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf für Voicemail aktivierte Benutzer finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass E.164-UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass das Postfach des Benutzers UM-aktiviert und mit einem Wählplan vom Typ "E.164" verknüpft wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass die E.164-Nummer, die dem Benutzer zugewiesen ist, gültig und ordnungsgemäß formatiert ist.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Hinzufügen einer primären oder sekundären E.164-Nummer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Listenansicht, wählen Sie das Postfach, für die Sie eine e. 164-Nummer hinzufügen möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Benutzerpostfach** unter **E-Mail-Adresse Hinzufügen**.
4. Wählen Sie auf der Seite **Neue E-Mail-Adresse** die Option **EUM** aus, und geben Sie in das Feld **Adresse/Durchwahl** die neue E.164-Nummer für den Benutzer ein.
5. Klicken Sie auf der Seite **Neue E-Mail-Adresse** unter **Wählplan** auf **Durchsuchen**, um den E.164-Wählplan auszuwählen. Klicken Sie anschließend auf **OK**.
6. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell eine e. 164-Nummer hinzufügen

In diesem Beispiel wird eine E.164-Nummer für Tony Smith, einen UM-aktivierten Benutzer, hinzugefügt.

#### NOTE

Bevor Sie eine e. 164-Nummer von Exchange Online PowerShell hinzufügen, müssen Sie die Position der EUM Proxy-Adresse zu ermitteln, die Sie hinzufügen möchten. Verwenden Sie zum Bestimmen der Position der **\$mbx. EmailAddresses** Befehl. Die erste Proxyadresse in der Liste wird 0 sein.

```
$mbx=Get-Mailbox tony.smith
$mbx.EmailAddresses.Item(2)="eum:+14255550123;phone-context=MyDialPlan.contoso.com"
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

# 164-Nummer

18.12.2018 • 6 minutes to read

Wenn Sie einen Benutzer für UM aktivieren und ihn einem E.164-Wählplan zuweisen, werden zwei Exchange Unified Messaging-Proxyadressen (EUM) erstellt. Eine enthält die Durchwahlnummer des Benutzers, die andere seine E.164-Adresse. Die Durchwahlnummer wird verwendet, wenn der Benutzer eine Outlook Voice Access-Nummer anruft.

Sie können die primäre E.164-Nummer, die beim Aktivieren des Benutzers für UM hinzugefügt wurde, oder eine sekundäre E.164-Nummer, die später zusammen mit der EUM-Proxyadresse für den Benutzer hinzugefügt wurde, entfernen. Die primäre E.164-Nummer, die Sie beim Aktivieren des Benutzers für UM hinzugefügt haben, wird als primäre EUM-Proxyadresse aufgeführt. Weitere von Ihnen hinzugefügte E.164-Nummern werden als sekundäre EUM-Proxyadressen aufgeführt. Wenn eine E.164-Nummer entfernt wird, können Anrufer über die entfernte E.164-Nummer keine Voicemail mehr für den Benutzer hinterlassen.

Wenn Sie die primäre e. 164-Nummer entfernen möchten, werden nicht UM zum Senden von Voicemail Postfach des Benutzers und das Anrufen, die antwortende Regeln werden nicht verarbeitet werden. Nachdem Sie die primäre e. 164-Nummer entfernen, wird die EUM-Proxy-Adresse für den Benutzer als **Null** auf das Postfach des Benutzers in der Exchange-Verwaltungskonsole und wenn Sie das Cmdlet **Get-Mailbox** in Exchange Online PowerShell führen aufgeführt. Auch, wenn Sie das Cmdlet **Get-UMMailbox** ausführen, werden die Parameter *Extensions*, *\_PhoneNumber* und *CallAnsweringRulesExtensions* leer oder null sein.

Der Exchange-Verwaltungskonsole oder die Exchange Online PowerShell können Sie um eine primäre oder eine sekundäre e. 164-Nummer für einen Benutzer zu entfernen. Die Seite **E-Mail-Adresse** können für das Postfach des Benutzers in der Exchange-Verwaltungskonsole Sie um eine primäre oder eine sekundäre e. 164-Nummer zu entfernen. Sie können nicht die Seite **UM-Postfach** in der Exchange-Verwaltungskonsole verwenden, um einen primären oder sekundären e. 164-Nummer zu entfernen.

Sie können die primären und sekundären e. 164-Rufnummern für einen Benutzer mit dem Cmdlet **Get-UMMailbox**, oder das Cmdlet **Get-Mailbox** in Exchange Online PowerShell anzeigen.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit für Voicemail aktivierte Benutzern finden Sie unter [VoIP-e-Mail-aktivierten Benutzer Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Bevor Sie dieses Verfahren ausführen, vergewissern Sie sich, dass eine e. 164-UM-Wählplan erstellt wurde. Ausführliche Schritte finden Sie unter [Erstellen einer UM-Wählplan](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass das Postfach des Benutzers UM-aktiviert und mit einem Wählplan vom Typ "E.164" verknüpft wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass die primären und sekundären E.164-

Nummern für den Benutzer konfiguriert sind.

- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Entfernen der primären oder einer sekundären E.164-Nummer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. In der Listenansicht, wählen Sie das Postfach aus der Sie eine e. 164-Nummer entfernen möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **Postfach des Benutzers**, klicken Sie unter **E-Mail-Adresse**, wählen Sie die e. 164-Nummer, die Sie aus der Liste entfernen möchten, und klicken Sie dann auf **Löschen**. Der primäre EUM Proxyadresse oder die e. 164-Nummer wird in fett und Zahlen aufgeführt.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell, entfernen Sie die primäre oder eine sekundäre e. 164-Nummer

In diesem Beispiel wird die E.164-Nummer +14255551010 aus dem Postfach des UM-aktivierten Benutzers Tony Smith entfernt.

#### NOTE

Bevor Sie eine e. 164-Nummer von Exchange Online PowerShell entfernen, müssen Sie die Position der EUM Proxy-Adresse zu ermitteln, die Sie ändern möchten. Verwenden Sie zum Bestimmen der Position der **\$mbx. EmailAddresses** Befehl. Die erste EUM-Proxy-Adresse in der Liste wird 0 sein.

```
$mbx = Get-Mailbox tony.smith
$mbx.EmailAddresses.Item(1) -="eum:+14255551010;phone-context=MyDialPlan.contoso.com"
Set-Mailbox tony.smith -EmailAddresses $mbx.EmailAddresses
```

# Einrichten von Client-Voicemailfunktionen in Exchange Online

18.12.2018 • 5 minutes to read

In diesem Thema werden die Clientfeatures beschrieben, die Exchange Unified Messaging-aktivierten Benutzern den Zugriff auf ihre E-Mails und Voicemailnachrichten in ihrem Postfach ermöglichen. Mithilfe dieser Features können Sie den Benutzern einen vereinfachten Voicemail- und E-Mail-Zugriff und eine bessere Benutzerfreundlichkeit bieten.

## VoiceMailclient-Unterstützung

**Exchange ActiveSync-Clients:** der Microsoft Exchange ActiveSync-Protokoll wird verwendet, um die mobile-Clients, z. B. von Internet-fähigen Mobilgeräten mit Exchange-Postfach verbinden. Benutzer können mobile Geräte auf ihre Postfächer zugreifen und Anzeigen von e-Mail-Nachrichten, anzeigen und ändern, Kalender und Kontaktinformationen und hören Sie sich ihre Voicemailnachrichten abrufen. Sie können auch e-Mail, Voicemail, Kalenderelemente synchronisieren und die Kontaktinformationen mit anderen Geräten.

**Integration mit Outlook:** Microsoft Outlook ermöglicht Benutzern Zugriff auf ihre Exchange-Postfach und Anzeigen von e-Mail-Nachrichten in ihren Posteingang, anzeigen und Ändern von Kalenderinformationen und Abhören von Voicemail-Nachrichten mithilfe von Microsoft Windows Media Player, ist in der e-Mail-Nachrichten eingebettet. Mithilfe einer unterstützte e-Mail-Clients erhalten Benutzer weitere Features wie am Telefon wiedergeben.

**Integration mit Outlook Web App:** Microsoft Outlook Web App bietet Benutzern eine Reihe von Schnittstellen UM und Tools, die eine voll funktionsfähige e-Mail-Client wie Outlook vergleichbar. Mit Outlook Web App können Benutzer ihr Exchange-Postfach mit einer kompatiblen Webbroweser zugreifen. Wie Outlook Outlook Web App bietet Windows Media Player eingebettet in e-Mail-Nachrichten, damit Benutzer können Sprachnachrichten hören, und ermöglicht es Benutzern Zugriff auf andere Features wie beispielsweise am Telefon wiedergeben.

## Outlook Voice Access

In Exchange Unified Messaging kann ein UM-aktivierter Benutzer zum Zugriff auf sein Postfach eine interne oder externe Telefonnummer anrufen (die im UM-Wählplan konfiguriert ist) und das Outlook Voice Access-Menüsystem verwenden. Mithilfe des Menüs können UM-aktivierte Benutzer E-Mails lesen, Sprachnachrichten abhören, mit ihrem Outlook-Kalender arbeiten, auf ihre persönlichen Kontakte zugreifen und Aufgaben ausführen, beispielsweise das Konfigurieren ihrer Outlook Voice Access-PIN oder das Aufzeichnen von Voicemails. Weitere Informationen finden Sie unter [Einrichten von Outlook Voice Access](#).

## Weiterleiten von Anrufen

Ein UM-aktivierter Benutzer kann Mailboxansageregeln mithilfe von Outlook oder Outlook Web App erstellen oder konfigurieren. Mithilfe von Mailboxansageregeln können Benutzer steuern, wie eingehende Anrufe behandelt werden. Diese Regeln werden auf ähnliche Weise auf eingehende Anrufe angewendet wie Posteingangsregeln auf eingehende E-Mails, und sie werden wie andere Spracheinstellungen im Postfach des Benutzers gespeichert. Für jedes UM-aktivierte Postfach können bis zu neun Mailboxansageregeln eingerichtet werden. Diese Regeln gelten unabhängig von den Posteingangsregeln und schmälern nicht das Kontingent der Posteingangsregeln. Weitere Informationen finden Sie unter [Zulassen, dass Voice Mailbenutzer Anrufe weitergeleitet werden sollen](#).

## VoiceMailvorschau

Die Voicemailvorschau ist ein Feature, das Benutzer beim Empfang ihrer Voicemailnachrichten vom UM-Voicemailsystem nutzen können. Die Voicemailvorschau erweitert die Voicemailfunktion, indem eine Textversion der Audioaufzeichnungen bereitgestellt wird. Weitere Informationen finden Sie unter [Zulassen der Anzeige von Voicemailtranskriptionen für Benutzer](#).

## Faxempfang

UM leitet eingehende Faxanrufe für einen UM-aktivierten Benutzer an eine dafür vorgesehene Faxpartnerlösung weiter, die dann die Faxverbindung mit dem Faxabsender aufbaut und die Nachricht für den Benutzer empfängt. Damit UM-aktivierte Benutzer Faxnachrichten in ihrem Postfach empfangen können, müssen Sie wie folgt vorgehen:

- Aktivieren Sie eingehende Faxe auf dem um-Wählplan den Benutzern verknüpft, indem der Parameter *FaxEnabled* auf `$true` .
- Aktivieren Sie eingehende Faxe auf dem um-Wählplan verknüpft den Benutzern durch Festlegen des Parameters *Allowfax* auf `$true` .
- Aktivieren Sie eingehende Faxe für die Benutzer durch Festlegen des Parameters *FaxEnabled* auf `$true` .
- Legen Sie den Partnerfaxserver-URI fest, um eingehende Faxe zuzulassen.
- Konfigurieren Sie die Authentifizierung zwischen dem Postfachserver und dem Server des Faxpartners.

# Einrichten von Outlook Voice Access

18.12.2018 • 17 minutes to read

Microsoft Outlook Voice Access ermöglicht Exchange Unified Messaging-aktivierten Benutzern den Zugriff auf ihr Postfach über analoge, digitale oder mobile Telefone.

Ein Outlook Voice Access-Benutzer (auch Teilnehmer genannt), ist ein Benutzer in einer Organisation, der für Unified Messaging aktiviert ist. Teilnehmer verwenden Outlook Voice Access, um per Telefon auf ihre Postfächer zuzugreifen und E-Mails, Voicemailnachrichten sowie Informationen zu persönlichen Kontakten und Kalenderdaten abzurufen.

## Outlook Voice Access - Übersicht

In Microsoft Exchange Unified Messaging kann ein UM-aktivierter Benutzer zum Zugriff auf sein Postfach eine interne oder externe Telefonnummer anrufen (die im UM-Wählplan konfiguriert ist) und das Outlook Voice Access-Menüsystem verwenden. Mithilfe des Menüs können UM-aktivierte Benutzer E-Mails lesen, Sprachnachrichten abhören, mit ihrem Outlook-Kalender arbeiten, auf ihre persönlichen Kontakte zugreifen und Aufgaben ausführen, beispielsweise das Konfigurieren ihrer Outlook Voice Access-PIN und das Aufzeichnen von Voicemails.

Zwei Benutzertypen (authentifiziert und nicht authentifiziert) können sich eine Outlook Voice Access-Nummer anrufen. Wenn ein nicht authentifizierter Benutzer eine Outlook Voice Access-Nummer anruft, die in einem UM-Wählplan festgelegt ist, kann er nur Verzeichnissuchen für Benutzer vornehmen. Authentifizierte Benutzer (jene, die ihre PIN eingeben) können Verzeichnissuchen vornehmen und sich an ihrem Postfach anmelden, um sich E-Mails, Kalenderelemente und Voicemail anzuhören und um persönliche Kontakte zu suchen. Wenn sie nach einem Benutzer im Verzeichnis oder nach persönlichen Kontakten suchen, können sie, nachdem der Benutzer gefunden wurde, Anrufe an den Benutzer weiterleiten oder die Benutzerdurchwahl anrufen.

## Benutzerschnittstellen zu Outlook Voice Access

Outlook Voice Access-Benutzern stehen zwei Unified Messaging-Benutzerschnittstellen zur Verfügung: die Benutzerschnittstelle für Telefoneingabe (Telephone User Interface, TUI) und die Benutzerschnittstelle für Spracheingabe (Voice User Interface, VUI), die die automatische Spracherkennung (Automatic Speech Recognition, ASR) verwendet.

Damit ein Benutzer die Benutzerschnittstelle für Spracheingabe in Outlook Voice Access verwenden kann, muss diese im UM-Wählplan und auch in der UM-Postfachrichtlinie für den Benutzer aktiviert werden. Wenn Sie einen Wählplan und eine UM-Postfachrichtlinie erstellen und die Voicemailfunktion für einen Benutzer aktivieren, kann der Benutzer standardmäßig die automatische Spracherkennung oder die Benutzerschnittstelle für Spracheingabe in Outlook Voice Access verwenden, um durch Menüs, Nachrichten und andere Optionen zu navigieren. Allerdings muss der Benutzer - selbst wenn er die Benutzerschnittstelle verwenden kann - zur Eingabe der PIN, zum Navigieren durch die persönlichen Optionen und zum Ausführen einer Verzeichnissuche die Telefontastatur verwenden. Die Standardeinstellungen sind in der folgenden Tabelle aufgeführt.

UM-KOMPONENTE	STANDARDEINSTELLUNG	BEISPIEL FÜR EXCHANGE ONLINE POWERSHELL ZU BENUTZERSCHNITTSTELLE FÜR SPRACHEINGABE ZUGRIFF ZU ERMÖGLICHEN
---------------	---------------------	---

UM-KOMPONENTE	STANDARDEINSTELLUNG	BEISPIEL FÜR EXCHANGE ONLINE POWERSHELL ZU BENUTZERSCHNITTSTELLE FÜR SPRACHEINGABE ZUGRIFF ZU ERMÖGLICHEN
UM-Wähleinstellungen	Aktiviert	<pre>Set-UMDialPlan -Identity MyUMDialPlan - AutomaticSpeechRecognitionEnabled \$true</pre>
UM-Postfachrichtlinie	Aktiviert	<pre>Set-UMMaiboxPolicy -Identity MyUMPolicy - AllowAutomaticSpeechRecognition \$true</pre>
Postfach des Benutzers	Aktiviert	<pre>Set-UMMailbox -Identity tonysmith - AutomaticSpeechRecognitionEnabled \$true</pre>

Der folgende Abschnitt umfasst Szenarien, die die VUI-Funktionalität beschreiben.

## Outlook Voice Access-Szenarien

Beispiele zur Verwendung von Outlook Voice Access über ein Telefon:

- **Access-e-Mail:** eine Outlook Voice Access-Benutzer über ein Telefon ein Anrufs an eine Outlook Voice Access-Nummer platziert und auf ihre e-Mails zugreifen möchte. Die Ansage lautet "Willkommen. Sie sind mit Microsoft Exchange verbunden. Geben Sie die Erweiterung ein Zugriff auf Ihr Postfach. Um eine andere Person zu kontaktieren, drücken Sie die Rautetaste." Nach der Eingabe einer Durchwahlnummer Postfach die Ansage lautet: "Bitte geben Sie Ihre PIN ein und drücken Sie die Taste Pfund." Nachdem der Benutzer eine PIN die Ansage lautet gibt: "Sie haben zwei neue Voicemails, 10 neue e-Mail-Nachrichten und die nächste Besprechung ist 10:00 Uhr Sprechen Sie Voicemail, e-Mail, Kalender, persönliche Kontakte, Directory oder persönlichen Optionen." Wenn der Benutzer "E-Mail" sagt, liest das Voicemailsystem der Nachrichtenkopf und klicken Sie dann den Namen, Betreff, die Zeit und Priorität der Nachrichten, die im Postfach des Benutzers befinden.
- **Access-Kalender:** eine Outlook Voice Access-Benutzer über ein Telefon ein Anrufs an eine Outlook Voice Access-Nummer platziert und auf ihren Kalender zugreifen möchte. Die Ansage lautet "Willkommen. Sie sind mit Microsoft Exchange verbunden. Geben Sie die Erweiterung ein Zugriff auf Ihr Postfach. Um eine andere Person zu kontaktieren, drücken Sie die Rautetaste." Nach der Eingabe einer Durchwahlnummer Postfach die Ansage lautet: "Bitte geben Sie Ihre PIN ein und drücken Sie die Taste Pfund." Nachdem der Benutzer eine PIN die Ansage lautet gibt: "Sie haben zwei neue Voicemails, 10 neue e-Mail-Nachrichten und die nächste Besprechung ist 10:00 Uhr Sprechen Sie Voicemail, e-Mail, Kalender, persönliche Kontakte, Directory oder persönlichen Optionen." Wenn der Benutzer "Kalender", das Voicemailsystem sagt sagt, "Sicher, dass, und welche Tag sollte ich Open?" der Benutzer sagt "Kalender des heutigen." Das Voicemalsystem antwortet mit den Worten "heute Öffnen des Kalenders." Das Voicemalsystem liest jede Kalendertermin für diesen Tag für den Benutzer.

### NOTE

Wenn ein Postfachserver mit dem Microsoft Exchange Unified Messaging-Dienst ein beschädigtes Kalenderelement in einem Benutzerpostfach vorfindet, kann das Element nicht vorgelesen werden. Stattdessen wird der Anrufer wieder ins Outlook Voice Access-Hauptmenü geleitet, und das Vorlesen aller weiteren Termine, die möglicherweise für den Rest des Tages geplant sind, wird ausgelassen.

- **Zugriff auf Voicemail:** eine Outlook Voice Access-Benutzer platziert ein Anrufs an eine Outlook Voice

Access-Nummer über ein Telefon und Voicemail zugreifen möchte. Die Ansage lautet "Willkommen. Sie sind mit Microsoft Exchange verbunden. Geben Sie die Erweiterung ein Zugriff auf Ihr Postfach. Um eine andere Person zu kontaktieren, drücken Sie die Rautetaste." Nach der Eingabe einer Durchwahlnummer Postfach die Ansage lautet: "Bitte geben Sie Ihre PIN ein und drücken Sie die Taste Pfund." Nachdem der Benutzer eine PIN die Ansage lautet gibt: "Sie haben zwei neue Voicemails, 10 neue e-Mail-Nachrichten und die nächste Besprechung ist 10:00 Uhr Sprechen Sie Voicemail, e-Mail, Kalender, persönliche Kontakte, Directory oder persönlichen Optionen." Der Benutzer sagt "Voicemail", und das Voicemailsystem liest die Nachrichtenkopfzeile und klicken Sie dann den Namen, Betreff, die Zeit und Priorität für die VoIP-Nachrichten, die im Postfach des Benutzers befinden.

#### NOTE

Wenn die Spracherkennung aktiviert ist, können Benutzer mithilfe von Spracheingaben auf ihr UM-aktiviertes Postfach zugreifen. Die Teilnehmer können auch Tonwahl- bzw. DTMF-Eingaben (Dual Tone Multi-Frequency) verwenden, indem sie „0“ drücken. Die Spracherkennung ist für PIN-Eingaben nicht aktiviert.

- **Suchen eines Benutzers im Verzeichnis:** eine Outlook Voice Access-Benutzer und platziert ein Anrufs an eine Outlook Voice Access-Nummer über ein Telefon, und eine Person in das Verzeichnis zu suchen, indem Sie ihre e-Mail-Alias Rechtschreibung möchte. Die Ansage lautet "Willkommen. Sie sind mit Microsoft Exchange verbunden. Um eine andere Person zu kontaktieren, drücken Sie die Rautetaste." Der Benutzer drückt die Taste Pfund und anschließend Mehrfrequenzwahlverfahren verwendet, um die SMTP-Adresse der Person Rechtschreibprüfung.

#### NOTE

Die Verzeichnissuchfunktion mit einer Outlook Voice Access-Nummer ist nicht sprachaktiviert. Benutzer können den Namen der Person, mit der sie Kontakt aufnehmen möchten, nur mithilfe von Tonwahleingaben buchstabieren.

#### IMPORTANT

In einigen Unternehmen (insbesondere in Ostasien) weisen die Tasten von Bürotelefonen möglicherweise keine Buchstaben auf. Diese Tatsache macht eine Verwendung der Funktion zum Buchstabieren des Namens über die Tonwahlschnittstelle nahezu unmöglich, wenn die Tastenzuordnungen nicht bekannt sind. Standardmäßig verwendet Unified Messaging die E.161-Tastenzuordnung. d. h. 2=ABC, 3=DEF, 4=GHI, 5=JKL, 6=MNO, 7=PQRS, 8=TUV, 9=WXYZ.

Beim Eingeben einer Kombination aus Buchstaben und Zahlen, z. B. "Mike1092", werden die numerischen Ziffern sich selbst zugeordnet. Damit ein E-Mail-Alias wie z. B. "Mike1092" richtig eingegeben wird, muss der Benutzer die Zifferntasten "64531092" drücken. Für andere Zeichen als A bis Z und 0 bis 9 gibt es kein Telefontastenäquivalent. Diese Zeichen sollten daher nicht eingegeben werden. Der E-Mail-Alias "jim.wilson" wird z. B. als "546945766" eingegeben. Obwohl 10 Zeichen einzugeben sind, werden vom Benutzer nur 9 Ziffern eingegeben, weil für den Punkt (.) keine Ziffernentsprechung vorhanden ist.

## Verteilergruppen und Kontaktgruppen

Benutzer können Outlook Voice Access zum Senden oder Weiterleiten von Sprachnachrichten, E-Mails oder Besprechungsanfragen verwenden. Nachrichten oder Besprechungsanfragen können an folgende Empfänger gesendet oder weitergeleitet werden:

- Eine Person im persönlichen Ordner "Kontakte"
- Eine Person im freigegebenen Adressbuch der Organisation

- Eine Kontaktgruppe, die im Ordner "Kontakte" erstellt wurde
- Eine Verteilergruppe im freigegebenen Adressbuch der Organisation

Sie können über die Benutzerschnittstelle für die Spracheingabe (sofern die automatische Spracherkennung aktiviert wurde) oder mittels Tonwahleingaben auf der Telefonatatur Nachrichten und Besprechungsanfragen senden. Sie können mit Outlook Voice Access auch Details zu einer Gruppe abhören, einschließlich der Mitglieder der Gruppe.

#### **NOTE**

Wenn Benutzer versuchen, eine Nachricht an eine Gruppe zu senden (entweder eine Verteilergruppe im freigegebenen Adressbuch oder eine Kontaktgruppe in ihrem persönlichen Ordner "Kontakte"), die keine Mitglieder enthält, bietet das Voicemailsyste keine Optionen zum Senden oder Weiterleiten der Nachricht bzw. Besprechungsanfrage. Wenn sie versuchen, eine Gruppe ohne Mitglieder als Empfänger einer Besprechungsanfrage oder einer über das Telefon erstellten Nachricht hinzuzufügen, wird die Gruppe nicht hinzugefügt, und stattdessen hören sie eine Ansage dazu, dass die Nachricht nicht gesendet werden konnte, da der Kontakt anscheinend nicht über eine gültige E-Mail-Adresse verfügt.

## Auswählen einer Sprache

Benutzer können nicht ändern die Sprache, dass Outlook Voice Access für diese sprechen verwendet und sie verwenden, wenn sie eine Nachricht zu antworten. Das Voicemailsyste versucht, suchen und verwenden Sie die beste Übereinstimmung für die Sprache, die der Benutzer ausgewählt hat, wenn sie Microsoft Outlook Web App oder die Sprache in den regionalen Einstellungen in Outlook Web App gewählten angemeldet. Wenn die Sprache, die sie ausgewählt haben von Outlook Voice Access nicht unterstützt wird, verwendet das Voicemailsyste die gleiche Sprache, die Anrufer hören, wenn sie aufgefordert werden, eine Sprachnachricht hinterlassen.

## Steuern von Outlook Voice Access-Features

In der Standardeinstellung Wenn Benutzer in Outlook Voice Access einwählen können sie das Telefon auf ihren Kalender, e-Mail und persönliche Kontakte zugreifen und das Verzeichnis durchsuchen verwenden. Exchange Online PowerShell können Sie verhindern, dass Benutzer den Zugriff auf eine oder mehrere der folgenden Features beim Verwenden von Outlook Voice Access auf ihre Postfächer zugreifen. Wenn Sie Outlook Voice Access-Features für eine um-Postfachrichtlinie ändern, wirkt sich auf die alle Benutzer, die die um-Postfachrichtlinie zugeordnet sind. Sie können auch einige Features für einen Einzelbenutzer-Postfach deaktivieren, obwohl andere Features nur auf einem UM-Postfachrichtlinie deaktiviert werden können und sind nicht für ein einzelnes Postfach verfügbar.

#### **NOTE**

Nur Exchange Online PowerShell können Sie um die Outlook Voice Access TUI Einstellungen für UM-aktivierten Postfächern oder UM-Postfachrichtlinien zu ändern.

**UM postfachrichtlinieneinstellungen:** Sie können den Benutzerzugriff auf die folgenden Features von Outlook Voice Access auf einem UM-Postfachrichtlinie deaktivieren:

- Automatische Spracherkennung (Automatic Speech Recognition, ASR)
- Zugriff ohne PIN auf Voicemail
- Sprachantworten auf andere Nachrichten
- TUI-Zugriff auf eigenen Kalender
- TUI-Zugriff auf Verzeichnis

- TUI-Zugriff auf eigene E-Mails
- TUI-Zugriff auf eigene persönliche Kontakte

**UM-aktivierten postfacheinstellungen:** Sie können einen Benutzer Zugriff auf die folgenden Features von Outlook Voice Access auf das Postfach des Benutzers deaktivieren:

- TUI-Zugriff auf den Kalender
- TUI-Zugriff auf E-Mails
- Automatische Spracherkennung (Automatic Speech Recognition, ASR)

Sie können bei bestimmten Benutzern den Empfang von Voicemails verhindern, ihnen aber dennoch die Möglichkeit einräumen, über Outlook Voice Access auf ihr Postfach zuzugreifen. Sie können einen Benutzer für Unified Messaging aktivieren und sein Postfach mit einer Durchwahlnummer konfigurieren, die aktuell von keinem anderen Benutzer in der Organisation verwendet wird.

# Outlook Voice Access-Befehle

18.12.2018 • 15 minutes to read

Outlook Voice Access ermöglicht UM-aktivierten Benutzern (Unified Messaging) den Zugriff auf ihr Postfach über analoge, digitale oder Mobiltelefone. Mithilfe des Menüsystens in Outlook Voice Access können UM-aktivierte Benutzer E-Mail lesen, Sprachnachrichten abhören, mit dem Outlook-Kalender arbeiten, auf ihre persönlichen Kontakte zugreifen und persönliche Konfigurationsoptionen wie ihre Outlook Voice Access-PIN oder das Aufzeichnen von Voicemails verwalten. Dieses Thema enthält eine Liste der Outlook Voice Access-Befehle und eine Beschreibung, wie Benutzer damit auf ihr Postfach zugreifen können, wenn sie eine Outlook Voice Access-Nummer anrufen.

## Outlook Voice Access-Benutzeroberflächen

Outlook Voice Access besteht aus zwei Benutzeroberflächen: der Benutzerschnittstelle für Telefoneingabe (Telephone User Interface, TUI), die eine Telefontastatur verwendet, und der Benutzerschnittstelle für Spracheingabe (Voice User Interface, VUI), die Sprachbefehle verwendet. Benutzer können mit Outlook Voice Access über ein externes oder internes Telefon auf das Voicemailsystem bzw. auf ihre persönlichen E-Mails, Sprachnachrichten, Kontakte und Kalenderinformationen in ihrem Postfach zugreifen.

## E-Mail und Voicemail - Befehlsreferenz

Als Outlook Voice Access-Benutzer werden Ihnen beim Anrufen einer Outlook Voice Access-Nummer Menüoptionen angeboten, mit denen Sie auf Ihr Postfach zugreifen und Ihre E-Mail und Voicemail verwalten können. In der folgenden Tabelle sind die Befehle aufgeführt, die für die Verwaltung Ihrer E-Mail und Voicemail verfügbar sind.

### E-Mail- und Voicemailbefehle

SPRACHBEFEHL	TONWAHLBEFEHL	BESCHREIBUNG
"Wiedergeben"		Gibt die aktuelle E-Mail- oder Voicemailnachricht wieder.
"Nächstes"	#	Gibt die nächste E-Mail- oder Voicemailnachricht wieder.
"Nächste ungelesene"	00 gefolgt von ##	Gibt die nächste ungelesene E-Mail-Nachricht wieder. Nur für E-Mail verfügbar.
"Löschen"	7	Löscht die aktuelle E-Mail- oder Voicemailnachricht.
"Antworten"	8	Antwortet dem Benutzer, der die aktuelle E-Mail- oder Voicemailnachricht gesendet hat.
"Allen antworten"	00 gefolgt von 88	Antwortet allen Benutzern in der aktuellen E-Mail-Nachricht. Dies ist keine verfügbare Option für Voicemailnachrichten.

SPRACHBEFEHL	TONWAHLBEFEHL	BESCHREIBUNG
"Als ungelesen markieren"	9	Kennzeichnet die E-Mail-Nachricht als "Ungelesen".
"Ende"	33	Beendet die Wiedergabe und springt zum Ende der aktuellen E-Mail- oder Voicemailnachricht.
"Weitere Optionen"	00	Öffnet das Menü Weitere Optionen.
"Vorherige"	00 gefolgt von 11	Gibt die vorherige E-Mail- oder Voicemailnachricht wieder.
"Kopfzeile wiedergeben"		Gibt die Kopfzeile der E-Mail- oder Voicemailnachricht wieder.
"Den Absender anrufen"	00 gefolgt von 2	Führt einen Anruf an den Benutzer aus, von dem die aktuelle E-Mail- oder Voicemailnachricht gesendet wurde.
"Weiterleiten"	00 gefolgt von 6	Leitet die aktuelle E-Mail- oder Voicemailnachricht an andere E-Mail-Empfänger oder -Gruppen weiter.
"Zur Nachverfolgung kennzeichnen"	00 gefolgt von 44	Markiert oder kennzeichnet die aktuelle E-Mail- oder Voicemailnachricht für die Nachverfolgung.
"Mit Namen suchen"		Verwendet den Namen des Benutzers, um E-Mail- oder Voicemailnachrichten im Postfach des Benutzers aufzufinden.
"Unterhaltung löschen"	00 gefolgt von 77	Löscht alle E-Mail-Nachrichten, die einer E-Mail-Unterhaltung zugeordnet sind. Nur für E-Mail verfügbar.
"Unterhaltung ausblenden"	00 gefolgt von 99	Blendet zusätzliche E-Mail-Nachrichten aus, die in derselben E-Mail-Unterhaltung enthalten sind. Nur für E-Mail verfügbar.
"Umschlaginformationen"	00 gefolgt von 5	Gibt die Umschlaginformationen für die E-Mail- oder Voicemailnachricht wieder.
"Sprache auswählen"	00 gefolgt von 55	Hiermit können Sie die Sprache auswählen, in der die E-Mail- oder Voicemailnachricht wiedergegeben werden soll.
"Rücklauf" oder "Wiederholen"	1	Führt einen Rücklauf der aktuellen E-Mail- oder Voicemailnachricht durch oder wiederholt sie. Nur während der Wiedergabe der Nachricht verfügbar.

SPRACHBEFEHL	TONWAHLBEFEHL	BESCHREIBUNG
"Anhalten"	2	Hält die Wiedergabe der aktuellen E-Mail- oder Voicemailnachricht an. Nur während der Wiedergabe der Nachricht verfügbar.
"Vorlauf"	3	Führt einen schnellen Vorlauf der aktuellen E-Mail- oder Voicemailnachricht durch. Nur während der Wiedergabe der Nachricht verfügbar.
"Verlangsamen"	4	Gibt die aktuelle E-Mail- oder Voicemailnachricht langsamer wieder. Nur während der Wiedergabe der Nachricht verfügbar.
"Schneller"	6	Gibt die aktuelle E-Mail- oder Voicemailnachricht schneller wieder. Nur während der Wiedergabe der Nachricht verfügbar.
"Vorherige"	11	Gibt die vorherige E-Mail-Nachricht von Anfang an wieder. Nur für E-Mail verfügbar.
"Erneut wiedergeben"	00 gefolgt von 1	Gibt die aktuelle E-Mail- oder Voicemailnachricht erneut wieder.
"Wiederholen"	0	Wiederholt die aktuellen Menüoptionen.
"Hauptmenü"	*	Beendet den aktuellen Vorgang und wechselt zum Hauptmenü.

#### IMPORTANT

Wenn Sie auf eine E-Mail-Nachricht zugreifen müssen, nachdem Sie diese mit Outlook Voice Access gelöscht haben, können Sie die E-Mail-Nachricht mithilfe von Outlook Web App oder Outlook aus dem Ordner "Gelöschte Elemente" wieder in den entsprechenden Ordner verschieben. Es ist nicht möglich, mithilfe von Outlook Voice Access auf den Ordner "Gelöschte Elemente" zuzugreifen.

## Kalenderoptionen - Befehlsreferenz

Als Outlook Voice Access-Benutzer werden Ihnen beim Anrufen einer Outlook Voice Access-Nummer Menüoptionen angeboten, mit denen Sie auf Ihr Postfach zugreifen und Ihren Kalender verwalten können. In der folgenden Tabelle sind die Befehle aufgeführt, die für die Verwaltung Ihres Kalenders verfügbar sind.

#### Kalenderbefehle

SPRACHBEFEHL	TONWAHLBEFEHL	BESCHREIBUNG
"Nächstes"	#	Gibt den nächsten Termin im Kalender wieder.

SPRACHBEFEHL	TONWAHLBEFEHL	BESCHREIBUNG
"Nächster Tag"	##	Öffnet die Kalendertermine für den nächsten Tag und gibt sie wieder.
"Wiederholen"	0	Gibt die verfügbaren Menüoptionen erneut wieder. Falls Sie die Benutzerschnittstelle für Spracheingabe verwenden, gibt das System stattdessen den Kalendertermin erneut wieder.
"Weitere Optionen"	00	Gibt das Kalendermenü Weitere Optionen wieder.
"Wiederholen"	1	Gibt den Kalendertermin erneut wieder.
"Vorherige Besprechung"	00 gefolgt von 11	Öffnet die vorherige geplante Besprechung.
"Ort anrufen"	2	Ruft die Telefonnummer an, die für den Besprechungsstandort aufgeführt ist.
"Den Organisator anrufen"	00 gefolgt von 22	Ruft die Telefonnummer an, die für den Organisator der Besprechung aufgeführt ist.
"Ich werde mich verspäten"	3	Sendet eine Nachricht mit dem Inhalt "Ich werde mich verspäten" an die Besprechungsteilnehmer.
"Bestätigen" oder "Mit Vorbehalt bestätigen"	4	Bestätigt die Besprechungsanfrage oder bestätigt sie mit Vorbehalt.
"Details zur Besprechung"	5	Gibt die Details der Besprechung, die zurzeit wiedergegeben wird, wieder.
"Teilnahmedetails"	00 gefolgt von 55	Gibt die Details einer geplanten Besprechung wieder.
"Weiterleiten"	00 gefolgt von 6	Leitet eine Besprechungsanfrage für die Besprechung an einen anderen Benutzer weiter.
"Ablehnen" oder "Streichen"	7	Lehnt die Besprechungsanfrage ab oder streicht sie.
"Meine Kalendereinträge löschen"	00 gefolgt von 77	Löscht die Einträge in Ihrem Kalender für einen bestimmten Zeitraum des Tages.
"Antworten"	00 gefolgt von 8	Antwortet dem Organisator der Besprechung.
"Allen antworten"	00 gefolgt von 88	Antwortet allen Teilnehmern der Besprechung.

SPRACHBEFEHL	TONWAHLBEFEHL	BESCHREIBUNG
"Menü wiederholen"	5 gefolgt von 0	Gibt die verfügbaren Menüoptionen erneut wieder.
"Rücklauf"	5 gefolgt von 1	Führt einen Rücklauf der Besprechungsdetails durch.
	5 gefolgt von 11	Wechselt zum Anfang der Besprechungsdetails zurück.
	5 gefolgt von 2	Hält die Wiedergabe der Besprechungsdetails an und setzt diese fort.
"Vorlauf"	5 gefolgt von 3	Führt einen schnellen Vorlauf der Besprechungsdetails durch.
"Ende"	5 gefolgt von 33	Wechselt zum Ende der Besprechungsdetails.
	5 gefolgt von 4	Gibt die Besprechungsdetails langsamer wieder.
	5 gefolgt von 55	Wählt die Sprache aus, in der die Besprechungsdetails wiedergegeben werden sollen.
	5 gefolgt von 6	Gibt die Besprechungsdetails schneller wieder.
"Hauptmenü"	*	Beendet den aktuellen Vorgang und wechselt zum Hauptmenü.

## Suchen eines Kontakts - Befehlsreferenz

Als Outlook Voice Access-Benutzer werden Ihnen beim Anrufen einer Voice Access-Nummer Menüoptionen angeboten, mit denen Sie auf Ihr Postfach zugreifen, persönliche Optionen ändern oder einen Kontakt anrufen bzw. diesem eine Nachricht senden können. Wenn Sie sich für die Verwendung der standardmäßig ausgewählten Sprachbenutzerschnittstelle entscheiden und die Menüoption "Kontakte" auswählen, werden Sie vom Voicemailsystem aufgefordert, mit der Telefontastatur durch die Optionen für die Suche nach Kontakten zu navigieren. Sie können mit der Telefontastatur auch einen Benutzer im Verzeichnis oder einen Kontakt suchen. In der folgenden Tabelle sind die Befehle aufgeführt, die für die Verwaltung Ihrer Kontakte oder für die Suche nach einem Benutzer verfügbar sind.

### Befehle für Kontakte

SPRACHBEFEHL	TONWAHLBEFEHL	BESCHREIBUNG
"Verzeichnis"	00	Durchsucht das Verzeichnis nach einem Benutzer.

SPRACHBEFEHL	TONWAHLBEFEHL	BESCHREIBUNG
"Details wiedergeben"	1	Gibt die Details des persönlichen Kontakts wieder, beispielsweise die Telefonnummern, die für den persönlichen Kontakt aufgeführt sind.
"Eine Nachricht senden"	3	Sendet eine Nachricht an den ausgewählten persönlichen Kontakt.
"Einen anderen Kontakt suchen"	4	Sucht einen anderen persönlichen Kontakt.
"Auf dem Handy anrufen"	2 gefolgt von 1	Ruft die Mobiltelefonnummer an, die für den persönlichen Kontakt aufgeführt ist.
"Im Büro anrufen"	2 gefolgt von 2	Ruft die geschäftliche Telefonnummer an, die für den persönlichen Kontakt aufgeführt ist.
"Zu Hause anrufen"	2 gefolgt von 3	Ruft die private Telefonnummer an, die für den persönlichen Kontakt aufgeführt ist.
	##	Ermöglicht bei Verwendung der Funktion "Verzeichnissuche" die Eingabe des E-Mail-Alias oder des Namens des Benutzers in das Verzeichnis.
"Hauptmenü"	*	Beendet den aktuellen Vorgang und wechselt zum Hauptmenü.

## Persönliche Optionen - Befehlsreferenz

Als Outlook Voice Access-Benutzer werden Ihnen beim Anrufen einer Outlook Voice Access-Nummer Menüoptionen angeboten, mit denen Sie auf Ihr Postfach zugreifen und Ihre persönlichen Optionen verwalten können. Wenn Sie persönliche Optionen mithilfe von Outlook Voice Access konfigurieren, können Sie nur die Telefontastatur benutzen, um durch die Menüs zu navigieren. Die Navigation durch die Menüs mit Ihrer Stimme ist zur Konfiguration persönlicher Optionen nicht möglich. In der folgenden Tabelle sind die Befehle aufgeführt, die für die Verwaltung Ihrer persönlichen Optionen verfügbar sind.

### Persönliche Optionen - Befehle

SPRACHBEFEHL	TONWAHLBEFEHL	BESCHREIBUNG
	1	Aktiviert oder deaktiviert die telefonische Abwesenheitsansage.
	2	Zeichnet die persönliche Voicemailansage oder die Voicemailansage bei Abwesenheit auf.
	3	Ändert die für Outlook Voice Access verwendete PIN.

SPRACHBEFEHL	TONWAHLBEFEHL	BESCHREIBUNG
	4	Startet die Nutzung der Benutzerschnittstelle für Spracheingabe oder der Tonwahlschnittstelle.
	5	Ermöglicht die Festlegung der zu verwendenden lokalen Zeitzone.
	6	Ermöglicht die Auswahl des 12- oder 24-Stunden-Uhrzeitformats.
	*	Wechselt zum Hauptmenü zurück.
	0	Gibt die verfügbaren Menüoptionen erneut wieder.

## Weitere Informationen

[Einrichten von Outlook Voice Access](#)

[Einrichten von Client-Voicemailfunktionen](#)

# Navigieren in Menüs mit Outlook Voice Access

18.12.2018 • 28 minutes to read

Mithilfe der Funktion Outlook Voice Access in Unified Messaging (UM) können Benutzer mit einem Analog-, Digital- oder Mobiltelefon E-Mail- und Voicemailnachrichten abrufen sowie ihren Kalender und ihre persönlichen Kontakte verwalten. Sie können über die Telefon tastatur oder Sprachbefehle mit dem Postfach interagieren, müssen jedoch die Tastatur auf dem Telefon verwenden, um nach einem Benutzer im Verzeichnis für Ihre Organisation zu suchen.

Wenn sich UM-aktivierte Benutzer über eine Outlook Voice Access-Nummer einwählen, können sie sich über ein Telefon bei ihrem Postfach anmelden und erhalten eine Reihe von Ansagen. Diese Ansagen erleichtern ihnen die Navigation durch die Menüs des Voicemailsystems und ermöglichen ihnen, auf ihr Postfach zuzugreifen. Mit Outlook Voice Access können Benutzer die folgenden Aufgaben ausführen:

- Abrufen, Abhören, Beantworten, Erstellen und Weiterleiten von Sprchnachrichten oder E-Mails
- Abhören oder Ändern von Kalenderinformationen
- Ändern persönlicher Optionen, z. B. einer PIN, oder Anrufen eines persönlichen Kontakts bzw. Senden einer Sprchnachricht an diesen.

Eine Outlook Voice Access-Nummer wird einem Benutzer zugewiesen, wenn er für UM aktiviert wird. Die Outlook Voice Access-Nummer für den Zugriff auf das Postfach kann der Benutzer in der Begrüßungsmeldung finden, die er erhält, wenn er für UM aktiviert wird. Er kann sich alternativ auch über Outlook Web App bei seinem Postfach anmelden, zu **Optionen > Telefon** wechseln und die Outlook Voice Access-Nummer oder -Nummern im Abschnitt **Outlook Voice Access** suchen.

Nachdem ein Benutzer seine Durchwahlnummer und PIN eingegeben hat, teil ihm das Voicemailsyste mit, wie viele neue Voicemail- und E-Mail-Nachrichten für ihn vorliegen, und wann die nächste Besprechung stattfindet. Nachdem das Voicemailsyste diese Ansage abgespielt hat, wird dem Benutzer ein Outlook Voice Access-Hauptmenü vorgelesen, und der Benutzer kann einen der folgenden Sprachbefehle verwenden:

- Voicemail
- E-Mail
- Kalender
- Persönliche Optionen

## Lesen und Prüfen von E-Mails

Benutzer können mithilfe des Telefons E-Mail-Nachrichten anhören, beantworten, erstellen und ungelesene E-Mail-Nachrichten weiterleiten. Wenn ein Benutzer z. B. eine wichtige E-Mail-Nachricht erwartet und keinen Internetzugriff hat, kann er auf einem Mobiltelefon eine Outlook Voice Access-Nummer wählen.

### Anhören von E-Mail-Nachrichten

Um E-Mail-Nachrichten per Sprachbefehl abzuhören, muss der Benutzer eine Outlook Voice Access-Nummer wählen, seine Durchwahlnummer und PIN eingeben und dann Folgendes tun:

1. "E-Mail" sagen, um auf seine E-Mails zuzugreifen.
2. Das Voicemailsyste liest den Namen, den Betreff, die Zeit und die Priorität der ersten ungelesenen E-Mail vor.

3. Anschließend kann der Benutzer eine der folgenden Optionen sagen:

- "Nächste Nachricht", um die Nachricht als gelesen zu markieren und mit der nächsten E-Mail-Nachricht fortzufahren.
- "Als ungelesen markieren", um die Nachricht als ungelesen zu markieren und mit der nächsten Nachricht fortzufahren.
- "Ende", um zum Ende der Nachricht zu springen.
- "Löschen", um die Nachricht zu löschen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um E-Mail-Nachrichten mithilfe der Telefontastatur anzuhören, müssen Benutzer eine Outlook Voice Access-Nummer wählen, ihre Durchwahlnummer und PIN eingeben und dann folgendermaßen vorgehen:

1. 2 drücken, um auf ihre E-Mails zuzugreifen.
2. Das Voicemailsysteem liest den Namen, den Betreff, die Zeit und die Priorität der ersten ungelesenen E-Mail vor.
3. Anschließend kann der Benutzer eine der folgenden Optionen drücken:
  - Die Rautetaste (#), um die Nachricht als gelesen zu markieren und mit der nächsten Nachricht fortzufahren.
  - 9, um die Nachricht als ungelesen zu markieren und mit der nächsten Nachricht fortzufahren.
  - 33, um zum Ende der Nachricht zu springen.
  - 7, um die Nachricht zu löschen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



## Beantworten von E-Mail-Nachrichten

Um E-Mail-Nachrichten abzuhören und sie dann per Sprachbefehl zu beantworten, müssen Benutzer folgendermaßen vorgehen:

1. "E-Mail" sagen.
2. Wiederholt "Nächste Nachricht" sagen, bis sie zu der E-Mail-Nachricht gelangen, auf die sie antworten möchten.
3. Die Nachricht abhören oder "Ende" sagen, um zum Ende der Nachricht zu gelangen.
4. Einen der folgenden Sprachbefehle verwenden:
  - "Antworten", um dem Absender zu antworten.
  - "Allen antworten", um dem Absender und allen anderen Empfängern zu antworten.
  - "Weiterleiten", um die Nachricht an einen anderen Benutzer oder eine andere Gruppe weiterzuleiten.
5. Eine Antwort aufzeichnen und dann auflegen, nichts sagen oder eine beliebige Taste drücken. Um die Antwortnachricht zu akzeptieren und zu senden, "Senden" sagen.

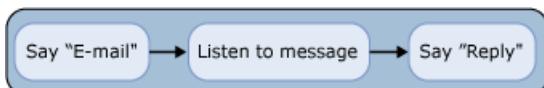
Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um E-Mail-Nachrichten abzuhören und sie dann mithilfe der Telefontastatur zu beantworten, müssen Benutzer folgendermaßen vorgehen:

1. 2 drücken.
2. Wiederholt die Taste mit dem Nummernzeichen (#) drücken, bis sie zu der E-Mail-Nachricht gelangen, auf die sie antworten möchten.
3. Die Nachricht abhören oder 33 drücken, um zum Ende der Nachricht zu gelangen.
4. Drücken Sie eine der folgenden Tasten:
  - 8, um dem Absender zu antworten.
  - 88, um dem Absender und allen anderen Empfängern zu antworten.
  - 6, um die Nachricht an einen anderen Benutzer oder eine andere Gruppe weiterzuleiten.
5. Eine Antwort aufzeichnen und dann die Rautetaste (#) drücken. Um die Antwortnachricht zu akzeptieren und zu senden, 1 drücken.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



### Abhören der nächsten ungelesenen E-Mail-Nachricht

Um eine E-Mail-Nachricht per Sprachbefehl abzuhören und dann zur nächsten ungelesenen E-Mail-Nachricht zu wechseln, müssen Benutzer folgendermaßen vorgehen:

1. "E-Mail" sagen.
2. "Nächste ungelesene" sagen. "Als ungelesen markieren" sagen, um die Nachricht als ungelesen zu markieren.

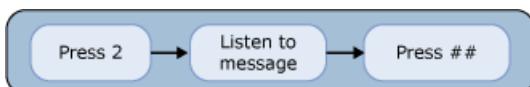
Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um eine E-Mail-Nachricht über die Telefontastatur abzuhören und dann zur nächsten ungelesenen E-Mail-Nachricht zu wechseln, müssen Benutzer folgendermaßen vorgehen:

1. 2 drücken.
2. Die Rautetaste zweimal (##) drücken, um die nächste ungelesene E-Mail-Nachricht anzuhören. 9 drücken, um die Nachricht als ungelesen zu markieren.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



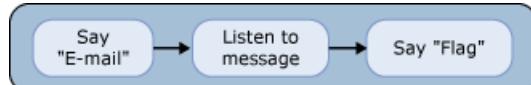
### Kennzeichnen einer Nachricht für die Nachverfolgung

Um E-Mail-Nachrichten abzuhören und sie dann per Sprachbefehl zu kennzeichnen, müssen Benutzer

folgendermaßen vorgehen:

1. "E-Mail" sagen.
2. Wiederholt "Nächste Nachricht" sagen, bis sie zu der E-Mail-Nachricht gelangen, die sie zur Nachverfolgung kennzeichnen möchten. "Als ungelesen markieren" sagen, um die Nachricht als ungelesen zu markieren.
3. Die Nachricht abhören oder "Ende" sagen, um zum Ende der Nachricht zu gelangen.
4. "Kennzeichnen" oder "Zur Nachverfolgung kennzeichnen" sagen, um die Nachricht zur Nachverfolgung zu kennzeichnen.

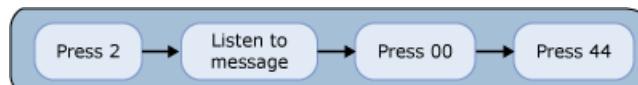
Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um E-Mail-Nachrichten abzuhören und sie dann mithilfe der Telefontastatur zu kennzeichnen, müssen Benutzer folgendermaßen vorgehen:

1. 2 drücken.
2. Wiederholt die Rautetaste (#) drücken, bis sie zu der E-Mail-Nachricht gelangen, die sie zur Nachverfolgung kennzeichnen möchten. 9 drücken, um die Nachricht als ungelesen zu markieren.
3. Die Nachricht abhören oder 33 drücken, um zum Ende der Nachricht zu gelangen.
4. Zweimal 0 drücken, um auf weitere Optionen zuzugreifen.
5. 44 drücken, um die Nachricht zur Nachverfolgung zu kennzeichnen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



### Ausblenden einer Unterhaltung

Um E-Mail-Nachrichten abzuhören und eine Unterhaltung per Sprachbefehl auszublenden, sodass das Voicemailsystem keine weiteren E-Mail-Nachrichten aus der gleichen E-Mail-Unterhaltung vorliest, müssen Benutzer folgendermaßen vorgehen:

1. "E-Mail" sagen.
2. Wiederholt "Nächste Nachricht" sagen, bis Sie zu der gewünschten E-Mail-Nachricht gelangen. "Als ungelesen markieren" sagen, um die Nachricht als ungelesen zu markieren.
3. Die Nachricht abhören oder "Ende" sagen, um zum Ende der Nachricht zu gelangen.
4. "Ausblenden" oder "Unterhaltung ausblenden" sagen, um die Unterhaltung auszublenden. Es wird die nächste E-Mail-Nachricht aus einer anderen Unterhaltung vorgelesen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um E-Mail-Nachrichten abzuhören und eine Unterhaltung mithilfe der Telefontastatur auszublenden, sodass das Voicemailsystem keine weiteren E-Mail-Nachrichten aus der gleichen E-Mail-Unterhaltung vorliest, müssen Benutzer folgendermaßen vorgehen:

1. 2 drücken.
2. Die Rautetaste (#) drücken, bis sie zu der E-Mail-Nachricht gelangen, die sie ausblenden möchten. 9 drücken, um die Nachricht als ungelesen zu markieren.
3. Die Nachricht abhören oder 33 drücken, um zum Ende der Nachricht zu gelangen.
4. 99 drücken, um die Unterhaltung auszublenden. Es wird die nächste E-Mail-Nachricht aus einer anderen Unterhaltung vorgelesen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



#### **NOTE**

Wenn eine Unterhaltung ausgeblendet ist, gilt dies nur für die aktuelle Sitzung. Wenn sich Benutzer bei ihrem Postfach abmelden und dann erneut anmelden, liest das Voicemailsyste E-Mail-Nachrichten vor, die zu der gleichen Unterhaltung gehören.

## Verwaltung von Kalendereinträgen und Terminen

Benutzer können mithilfe des Telefons Besprechungsanfragen und Termine in ihrem Kalender anhören, beantworten, erstellen und weiterleiten.

Angenommen, um 10:00 Uhr findet eine Besprechung statt. Einer der Teilnehmer wird unerwarteterweise aufgehalten und wird ungefähr 15 Minuten zu spät kommen. Er kann die anderen Besprechungsteilnehmer über diese Verspätung informieren, indem er die Telefonnummer für Outlook Voice Access anruft, sich an seinem Postfach anmeldet und auf seine Liste der Besprechungen für den betreffenden Tag im Kalender zugreift. Nachdem das Voicemailsyste die Besprechungsanfrage für die Besprechung um 10:00 Uhr vorgelesen hat, kann der Benutzer die Funktion Verspätung verwenden, um alle Besprechungsteilnehmer über die Verspätung von 15 Minuten zu informieren. Jeder Teilnehmer erhält eine E-Mail-Nachricht mit der Information, dass sich der Benutzer 15 Minuten verspätet. Der Benutzer kann optional eine Voicemailnachricht anhängen.

In einem anderen Szenario hat ein Benutzer einen wichtigen Kunden, der sehr kurzfristig eine ganztägige Besprechung einplant. Der Benutzer muss auf möglichst einfache Weise alle zuvor geplanten Besprechungen für den betreffenden Tag absagen. Mithilfe der Funktion Meinen Kalender löschen können Benutzer schnell und einfach die Termine für den gesamten Tag löschen.

### **Senden einer Verspätungsmeldung**

Um per Sprachbefehl eine Verspätungsmeldung an die Besprechungsteilnehmer zu senden, müssen Benutzer die Outlook Voice Access-Nummer wählen, ihre Durchwahlnummer und PIN eingeben und dann folgendermaßen vorgehen:

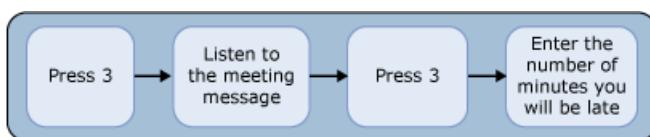
1. "Kalender für heute" sagen, um auf den Kalender zuzugreifen.
2. Die Besprechungsanfragen anhören, um die Besprechung zu suchen, für die die Nachricht "Verspätung" gesendet werden soll.
3. "Verspätung" sagen, nachdem die Besprechungsanfrage vorgelesen wurde.
4. Wenn das Voicemailsyste fragt: "Um wie viele Minuten?" "10 Minuten" sagen.
5. Wenn das Voicemailsyste fragt: "Möchten Sie eine Nachricht aufzeichnen?" Wenn ja, "Ja" sagen, die Nachricht aufzeichnen und dann "Senden" sagen. Wenn nicht, "Nein" sagen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um mithilfe der Telefontastatur eine Verspätungsmitteilung an die Besprechungsteilnehmer zu senden, müssen Benutzer die Outlook Voice Access-Nummer wählen, ihre Durchwahlnummer und PIN eingeben und dann folgendermaßen vorgehen:

1. 3, um auf den Kalender zuzugreifen.
2. Die Besprechungsanfragen anhören, um die Besprechung zu suchen, für die die Nachricht "Verspätung" gesendet werden soll.
3. Nachdem die Besprechungsanfrage vorgelesen wurde, 3 drücken.
4. Wenn das Voicemailsystem fragt: "Um wie viele Minuten?" Über die Telefontastatur "10" eingeben.

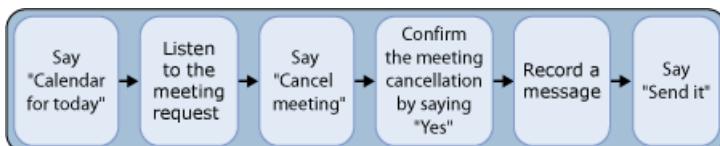


### Absagen einer Besprechung

Um eine Besprechung absagen zu können, muss der Benutzer der Besprechungsorganisator sein. Um die Besprechung per Sprachbefehl abzusagen, müssen Besprechungsorganisatoren folgendermaßen vorgehen:

1. "Kalender für heute" sagen.
2. Die Besprechungsanfragen abhören, um nach der abzusagenden Besprechung zu suchen.
3. Nachdem die Besprechungsanfrage vorgelesen wurde, "Besprechung absagen" sagen.
4. "Ja" sagen, um die Besprechungsabsage zu bestätigen.
5. Wenn der Besprechungsorganisator eine Sprachnachricht senden möchte, kann er dann "Ja" sagen, die Nachricht aufzeichnen und dann "Senden" sagen.

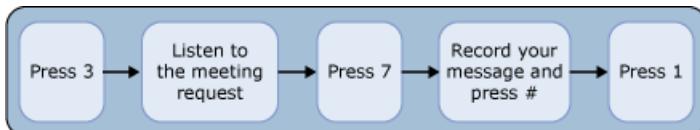
Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um eine Besprechung absagen zu können, muss der Benutzer der Besprechungsorganisator sein. Um die Besprechung mithilfe der Telefontastatur abzusagen, müssen Besprechungsorganisatoren folgendermaßen vorgehen:

1. 3 drücken.
2. Die Besprechungsanfragen abhören, um nach der abzusagenden Besprechung zu suchen.
3. 7 drücken, um die Besprechung abzusagen.
4. Wenn der Besprechungsorganisator eine Sprachnachricht senden möchte, kann er eine der folgenden Optionen drücken:
  - Pfund-Taste, um die Nachricht Aufzeichnung beenden.
  - 1, um die aufgezeichnete Nachricht zu übernehmen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.

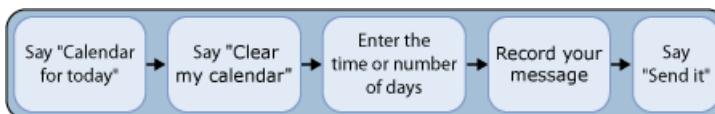


### Löschen von Kalendereinträgen

Um Kalendereinträge per Sprachbefehl zu löschen, müssen Benutzer folgendermaßen vorgehen:

1. "Kalender für heute" sagen.
2. "Meinen Kalender löschen" sagen.
3. Die zu löschenende Uhrzeit oder die Anzahl zu löschernder Tage eingeben.
4. Das Voicemailsysteem fragt, ob sie eine aufgezeichnete Sprachnachricht anhängen möchten. Wenn ja, "Ja" sagen, die Nachricht aufzeichnen und dann "Senden" sagen. Wenn nicht, "Nein" sagen.

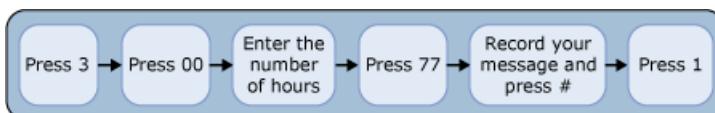
Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um Kalendereinträge mithilfe der Telefontastatur zu löschen, müssen Benutzer folgendermaßen vorgehen:

1. 3 drücken.
2. 00 drücken, um zum Menü "Weitere Optionen" zu gelangen.
3. 77 drücken, um den Inhalt des Kalenders zu löschen.
4. Die Anzahl von Stunden eingeben, die aus dem Kalender gelöscht werden sollen.
5. Wenn Benutzer eine Sprachnachricht senden möchten, führen sie eine der folgenden Aktionen aus:
  - Die Rautetaste (#) drücken, um eine Sprachnachricht zu senden.
  - Die Sprachnachricht aufzeichnen, wenn sie dazu aufgefordert werden, die Rautetaste (#) drücken, um die Aufzeichnung der Nachricht zu beenden, und dann 1 drücken, um die aufgezeichnete Nachricht zu übernehmen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



### Annehmen einer Besprechungsanfrage

Um eine Besprechungsanfrage per Sprachbefehl anzunehmen, müssen Benutzer folgendermaßen vorgehen:

1. "E-Mail" sagen, um auf ihre E-Mails zuzugreifen.
2. Die E-Mail mit der Besprechungsanfrage abhören.
3. "Zusagen" sagen, um die Besprechungsanfrage zu akzeptieren.

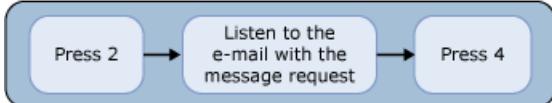
Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um eine Besprechungsanfrage mithilfe der Telefontastatur zu akzeptieren, müssen Benutzer folgendermaßen vorgehen:

1. 2 drücken, um auf ihre E-Mails zuzugreifen.
2. Die E-Mail mit der Besprechungsanfrage abhören.
3. 4 drücken, um die Besprechungsanfrage zu akzeptieren.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.

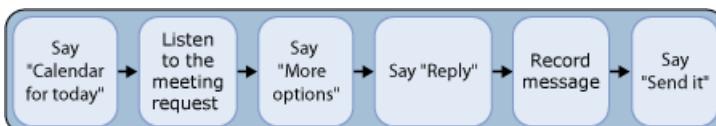


### **Beantworten einer Besprechungsanfrage**

Um eine Besprechungsanfrage per Sprachbefehl zu beantworten, müssen Benutzer folgendermaßen vorgehen:

1. "Kalender für heute" sagen.
2. Die Besprechungsanfragen abhören, um nach der Besprechungsanfrage zu suchen, die sie beantworten möchten.
3. "Weitere Optionen" sagen, um zum Menü "Weitere Optionen" zu gelangen.
4. "Antworten" sagen, um dem Besprechungsorganisator zu antworten.
5. Eine Nachricht aufzeichnen.
6. "Senden" sagen.

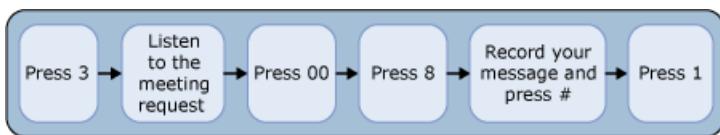
Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um eine Besprechungsanfrage mithilfe der Telefontastatur zu beantworten, müssen Benutzer folgendermaßen vorgehen:

1. 3 drücken.
2. Die Besprechungsanfragen abhören, um nach der Besprechungsanfrage zu suchen, die sie beantworten möchten.
3. 00 drücken, um weitere Optionen zu erhalten.
4. 8 drücken, um dem Besprechungsorganisator zu antworten.
5. Eine Nachricht aufzeichnen und drücken dann die Rautetaste (#) drücken.
6. 1 drücken, um die Aufzeichnung zu übernehmen und die Nachricht zu senden.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



## Verwalten persönlicher Optionen und Kontakte

Benutzer können ihre persönlichen Optionen und Kontakte mithilfe von Outlook Voice Access verwalten. Sie können die folgenden Aufgaben durchführen:

- Anrufen eines persönlichen Kontakts.
- Ermitteln und Anrufen eines Benutzers im Verzeichnis.
- Konfigurieren persönlicher Optionen, z. B. Ändern der PIN, mithilfe des Telefons.

Wenn ein Benutzer sein Postfach erstmals einrichtet, muss er eine persönliche Begrüßung und automatische Antworten erstellen, die Anrufer hören, wenn der Benutzer einen Anruf nicht entgegennehmen kann.

Angenommen, ein Benutzer stellt fest, dass er vergessen hat, eine Voicemailansage mit einer automatischen Antwort zu aktivieren, die Anrufern eine alternative Telefonnummer zur Verfügung stellt, wenn ein akutes Problem vorliegt. In diesem Fall kann der Benutzer Outlook Voice Access für den Zugriff auf seine persönlichen Optionen verwenden und über ein beliebiges Telefon eine Voicemailansage mit einer automatischen Antwort aufzeichnen und aktivieren.

Wenn ein Benutzer einem Account Manager wichtige Informationen zu einem Kunden übermitteln möchte, kann er die Nummer anrufen, die für Outlook Voice Access verwendet wird, über die Telefontastatur mithilfe der Funktion "Verzeichnissuche" den Account Manager ermitteln und dann den Anruf tätigen.

### NOTE

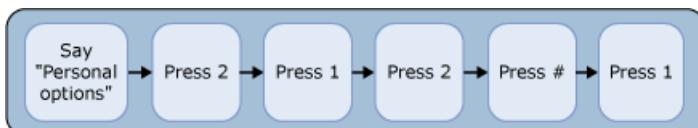
Für den Zugriff auf das Menü "Persönliche Optionen" müssen Benutzer die Telefontastatur verwenden.

### Aufzeichnen einer persönlichen Begrüßung

Um per Sprachbefehl eine persönliche Begrüßung aufzuzeichnen, müssen Benutzer eine Outlook Voice Access-Nummer wählen, ihre Durchwahlnummer und PIN eingeben und dann folgendermaßen vorgehen:

1. "Persönliche Optionen" sagen, um auf die persönlichen Optionen zuzugreifen.
- 2 drücken, um Begrüßungen aufzuzeichnen.
3. 1 drücken, um eine persönliche Begrüßung aufzuzeichnen. 2 drücken, um die persönliche Begrüßung erneut aufzuzeichnen.
4. Die Rautentaste (#) drücken, um die Aufzeichnung der persönlichen Begrüßung zu beenden.
5. 1 drücken, um die persönliche Begrüßung zu übernehmen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.

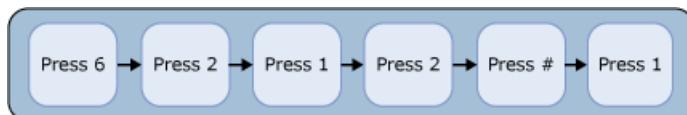


Um eine persönliche Begrüßung mithilfe der Telefontastatur aufzuzeichnen, müssen Benutzer eine Outlook Voice Access-Nummer wählen, ihre Durchwahlnummer und PIN eingeben und dann folgendermaßen vorgehen:

1. 6 drücken, um auf die persönlichen Optionen zuzugreifen.

2. 2 drücken, um Begrüßungen aufzuzeichnen.
3. 1 drücken, um eine persönliche Begrüßung aufzuzeichnen. 2 drücken, um die persönliche Begrüßung erneut aufzuzeichnen.
4. Die Rautetaste (#) drücken, um die Aufzeichnung der persönlichen Begrüßung zu beenden.
5. 1 drücken, um die persönliche Begrüßung zu übernehmen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



#### **NOTE**

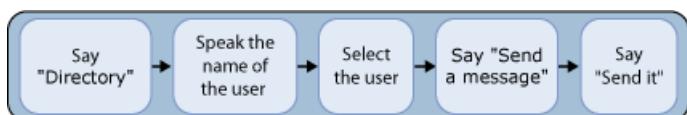
Wenn ein Benutzer seine Telefonansage ändert, kann er optional auch seine automatische E-Mail-Abwesenheitsmitteilung aktivieren bzw. deaktivieren.

### **Senden einer Sprachnachricht an einen Benutzer**

Um eine Sprachnachricht per Sprachbefehl zu suchen und an einen anderen UM-aktivieren Benutzer zu senden, müssen Benutzer folgendermaßen vorgehen:

1. "Verzeichnis" sagen.
2. Den Namen der Person sagen, nach der sie suchen.
3. Die richtige Person in der Liste auswählen.
4. "Eine Nachricht senden" sagen und dann die Sprachnachricht aufzeichnen.
5. "Senden" sagen, um die Nachricht zu senden.

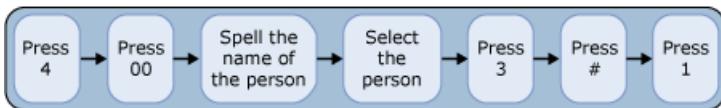
Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um eine Sprachnachricht mithilfe der Telefontastatur zu suchen und an einen anderen UM-aktivieren Benutzer zu senden, müssen Benutzer folgendermaßen vorgehen:

1. 4 drücken, um nach einem Kontakt zu suchen.
2. 00 drücken, um im Verzeichnis nach der entsprechenden Person zu suchen.
3. Den Namen der zu suchenden Person mithilfe der Telefontastatur buchstabieren.
4. Die richtige Person in der Liste auswählen.
5. 3 drücken, um eine Sprachnachricht an die Person zu senden.
6. Die Sprachnachricht aufzeichnen und dann die Rautetaste (#) drücken, um die Aufzeichnung zu beenden.
7. 1 drücken, um die Sprachnachricht zu übernehmen und zu senden.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



## Ändern einer PIN

Um ihre PIN per Sprachbefehl zu ändern, müssen Benutzer folgendermaßen vorgehen:

1. "Persönliche Optionen" sagen.
2. 3 drücken, um die PIN zu ändern.
3. Die neue PIN eingeben und dann die Rautetaste (#) drücken.
4. Die Rautetaste (#) drücken, um die neue PIN zu bestätigen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



Um ihre PIN mithilfe der Telefontastatur zu ändern, müssen Benutzer folgendermaßen vorgehen:

1. 6 drücken, um auf die persönlichen Optionen zuzugreifen.
2. 3 drücken, um die PIN zu ändern.
3. Die neue PIN eingeben und dann die Rautetaste (#) drücken.
4. Die Rautetaste (#) drücken, um die neue PIN zu bestätigen.

Dieser Prozess wird in der folgenden Abbildung veranschaulicht.



# Wiedergabe über Telefon

18.12.2018 • 7 minutes to read

Nachdem eine Voicemailnachricht eingegangen ist, können Benutzer die Voicemailnachricht über die Lautsprecher oder den Kopfhörer Ihres Computers wiedergeben oder die Funktion zur Wiedergabe über Telefon verwenden. Die Funktion zur Wiedergabe über Telefon ist in Microsoft Outlook und Outlook Web App enthalten, und Einstellungen für Wiedergabe über Telefon sind im Abschnitt **Wiedergabe über Telefon** unter den Optionen für **Voicemail** verfügbar. In diesem Thema wird erläutert, wie ein UM-aktivierter Benutzer die Funktion zur Wiedergabe über Telefon verwenden kann.

## Was ist Wiedergabe über Telefon?

Die Funktion zur Wiedergabe über Telefon ermöglicht UM-aktivierten Benutzern die Wiedergabe der Sprachnachricht über ein Telefon. Wenn ein UM-aktivierter Benutzer in einem Großraumbüro arbeitet, einen öffentlichen Computer bzw. einen Computer verwendet, der nicht für Multimedia aktiviert ist, oder eine vertrauliche Sprachnachricht wiedergibt, möchte er die Wiedergabe der Sprachnachricht möglicherweise nicht über die Computerlautsprecher vornehmen. Alternativ kann er die Sprachnachricht mithilfe eines privaten, geschäftlichen oder Mobiltelefons wiedergeben. Wechseln Sie zur Überprüfung der Einstellungen für die Wiedergabe über Telefon in Outlook zu **Datei > Info > Voicemail verwalten**. Mit einem Klick auf die Schaltfläche **Voicemail verwalten** werden Sie automatisch bei Outlook Web App angemeldet, oder Sie können sich mit einem Webbrower bei Outlook Web App anmelden. Wechseln Sie in Outlook Web App zum Abschnitt **Optionen > Telefon > Voicemail > Wiedergabe über Telefon** auf der Seite **Voicemail**.

Wenn der Benutzer im Voicemailformular auf die Symbolleistenoption "Wiedergabe über Telefon" klickt, wird das Dialogfeld **Wiedergabe über Telefon** angezeigt. Das Dialogfeld **Wiedergabe über Telefon** stellt die Steuerelemente zum Auswählen oder Eingeben der Rufnummer, die für die Wiedergabe einer Sprachnachricht verwendet werden soll, ebenso wie die Steuerelemente zum Starten und Beenden des Anrufs sowie die Statusmeldung zum Überwachen des Anrufs zur Verfügung. Ist der Benutzer mit einem SIP-URI-Wählplan verknüpft, wird die SIP-Adresse im Feld **Wählen** angezeigt. Ist der Benutzer mit einem E.164-Wählplan verknüpft, erscheint die vollständige E.164-Nummer im Feld **Wählen**.

### NOTE

Es kann jeweils nur eine Sprachnachricht wiedergegeben werden. Wenn der Benutzer versucht, einen zweiten Anruf über Telefon wiederzugeben, während ein vorheriger Anruf noch verarbeitet wird, wird eine Fehlermeldung angezeigt.

## Liste der zuletzt verwendeten Rufnummern

Benutzer können eine Liste der Rufnummern im Feld **Wählen** anzeigen, die sie zuletzt verwendet haben. Die im Abschnitt **Wiedergabe über Telefon** angegebene Rufnummer wird immer als erster Eintrag angezeigt und für den Benutzer automatisch als primäre Rufnummer ausgewählt. Benutzer können das Dropdownmenü zum Auswählen anderer Rufnummern verwenden, die anstelle der als primäre Rufnummer konfigurierten Rufnummer verwendet werden sollen.

#### **NOTE**

Wenn es Benutzern, die das Feature "Wiedergabe über Telefon" verwenden, möglich sein soll, eine externe Rufnummer ohne einen Zugangscode für die Amtsleitung wählen zu können (z. B. 0425-555-1234 anstelle von 0-0425-555-1234) konfigurieren Sie nationale/regionale Wählregeln für einen UM-Wählplan, die die folgende Zeile enthalten: group1, 9xxxxxxxxx, 91xxxxxxxx. Nachdem Sie die nationalen/regionalen Wählregeln konfiguriert haben, fügen Sie diese Liste der UM-Postfachrichtlinie hinzu.

## Schaltflächen für "Wiedergabe über Telefon"

Das Dialogfeld **Wiedergabe über Telefon** stellt Benutzern die Optionen **Wählen** und **Auflegen** zur Verfügung. Beim erstmaligen Öffnen des Dialogfelds **Wiedergabe über Telefon** ist die Schaltfläche **Wählen** aktiviert, und die Schaltfläche **Auflegen** ist deaktiviert. Nachdem der Anruf eingeleitet wurde, bleibt die Schaltfläche **Wählen** deaktiviert, bis der Anruf beendet wurde. Der Anruf kann durch Klicken auf die Schaltfläche **Auflegen** oder durch physisches Auflegen des Telefons beendet werden. Wenn Sie das Dialogfeld **Wiedergabe über Telefon** mithilfe der Schaltfläche **Schließen** schließen, wird der ggf. zurzeit stattfindende Anruf beendet. Die Option **Wiedergabe über Telefon** sowie weitere Optionen sind auch in der **Lesebereich**-Vorschau in Outlook verfügbar. Wenn Sie die Voicemailnachricht in einem eigenen Fenster aufrufen, ist die Schaltfläche **Wiedergabe über Telefon** auf der Symbolleiste vorhanden.

## Betreff, Gesendet und Status

Der untere Abschnitt des Dialogfelds **Wiedergabe über Telefon** zeigt den Betreff der Sprachnachricht, Datum und Uhrzeit der Übermittlung sowie eine Nachricht an, die den aktuellen Status des Anrufs angibt. Fehler, die sich auf den Vorgang der Wiedergabe über Telefon beziehen, werden dem Benutzer ggf. in diesem Abschnitt des Dialogfelds **Wiedergabe über Telefon** angezeigt.

## Rufnummerüberprüfung

Bei der Wiedergabe über Telefon wird nur eine einfache Überprüfung der Eingabe im Dialogfeld **Wiedergabe über Telefon** vorgenommen. "Wiedergabe über Telefon" überprüft keine Rufnummern. Ist eine Rufnummer nicht gültig, gibt der Microsoft Exchange Unified Messaging-Dienst einen aussagekräftigen Fehlercode an den Benutzer zurück.

# Outlook Voice Access-Prozeduren

18.12.2018 • 2 minutes to read

Aktivieren oder Deaktivieren von Outlook Voice Access für Benutzer

Konfigurieren einer Outlook Voice Access-Nummer

Deaktivieren von ausgewählten Features für Outlook Voice Access-Benutzer

Festlegen von Postfachfunktionen für Outlook Voice Access-Benutzer

Festlegen von Postfachfeatures für einen Benutzer Outlook Voice Access

Aktivieren oder Deaktivieren der automatischen Spracherkennung für einen Outlook Voice Access-Benutzer

Aktivieren einer Informationsansage für Outlook Voice Access-Benutzer

Aktivieren einer benutzerdefinierten Begrüßung für Outlook Voice Access-Benutzer

Aktivieren oder Deaktivieren der Funktion "Wiedergabe über Telefon" für Outlook Voice Access-Benutzer

Aktivieren Sie oder deaktivieren Sie der sendenden Sprachnachrichten aus Outlook Voice Access

Ermöglichen oder verhindern, dass Weiterleiten von Anrufen von Outlook Voice Access

Konfigurieren Sie die Gruppe von Benutzern, die Outlook Voice Access-Benutzer wenden können

Konfigurieren Sie die primäre Methode für Outlook Voice Access-Benutzer suchen

Konfigurieren Sie die sekundäre Methode für Outlook Voice Access-Benutzer suchen

Konfigurieren der Anzahl von Anmeldefehlern, bevor Outlook Voice Access-Benutzer getrennt werden

Die Anzahl der Eingabefehler zu konfigurieren, bevor Outlook Voice Access-Benutzer getrennt sind

Konfigurieren Sie den Grenzwert auf persönliche Begrüßung für Outlook Voice Access-Benutzer

# Aktivieren oder Deaktivieren von Outlook Voice Access für Benutzer

18.12.2018 • 3 minutes to read

Der Zugriff auf Outlook Voice Access kann für UM-aktivierte Benutzer, die einer UM-Postfachrichtlinie (Unified Messaging) zugeordnet sind, aktiviert oder deaktiviert werden. Mit Outlook Voice Access können UM-aktivierte Benutzer über ein Telefon auf ihr Postfach zugreifen. Diese Einstellung ist standardmäßig aktiviert.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren oder Deaktivieren von Outlook Voice Access mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten**
3. Deaktivieren Sie auf der Seite **UM-Postfachrichtlinie** das Kontrollkästchen für **Outlook Voice Access zulassen**.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren von Outlook Voice Access

In diesem Beispiel können Benutzer, die die um-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy` Outlook Voice Access verwenden.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowSubscriberAccess $true
```

In diesem Beispiel wird verhindert, dass Benutzer, die die um-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy` aus Outlook Voice Access verwenden.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowSubscriberAccess $false
```

# Konfigurieren einer Outlook Voice Access-Nummer

18.12.2018 • 4 minutes to read

Eine Outlook Voice Access-Nummer ermöglicht es einem für Unified Messaging (UM) und Voicemailzugriff aktivierte Benutzer, mithilfe von Outlook Voice Access auf sein Postfach zuzugreifen. Wenn Sie eine Outlook Voice Access- oder Teilnehmerzugriffsnummer für einen Wählplan konfigurieren, können UM-aktivierte Benutzer die Teilnehmerzugriffsnummer anrufen, sich bei ihrem Postfach anmelden und dann auf E-Mails und Voicemailnachrichten, ihren Kalender und persönliche Kontaktinformationen zugreifen.

Beim Erstellen eines UM-Wählplans werden standardmäßig keine Outlook Voice Access-Nummern konfiguriert. Zum Konfigurieren einer Outlook Voice Access-Nummer müssen Sie zunächst einen Wählplan erstellen und dann eine Outlook Voice Access-Nummer unter der Option **Outlook Voice Access** des Wählplans konfigurieren. Auch wenn keine Outlook Voice Access-Nummer erforderlich ist, müssen Sie mindestens eine Outlook Voice Access-Nummer konfigurieren, um UM-aktivierten Benutzern die Verwendung von Outlook Voice Access für den Zugriff auf ihr Postfach zu ermöglichen. Sie können für einen einzelnen Wählplan auch mehrere Outlook Voice Access-Nummern konfigurieren.

Outlook Voice Access-Nummer können Buchstaben, numerische Zeichen und Sonderzeichen sowie Trennzeichen und Leerzeichen enthalten. Beispiel:

- +14255551010
- +1-425-555-1010
- 4255551010
- +1 425 555 1010
- 1-800-555-CALL

Weitere Informationen zu den Menüoptionen, die für Benutzer von Outlook Voice Access verfügbar sind, finden Sie in der Schnellreferenz zu Outlook Voice Access, die im [Microsoft Download Center](#) abgerufen werden kann.

Zusätzliche Verwaltungsaufgaben im Zusammenhang mit UM-Wählplänen finden Sie unter [Dial Plan Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren einer Outlook Voice Access-Nummer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. Wählen Sie in der Listenansicht den UM-Wählplan zu ändern, und klicken Sie auf der Symbolleiste auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Verwenden Sie das in **Outlook Voice Access** unter **Outlook Voice Access-Nummern** eingeben die Nummer, die Sie verwenden möchten, und klicken Sie dann auf **Hinzufügen**.
5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie eine Outlook Voice Access-Nummer

In diesem Beispiel wird die Anzahl von Outlook Voice Access 4255550100 für einen UM-Wählplan mit dem Namen **MyUMDialPlan**.

```
Set-UMDialPlan -identity MyUMDialPlan -AccessTelephoneNumberNumbers 4255550100
```

# Deaktivieren ausgewählter Funktionen für Outlook Voice Access-Benutzer

18.12.2018 • 6 minutes to read

Outlook Voice Access enthält zwei Schnittstellen: der Telefon-Benutzeroberfläche (TUI) und der VoIP-Benutzeroberfläche (Benutzerschnittstelle für Spracheingabe). Standardmäßig wenn Benutzer in Outlook Voice Access einwählen können sie Zugriff auf ihren Kalender, e-Mail und persönliche Kontakte, und Durchsuchen Sie das Verzeichnis. Exchange Online PowerShell können Sie verhindern, dass Benutzer den Zugriff auf eine oder mehrere der folgenden Features beim Verwenden von Outlook Voice Access auf ihre Postfächer zugreifen. Wenn Sie Outlook Voice Access-Features für eine Postfachrichtlinie für Unified Messaging (UM) ändern, wirkt sich auf die alle Benutzer, die die um-Postfachrichtlinie zugeordnet sind.

In einer UM-Postfachrichtlinie können Sie für Benutzer den Zugriff auf folgende Outlook Voice Access-Funktionen deaktivieren:

- Kalender
- Verzeichnis
- E-Mail
- Persönliche Kontakte

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

Exchange Online PowerShell können auch um Outlook Voice Access-Features für das Postfach von einem einzelnen UM-aktivierten Benutzer zu deaktivieren. Wenn Sie dies tun, werden die Funktionen nur für diesen Benutzer deaktiviert. Obwohl Sie nicht alle Features von Outlook Voice Access deaktivieren können, die auf einer um-Postfachrichtlinie für einen einzelnen Benutzer gefunden werden, können Sie den Zugriff auf ihren Kalender und zu ihren e-Mail deaktivieren.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit UM-Postfächern finden Sie unter [Voicemail für Benutzer](#).

## NOTE

Nur Exchange Online PowerShell können Sie um die Outlook Voice Access-Features für UM-aktivierte Benutzer für das Postfach eines einzelnen UM-aktivierten Benutzers oder einer um-Postfachrichtlinie zu ändern.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Für die Verfahren in diesem Thema sind bestimmte Berechtigungen erforderlich. Informationen zu den Berechtigungen finden Sie in den einzelnen Verfahren.
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).

- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein Benutzer für UM aktiviert wurde. Weitere Informationen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell zum Deaktivieren von ausgewählten Outlook Voice Access-Features für UM-aktivierten Benutzer auf eine um-Postfachrichtlinie

Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).

In diesem Beispiel wird verhindert, dass Benutzer mit dem Namen einer UM-Postfachrichtlinie zugeordnet `MyUMMailboxPolicy` den Zugriff auf ihren Kalender, wenn sie in Outlook Voice Access einwählen.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowTUIAccessToCalendar $false
```

In diesem Beispiel wird verhindert, dass Benutzer mit dem Namen der UM-Postfachrichtlinie zugeordnet `MyUMMailboxPolicy` aus den Zugriff auf das Verzeichnis, wenn sie in Outlook Voice Access einwählen.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowTUIAccessToDirectory $false
```

In diesem Beispiel wird verhindert, dass Benutzer mit dem Namen der UM-Postfachrichtlinie zugeordnet `MyUMMailboxPolicy` aus den Zugriff auf ihre e-Mails, wenn sie in Outlook Voice Access einwählen.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowTUIAccessToEmail -$false
```

In diesem Beispiel wird verhindert, dass Benutzer mit dem Namen der UM-Postfachrichtlinie zugeordnet `MyUMMailboxPolicy` auf persönliche Kontakte zugreifen, wenn sie in Outlook Voice Access einwählen.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowTUIAccessToPersonalContacts $false
```

## Verwenden von Exchange Online PowerShell zum Deaktivieren von ausgewählten Outlook Voice Access-Features für das Postfach eines einzelnen UM-aktivierten Benutzers

Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).

In diesem Beispiel wird der Zugriff auf den Kalender in einem UM-Postfach mit dem Namen "tony@contoso.com" deaktiviert, wenn sich der Benutzer in Outlook Voice Access einwählt.

```
Set-UMMailbox -Identity tony@contoso.com -TUIAccessToCalendarEnabled $false
```

In diesem Beispiel wird der Zugriff auf die E-Mails in einem UM-Postfach mit dem Namen "tony@contoso.com" deaktiviert, wenn sich der Benutzer in Outlook Voice Access ein wählt.

```
Set-UMMailbox -Identity tony@contoso.com -TUIAccessToEmailEnabled $false
```

# Festlegen von Postfachfunktionen für Outlook Voice Access-Benutzer

18.12.2018 • 2 minutes to read

Outlook Voice Access enthält zwei Schnittstellen: ein Telefon-Benutzeroberfläche (TUI) und eine VoIP-Benutzeroberfläche (Benutzerschnittstelle für Spracheingabe). Sie können ein UM-aktivierten Benutzer TUI Einstellungen konfigurieren, wenn der Benutzer einem Postfach mithilfe des Systems Unified Messaging (UM) in Exchange Server zugreift. Wenn Sie einen UM-aktivierten Benutzer TUI Einstellungen auf einem UM-Postfachrichtlinie ändern, wirkt sich auf die alle Benutzer, die die um-Postfachrichtlinie zugeordnet sind. Sie können die folgenden TUI Einstellungen auf einem UM-Postfachrichtlinie ändern:

- Zugriff ohne PIN auf Voicemail
- Sprachantworten auf andere Nachrichten
- TUI-Zugriff auf eigenen Kalender
- TUI-Zugriff auf Verzeichnis
- TUI-Zugriff auf eigene E-Mails
- TUI-Zugriff auf eigene persönliche Kontakte

## NOTE

Nur mithilfe der Shell können Sie die TUI-Einstellungen für Outlook Voice Access für UM-aktivierte Benutzer ändern.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen für die Verfahren in diesem Thema finden Sie unter [Tastenkombinationen in der Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Bitten Sie in den Exchange-Foren um Hilfe. Besuchen Sie die Foren unter [Exchange Server](#), [Exchange Online](#) oder [Exchange Online Protection](#)..

## Verwenden der Shell zum Ändern von TUI-Einstellungen für eine UM-Postfachrichtlinie

In diesem Beispiel werden TUI-bezogene Einstellungen für die UM-Postfachrichtlinie `MyUMMailboxPolicy` festgelegt.

```
Set-UMMailbox -identity MyUMMailboxPolicy -AllowSubscriberAccess $true -AllowTUIAccessToCalendar $false -  
AllowTUIAccessToDirectory $false -AllowTUIAccessToEmail -$true -AllowTUIAccessToPersonalContacts $true
```

# Festlegen von Postfachfeatures für einen Benutzer Outlook Voice Access

18.12.2018 • 3 minutes to read

TUI-Einstellungen (Telephone User Interface, Telefonbenutzerschnittstelle) werden verwendet, wenn ein Benutzer unter Verwendung von Outlook Voice Access auf das Unified Messaging-System zugreift. Wenn Sie TUI-Konfigurationseinstellungen eines UM-aktivierten Benutzers ändern, ändern Sie Eigenschaften des Postfachs des UM-aktivierten Benutzers zusammen mit deren Werten.

Sie können die folgenden TUI-Einstellungen für einen UM-aktivierten Benutzer ändern:

- Zulassen des Teilnehmerzugriffs
- Zulassen des TUI-Zugriffs auf den Kalender
- Zulassen des TUI-Zugriffs auf E-Mail
- Zulassen von automatischer Spracherkennung

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Benutzer finden Sie unter [Festlegen von Postfachfeatures für einen Benutzer Outlook Voice Access](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass der vorhandene Exchange-Empfänger für Unified Messaging und Voicemail aktiviert ist. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell zum Ändern eines einzelnen UM-aktivierten Benutzers TUI Einstellungen

In diesem Beispiel werden unter Verwendung der TUI-Einstellungen der Kalender- und E-Mail-Zugriff für den

UM-aktivierten Benutzer Tony Smith aktiviert.

```
Set-UMMailbox -Identity tony@contoso.com TUIAccessToCal True -TUIAccessToEmail True -OperatorNumber 111111 -  
DisableMissedCallNotification False -AnonCallBlock True
```

**NOTE**

TUI-Einstellungen für Benutzer sind auch für UM-Postfachrichtlinien verfügbar. Das Ändern der TUI-Einstellungen einer UM-Postfachrichtlinie wirkt sich auf alle Benutzer aus, denen die UM-Postfachrichtlinie zugeordnet ist. Weitere Informationen zum Ändern von TUI-Einstellungen für eine UM-Postfachrichtlinie finden Sie unter [Festlegen von Postfachfunktionen für Outlook Voice Access-Benutzer](#).

# Aktivieren oder Deaktivieren der automatischen Spracherkennung für einen Outlook Voice Access-Benutzer

18.12.2018 • 3 minutes to read

Sie können die automatische Spracherkennung (Automatic Speech Recognition, ASR) für einen Benutzer konfigurieren, der für Unified Messaging und Voicemail aktiviert wurde. Wenn ASR für das Postfach eines Outlook Voice Access-Benutzers aktiviert ist, kann der Benutzer mithilfe von Sprachbefehlen durch die Postfachmenüs navigieren. Die automatische Spracherkennung ist standardmäßig aktiviert. Wenn ASR deaktiviert ist, muss der Benutzer DTMF-Eingaben (Dual Tone Multi-Frequency), auch Tonwahl genannt, verwenden, um durch die Menüs zu navigieren.

## NOTE

Der Exchange-Verwaltungskonsole können Sie um diese Funktion zu konfigurieren. Sie müssen Exchange Online PowerShell verwenden, aktivieren oder Deaktivieren von ASR für eine VoIP-e-Mail-Benutzer.

Weitere Verwaltungsaufgaben im Zusammenhang mit e-Mail-Benutzer UM oder VoIP finden Sie unter [Voice e-Mail-aktivierten Benutzer Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass das Postfach des Benutzers UM-aktiviert wurde. Genaue Anweisungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren von ASR für einen UM-aktivierten Benutzer

Dieses Beispiel aktiviert die ASR für einen UM-aktivierten Benutzer namens `tonysmith`.

```
Set-UMMailbox -Identity tony smith@contoso.com -AutomaticSpeechRecognitionEnabled $true
```

Dieses Beispiel deaktiviert die ASR für einen UM-aktivierten Benutzer namens `tonysmith`.

```
Set-UMMailbox -Identity tony smith@contoso.com -AutomaticSpeechRecognitionEnabled $false
```

# Aktivieren einer Informationsansage für Outlook Voice Access-Benutzer

18.12.2018 • 4 minutes to read

Sie können eine Informationsansage für einen UM-Wählplan (Unified Messaging) aktivieren. Die Informationsansagen werden für allgemeine Ankündigungen, die sich häufiger ändern als die Begrüßung, oder für Ankündigungen verwendet, die zur Einhaltung von Unternehmensrichtlinien erforderlich sind.

Standardmäßig hören Anrufer, u. a. Outlook Voice Access-Benutzer, die sich in eine konfigurierte Outlook Voice Access-Nummer einwählen, keine Informationsansage. Wenn eine Ansage wiedergegeben werden soll, müssen Sie eine WAV- oder WMA-Datei erstellen, die für die Informationsansage verwendet wird, nachdem Sie einen Wähler erstellt haben. Anschließend müssen Sie die Informationsansage für den Wähler aktivieren.

Wenn Anrufer unbedingt die gesamte Informationsansage abhören sollen, kann diese als nicht unterbrechbar konfiguriert werden. In diesem Fall kann ein Anrufer die Ansage nicht durch Drücken einer Taste oder Sprechen eines Befehls abbrechen.

Weitere Informationen zu den Menüoptionen, die für Benutzer von Outlook Voice Access verfügbar sind, finden Sie in der Schnellreferenz für Outlook Voice Access, die im [Microsoft Download Center](#) verfügbar ist.

Zusätzliche Verwaltungsaufgaben im Zusammenhang mit UM-Wählplänen finden Sie unter [Dial Plan Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren einer Informationsansage mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Klicken Sie in **Outlook Voice Access** unter **Informationsansage** auf **Ändern** und anschließend auf

**Durchsuchen**, um zur Ansagedatei zu navigieren.

**IMPORTANT**

Die Datei, die für die Informationsansage verwendet werden soll, muss eine WAV- oder WMA-Datei sein.

5. Nachdem Sie die Datei bestimmt haben, klicken Sie auf **Öffnen** und anschließend auf **Speichern**.

## Verwenden von Exchange Online PowerShell, eine Informationsansage aktivieren

In diesem Beispiel wird eine Informationsansage an, die die informational.wav Informationsansage-Datei auf einem um-Wählplan mit dem Namen verwendet ermöglicht `MyUMDialPlan`.

```
Set-UMDialPlan -Identity MyUMDialPlan -InfoAnnouncementEnabled $true -InfoAnnouncementFilename  
c:\UMGreetings\informational.wav
```

# Aktivieren einer benutzerdefinierten Begrüßung für Outlook Voice Access-Benutzer

18.12.2018 • 3 minutes to read

Standardmäßig gehört zu jedem UM-Wählplan (Unified Messaging) eine WAV-Standarddatei mit der Begrüßung, die Anrufern wiedergegeben wird, einschließlich Outlook Voice Access-Benutzern, die eine konfigurierte Outlook Voice Access-Nummer anrufen. Sie können jedoch für die Begrüßung eine WAV- oder WMA-Datei erstellen und diese für den UM-Wählplan aktivieren.

Sie können beispielsweise diese Standardbegrüßung ändern und stattdessen eine firmenspezifische Ansage verwenden wie "Willkommen bei Outlook Voice Access der Woodgrove Bank." Hierzu zeichnen Sie die angepasste Begrüßung auf und speichern sie als WAV- oder WMA-Datei. Anschließend konfigurieren Sie den Wählplan so, dass die angepassten Begrüßung verwendet wird.

Weitere Informationen zu den Menüoptionen, die für Benutzer von Outlook Voice Access verfügbar sind, finden Sie in der Schnellreferenz zu Outlook Voice Access, die im [Microsoft Download Center](#) abgerufen werden kann.

Zusätzliche Verwaltungsaufgaben im Zusammenhang mit UM-Wählplänen finden Sie unter [Dial Plan Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren einer angepassten Begrüßung mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Klicken Sie in **Outlook Voice Access** unter **Begrüßung** auf **Ändern** und anschließend auf **Durchsuchen**, um zur Begrüßungsdatei zu navigieren.

**IMPORTANT**

Die Datei, die für die Begrüßung verwendet werden soll, muss eine WAV- oder WMA-Datei sein.

5. Nachdem Sie die Datei bestimmt haben, klicken Sie auf **Öffnen** und anschließend auf **Speichern**.

## Verwenden Sie Exchange Online PowerShell, um eine benutzerdefinierte Begrüßung aktivieren

In diesem Beispiel wird eine Begrüßung, die die C:\UMPrompts\welcome.wav-Datei auf einem um-Wählplan mit dem Namen verwendet ermöglicht **MyUMDialPlan**.

```
Set-UMDialPlan -Identity MyUMDialPlan -WelcomeGreetingEnabled $true -WelcomeGreetingFilename  
c:\UMPrompts\welcome.wav
```

# Aktivieren oder Deaktivieren der Funktion „Wiedergabe über Telefon“ für Outlook Voice Access-Benutzer

18.12.2018 • 3 minutes to read

Sie können aktivieren oder deaktivieren den am Telefon-Feature für Benutzer, die eine Postfachrichtlinie für Unified Messaging (UM) wiedergeben. Diese Option ist standardmäßig aktiviert und ermöglicht es Benutzern, ihre Voicemail-Mail-Nachrichten über ein beliebiges Telefon wiedergeben. Diese Option ist nicht verfügbar für UM-aktivierten Benutzer mit einem Postfach auf einem Microsoft Exchange Server 2007-Server.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren oder Deaktivieren der Wiedergabe über Telefon mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten** .
3. Deaktivieren Sie auf der Seite **UM-Postfachrichtlinie** das Kontrollkästchen für **Voicemail-Wiedergabe über Telefon zulassen**.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell aktivieren oder deaktivieren die Wiedergabe über Telefon

Dieses Beispiel aktiviert den am Telefon-Feature für Benutzer, die die um-Postfachrichtlinie zugeordnet sind wiedergeben `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowPlayOnPhone $true
```

Dieses Beispiel deaktiviert den am Telefon-Feature für Benutzer, die die um-Postfachrichtlinie zugeordnet sind wiedergeben `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowPlayOnPhone $false
```

# Aktivieren Sie oder deaktivieren Sie die sendenden Sprachnachrichten aus Outlook Voice Access

18.12.2018 • 3 minutes to read

Sie können für Outlook Voice Access-Benutzer das Senden von Voicemailnachrichten an andere UM-aktivierte Benutzer, die denselben Wählplan zugeordnet sind, aktivieren oder deaktivieren.

Diese Einstellung ist standardmäßig aktiviert. Wenn Sie diese Einstellung deaktivieren, können Outlook Voice Access-Benutzer, die eine Outlook Voice Access-Nummer anrufen, keine Sprachnachrichten an Benutzer im selben Wählplan senden.

Zusätzliche Aufgaben im Zusammenhang mit um-Wählpläne finden Sie unter [Planen von Verfahren UM einwählen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

Verwenden der Exchange-Verwaltungskonsole, um zu ermöglichen oder zu verhindern, dass Outlook Voice Access-Benutzer Sprachnachrichten an Benutzer im selben Wählplan senden

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Wählen Sie im **Übertragung & Suche**, unter **Anrufer zulassen** Senden von Sprachnachrichten zugelassen **Sprachnachrichten ohne einen Benutzers Telefon klingeln lassen**. Wenn Sie verhindern, Senden von möchten Nachrichten VoIP für Benutzer, deaktivieren diese Einstellung.
5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell zu aktivieren oder zu verhindern, dass Outlook Voice Access-Benutzer in den gleichen Wähleinstellungen Sprachnachrichten an Benutzer senden

Dieses Beispiel aktiviert Outlook Voice Access-Benutzer, die mit dem Namen der UM-Wählplan zugeordnet MyUMDialPlan zum Senden von Sprachnachrichten für Benutzer, die die gleichen Wählplan zugeordnet.

```
Set-UMDialPlan -identity MyUMDialPlan -SendVoiceMsgEnabled $true
```

In diesem Beispiel wird verhindert, dass Outlook Voice Access-Benutzer, die mit dem Namen der UM-Wählplan zugeordnet MyUMDialPlan am Senden von Sprachnachrichten für Benutzer, die die gleichen Wählplan zugeordnet.

```
Set-UMDialPlan -identity MyUMDialPlan -SendVoiceMsgEnabled $false
```

# Ermöglichen oder verhindern, dass Weiterleiten von Anrufen von Outlook Voice Access

18.12.2018 • 3 minutes to read

Sie können für Outlook Voice Access-Benutzer das Weiterleiten von Anrufen an Benutzer, die einem Unified Messaging-Wählplan (UM) zugeordnet sind, aktivieren oder deaktivieren. Standardmäßig sind sowohl diese Option als auch die Option **Sprachnachrichten ohne Klingeln des Telefons des Benutzers hinterlassen** aktiviert, sodass Outlook Voice Access-Benutzer Anrufe an Benutzer im selben UM-Wählplan weiterleiten und Sprachnachrichten für sie hinterlassen können. Diese Einstellung gilt nur für Outlook Voice Access-Benutzer, die ihre PIN eingegeben und sich authentifiziert haben.

Zusätzliche Aufgaben im Zusammenhang mit um-Wählpläne finden Sie unter [Planen von Verfahren UM einwählen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren oder Deaktivieren der Weiterleitung von Anrufen durch Outlook Voice Access-Benutzer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  

2. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
3. Aktivieren Sie in **Weiterleitung und Suche** unter **Ermöglicht Anrufern Folgendes** das Kontrollkästchen neben **Weiterleiten an Benutzer**, um Anrufern das Weiterleiten von Anrufen an andere Benutzer im Wählplan zu ermöglichen. Wenn Sie nicht möchten, dass Outlook Voice Access-Benutzer Anrufe an Benutzer weiterleiten, deaktivieren Sie dieses Kontrollkästchen.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell zu aktivieren oder zu verhindern, dass Outlook Voice Access-Benutzer Weiterleiten von Anrufen

Dieses Beispiel aktiviert Outlook Voice Access-Benutzer zum Übertragen von Anrufen an Benutzer in den gleichen Wähleinstellungen auf einem um-Wählplan mit dem Namen `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -AllowDialPlanSubscribers $true
```

In diesem Beispiel wird verhindert, dass Outlook Voice Access-Benutzer Weiterleiten von Anrufen für Benutzer in den gleichen Wähleinstellungen auf einem um-Wählplan mit dem Namen `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -AllowDialPlanSubscribers $false
```

# Konfigurieren Sie die Gruppe von Benutzern, die Outlook Voice Access-Benutzer wenden können

18.12.2018 • 5 minutes to read

Sie können angeben, welche Benutzer weitergeleitete Anrufe oder Voicemailnachrichten von Outlook Voice Access-Benutzern empfangen können. Standardmäßig ist die Option **Nur in diesem Wählplan** aktiviert. Sie können diese Einstellung ändern, um Outlook Voice Access-Benutzern die Weiterleitung von Anrufern oder das Senden von Sprachnachrichten an Benutzer, die sich in der gesamten Organisation befinden, an eine automatische UM-Telefonzentrale oder an eine bestimmte Durchwahlnummer zu ermöglichen.

Zusätzliche Aufgaben im Zusammenhang mit um-Wählpläne finden Sie unter [Planen von Verfahren UM einwählen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

Mit der Exchange-Verwaltungskonsole die Gruppe der Benutzer konfigurieren, mit denen Voice Access-Benutzer verbunden werden können

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Wählen Sie in **Weiterleitung und Suche** unter **Anrufer dürfen Benutzer nach Name oder Alias suchen** eine der folgenden Optionen aus:
  - **In diesen Wähleinstellungen nur:** mit dieser Option können Sie Outlook Voice Access-Benutzern, die an eine Outlook Voice Access-Nummer zu suchen, und wenden Sie sich an Benutzer, die innerhalb desselben Wählplans sind in aufrufen.
  - **In der gesamten Organisation:** mit dieser Option können Sie Outlook Voice Access-Benutzern, die an

eine Outlook Voice Access-Nummer zu suchen, und wenden Sie sich an alle Benutzer in der gesamten Organisation anrufen. Dazu gehören alle Benutzer, die Postfach aktiviert werden.

- **Nur für diese automatische Telefonzentrale:** mit dieser Option können Sie Outlook Voice Access-Benutzern, die eine Verbindung mit einer bestimmten Telefonzentrale Outlook Voice Access-Nummer anrufen. Sie müssen die automatische Telefonzentrale erstellen, bevor Sie hier angeben. Dadurch können Benutzer von Outlook Voice Access in eine andere automatische Telefonzentrale übertragen werden. Die automatische Telefonzentrale hier gewählte kann eine sprachaktivierte oder nicht-Sprachaktivierte automatische Telefonzentrale sein.
- **Nur für diese Erweiterung:** Verwenden Sie diese Option, damit Outlook Voice Access-Benutzer mit einer Durchwahlnummer verbinden, die Sie angeben. Sie können nur Ziffern für die Erweiterung verwenden. Die Anzahl der Ziffern, die in diesem Feld definiert, muss die Anzahl der Stellen in den Durchwahlnummern übereinstimmen, die auf dem um-Wählplan konfiguriert sind.

5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie die Gruppe von Benutzern, die Outlook Voice Access-Benutzer wenden können

In diesem Beispiel wird die Gruppe von Benutzern, die Outlook Voice Access-Benutzer für UM-Wähleinstellungen namens wenden können `MyUMDialPlan` für die gesamte Organisation.

```
Set-UMDialPlan -Identity MyUMDialPlan -ContactScope 'GlobalAddressList' -UMAutoAttendant $null -  
AllowDialPlanSubscribers $false -AllowExtensions $false
```

In diesem Beispiel wird die Gruppe von Benutzern, die Outlook Voice Access-Benutzer für UM-Wähleinstellungen namens wenden können `MyUMDialPlan` an die `DialPlan`.

```
Set-UMDialPlan -Identity MyUMDialPlan -ContactScope DialPlan -AllowDialPlanSubscribers $false -AllowExtensions  
$false
```

# Konfigurieren Sie die primäre Methode für Outlook Voice Access-Benutzer suchen

18.12.2018 • 4 minutes to read

Beim Erstellen eines Unified Messaging-Wählplans (UM) können Sie die primäre und sekundäre Methode konfigurieren, mit der Anrufer nach Namen suchen können, um einen Benutzer zu ermitteln, wenn sie eine Outlook Voice Access-Nummer oder die Nummer einer automatischen UM-Telefonzentrale anrufen, die dem Wählerplan zugeordnet ist. Anrufer können Tonwahleingaben für die Suche nach einem UM-aktivierten Benutzer verwenden.

## NOTE

**Keine** ist keine verfügbare Option für die primäre Methode zur Namenssuche. Wenn als sekundäre Methode für die Namenssuche **Keine** ausgewählt ist, steht Anrufern nur die primäre Methode zur Verfügung. Wenn Sie sowohl die primäre als auch die sekundäre Methode für die Namenssuche konfigurieren, können Anrufer beide Methoden nutzen.

Weitere Verwaltungsaufgaben im Zusammenhang mit um-Wählpläne finden Sie unter [Planen von Verfahren UM einwählen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern der primären Methode für die Wahl nach Namen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Verwenden Sie im Abschnitt **Einstellungen** unterhalb von **Primäre Methode für Namenssuche** die Dropdownliste, um die gewünschte Option auszuwählen:

- **Nachname Vorname** (Standardeinstellung)

- **Vorname Nachname**

- **SMTP-Adresse**

5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so ändern Sie den primären Wähleinstellungen durch Name (Methode)

In diesem Beispiel wird die primäre Zugriffsnummern von Namensgebungsmethode, um `FirstLast`. Auf diese Weise können Anrufer, die die Anzahl Outlook Voice Access oder einer automatischen um-Telefonzentrale die Wählplan zugeordnet für einen UM-aktivierten Benutzer durch ihre erste suchen, und klicken Sie dann Nachname aufrufen.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNamePrimary FirstLast
```

In diesem Beispiel wird die primäre Zugriffsnummern von Namensgebungsmethode, um `LastFirst`. Auf diese Weise können Anrufer, die die Anzahl von Outlook Voice Access oder einer automatischen um-Telefonzentrale die Suche nach einem UM-aktivierten Benutzer durch ihre letzten und klicken Sie dann Vorname Wählplan zugeordnet aufrufen.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNamePrimary LastFirst
```

In diesem Beispiel wird die primäre Zugriffsnummern von Namensgebungsmethode, um `SMTP address`. Auf diese Weise können Anrufer, die die Outlook Voice Access-Nummer anrufen oder eine automatische um-Telefonzentrale zugeordnet die Wähleinstellungen für einen UM-aktivierten Benutzer ihre SMTP-Adresse ein.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNamePrimary SMTPAddress
```

# Konfigurieren Sie die sekundäre Methode für Outlook Voice Access-Benutzer suchen

18.12.2018 • 5 minutes to read

Bei der Erstellung eines Wählplans können Sie die primäre und die sekundäre Wahlmethode nach Namen oder Möglichkeiten konfigurieren, mit denen Anrufer nach Namen suchen können. Mithilfe dieser Methoden für die Wahl nach Namen können Anrufer Namen nachschlagen, um einen Benutzer zu ermitteln und zu kontaktieren, wenn sie eine Outlook Voice Access-Nummer oder eine automatische UM-Telefonzentrale anrufen, die dem Wählplan zugeordnet ist. Anrufer können Tonwahleingaben für die Suche nach einem UM-aktivierten Benutzer verwenden.

## NOTE

Wenn **Keine** als sekundäre Methode für die Suche nach Namen ausgewählt ist, steht Anrufern beim Suchen nach Benutzern nur die primäre Methode für die Namenssuche zur Verfügung. Wenn Sie sowohl die primäre als auch die sekundäre Methode für die Namenssuche konfigurieren, können Anrufer beide Methoden nutzen.

Weitere Verwaltungsaufgaben im Zusammenhang mit um-Wählpläne finden Sie unter [Planen von Verfahren UM einwählen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern der sekundären Methode für die Wahl nach Namen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Verwenden Sie im Abschnitt **Einstellungen** unter **Sekundäre Methode für Namenssuche** die

Dropdownliste, um die gewünschte Option auszuwählen:

- **Nachname Vorname** (Standardeinstellung)
- **Vorname Nachname**
- **SMTP-Adresse**
- **Keine**

5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so ändern Sie den sekundären Wähleinstellungen durch Name (Methode)

In diesem Beispiel wird festgelegt, dass der sekundären Dial durch Namensgebungsmethode, um `FirstLast`. Auf diese Weise können Anrufer, die die Anzahl Outlook Voice Access oder einer automatischen um-Telefonzentrale die Wahlplan zugeordnet für einen UM-aktivierten Benutzer durch ihre erste suchen, und klicken Sie dann Nachname aufrufen.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNameSecondary FirstLast
```

In diesem Beispiel wird festgelegt, dass der sekundären Dial durch Namensgebungsmethode, um `LastFirst`. Auf diese Weise können Anrufer, die die Anzahl von Outlook Voice Access oder einer automatischen um-Telefonzentrale die Suche nach einem UM-aktivierten Benutzer durch ihre letzten und klicken Sie dann Vorname Wahlplan zugeordnet aufrufen.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNameSecondary LastFirst
```

In diesem Beispiel wird festgelegt, dass der sekundären Dial durch Namensgebungsmethode, um `SMTP address`. Auf diese Weise können Anrufer, die die Outlook Voice Access-Nummer anrufen oder eine automatische um-Telefonzentrale zugeordnet die Wähleinstellungen für einen UM-aktivierten Benutzer ihre SMTP-Adresse ein.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNameSecondary SMTPAddress
```

In diesem Beispiel wird festgelegt, dass der sekundären Dial durch Namensgebungsmethode, um `None` und die primäre wählen, indem Sie Namensgebungsmethode, um `SMTP address`. Auf diese Weise können Anrufer, die die Outlook Voice Access-Nummer anrufen oder eine automatische um-Telefonzentrale zugeordnet die Wähleinstellungen für einen UM-aktivierten Benutzer nur ihre SMTP-Adresse ein.

```
Set-UMDialPlan -Identity MyUMDialPlan -DialByNamePrimary SMTPAddress -DialByNameSecondary None
```

# Konfigurieren der Anzahl von Anmeldefehlern, bevor Outlook Voice Access-Benutzer getrennt werden

18.12.2018 • 2 minutes to read

Sie können die zulässige Anzahl von aufeinander folgenden Anmeldefehlversuchen angeben, bevor eine Verbindung getrennt wird. Der Wertebereich dieser Einstellung ist 1 bis 20. Bei einem zu niedrigen Wert reagieren Benutzer unter Umständen verärgert. Für die meisten Organisationen sollte dieser Wert auf die Standardeinstellung von drei Versuchen festgelegt werden.

Zusätzliche Verwaltungsaufgaben im Zusammenhang mit UM-Wählplänen finden Sie unter [UM Dial Plan Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der Anzahl von Anmeldefehlversuchen, bevor eine Verbindung getrennt wird, mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Geben Sie im Abschnitt **Einstellungen** unter **Anzahl der Anmeldefehler vor dem Trennen der Verbindung** die Anzahl von Anmeldefehlversuchen ein.
5. Klicken Sie auf **Speichern**.

## Verwenden Sie Exchange Online PowerShell, um die Zahl der ungünstigen-Anmeldung konfigurieren, bevor Benutzer getrennt sind

In diesem Beispiel wird die Zahl der ungünstigen-Anmeldung an, bevor Benutzer auf 5 für einen UM-Wählplan

mit dem Namen getrennt sind `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -LogonFailuresBeforeDisconnect 5
```

# Die Anzahl der Eingabefehler zu konfigurieren, bevor Outlook Voice Access-Benutzer getrennt sind

18.12.2018 • 3 minutes to read

Sie können die Anzahl der zulässigen fehlerhaften Eingaben konfigurieren, die Benutzer beim Anruf einer Outlook Voice Access-Nummer machen können, bevor die Verbindung beendet wird. Diese Einstellung gilt sowohl für Outlook Voice Access-Benutzer als auch für nicht authentifizierte Benutzer, die die Verzeichnissuche verwenden.

Im Folgenden werden Beispiele für Datentypen aufgeführt, die als falsch betrachtet werden:

- Ein Anrufer fordert eine Durchwahl an, die nicht im System gefunden wird.
- Das System kann die Durchwahl des Benutzers nicht finden, um den Anruf weiterzuleiten.
- Ein Anrufer drückt eine Menüoption, die nicht gültig ist.

Der Wert dieser Einstellung kann zwischen 1 und 20 liegen. Für die meisten Organisationen sollte ein Standardwert von drei Versuchen festgelegt werden. Wird dieser Wert zu niedrig festgelegt, können Anrufer vorzeitig getrennt werden.

Zusätzliche Verwaltungsaufgaben im Zusammenhang mit UM-Wählplänen finden Sie unter [UM Dial Plan Procedures](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der Eingabefehler vor dem Trennen der Verbindung mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.

4. Geben Sie im Abschnitt **Einstellungen** unter **Anzahl der Eingabefehler vor dem Trennen der Verbindung** die Anzahl von Eingabefehlern ein.

5. Klicken Sie auf **Speichern**.

## Trennen Sie die Verbindung mit Exchange Online PowerShell Eingabefehler vor dem Konfigurieren

Dieses Beispiel legt die Eingabefehler vor dem Trennen auf einem um-WÄHLPLAN auf 5-Wählplan mit dem Namen `MyUMDialPlan`.

```
Set-UMDialPlan -identity MyUMDialPlan -InputFailuresBeforeDisconnect 5
```

# Konfigurieren Sie den Grenzwert auf persönliche Begrüßung für Outlook Voice Access-Benutzer

18.12.2018 • 3 minutes to read

Über die Einstellung **Beschränkung der persönlichen Begrüßungstexte (Minuten)** können Sie die maximale Dauer in Minuten angeben, die Benutzer, die der Unified Messaging-Postfachrichtlinie (UM) unterliegen, zum Aufzeichnen von Voicemailbegrüßungen verwenden können. Diese Einstellung gilt sowohl für die Standardvoicemail- als auch für Abwesenheitsansagen. Standardmäßig ist die maximale Dauer der Begrüßung auf fünf Minuten festgelegt. Sie können jedoch nach Wunsch einen Wert von 1 bis 10 Minuten festlegen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern der maximalen Begrüßungsdauer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf der Symbolleiste auf **Bearbeiten** .
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf der Symbolleiste auf **Bearbeiten** .
3. Geben Sie auf der Seite **UM-Postfachrichtlinie > Allgemein** unter **Beschränkung der persönlichen Begrüßungstexte (Minuten)** die Anzahl der Minuten ein, die Voicemailbenutzer für persönliche Begrüßungen zur Verfügung stehen.
4. Klicken Sie auf **Speichern**.

## Verwenden Sie Exchange Online PowerShell, um die maximale Dauer der Begrüßung ändern

In diesem Beispiel wird die maximale Dauer der Begrüßung auf die um-Postfachrichtlinie konfiguriert  
MyUMMailboxPolicy auf 3 Minuten.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy MaxGreetingDuration 3
```

# Schützen von Voicemail in Exchange Online

18.12.2018 • 15 minutes to read

Einige Nebenstellenanlagen und IP-Nebenstellenanlagen ermöglichen dem Anrufer, eine Voicemailnachricht als privat zu kennzeichnen, wodurch der vorgesehene Empfänger der Nachricht daran gehindert wird, die Nachricht beim Abhören an andere Personen weiterzuleiten. In integrierten Voicemailsystmen kann auf eine Sprachnachricht in verschiedener Weise zugegriffen werden. Dies erschwert es, als privat gekennzeichnete Sprachnachrichten vor einem Zugriff durch nicht autorisierte Personen zu schützen. Unified Messaging (UM) kann so konfiguriert werden, dass Sprachnachrichten für eine Organisation geschützt werden. Diese Funktion wird als geschützte Voicemail bezeichnet.

Wenn eine Sprachnachricht geschützt ist, kann der Empfänger die Nachricht nicht weiterleiten. Darüber hinaus wird über Unified Messaging (UM) sichergestellt, dass nur der vorgesehene Empfänger der Nachricht auf deren Inhalte zugreifen kann. Auf geschützte Sprachnachrichten kann mithilfe von Outlook Web App oder Outlook Voice Access zugegriffen werden.

## Übersicht über geschützte Voicemail

Das geschützte Voicemail-Feature ist verfügbar mit Unified Messaging (UM). Kann auf eine um-Postfachrichtlinie konfiguriert werden, und alle geschützte Voicemail-Einstellungen können mithilfe der Exchange-Verwaltungskonsole (EAC) oder Cmdlets in Exchange Online PowerShell in Exchange Server konfiguriert werden.

Die Funktionalität für geschützte Voicemail wird durch Aktivierung von IRM (Information Rights Management, Verwaltung von Informationsrechten) für Sprachnachrichten implementiert. Für UM-geschützte Sprachnachrichten gilt Folgendes:

- Benutzer können auf geschützte Sprachnachrichten antworten.
- Empfänger einer Sprachnachricht können diese nicht weiterleiten.
- Benutzer können keine Kopie der Sprachnachricht speichern.
- Benutzer können die angehängte Audiodatei der Sprachnachricht weder speichern noch kopieren.
- Eine Sprachnachricht kann nur von den vorgesehenen Empfängern geöffnet werden.

Sowohl Sprachnachrichten für Mailboxansagen als auch Sprachnachrichten zwischen Benutzern (Sprachnachrichten, die über Outlook Voice Access an einen Benutzer gesendet werden) können von UM geschützt werden. Der Schutz erstreckt sich jedoch nicht auf folgende Nachrichtentypen:

- Faxnachrichten.
- Nicht-Sprachnachrichten. Hierzu gehören beispielsweise E-Mail-Nachrichten oder Besprechungsanfragen, selbst wenn diese mit Outlook Voice Access erstellt werden (Sprachantworten).

## Clientunterstützung und Endbenutzerfunktionen

Die E-Mail-Clientsoftware, die zum Abhören einer geschützten Voicemailnachricht verwendet wird, muss IRM unterstützen und eine UM-geschützte Sprachnachricht lesen können. Zu den unterstützten E-Mail-Clients gehören beispielsweise Outlook, Outlook Web App und Outlook Voice Access. Die folgende Tabelle enthält eine Liste von E-Mail-Clients sowie Informationen dazu, ob diese unterstützt werden oder nicht.

E-MAIL-CLIENT	BESCHREIBUNG
Outlook	Geschützte Sprachnachrichten werden nur in Outlook 2010 und späteren Versionen unterstützt.
Outlook Web App	Outlook Web App unterstützt geschützte Voicemailnachrichten.
Outlook Voice Access	Outlook Voice Access unterstützt geschützte Voicemail.
Windows Mobile oder Windows Phone	Windows Mobile bietet keine Unterstützung für geschützte Voicemail. Allerdings unterstützen Windows Phone 7 und Windows Phone 8 geschützte Voicemail.
Andere E-Mail-Clients von Drittanbietern	Keine Unterstützung für geschützte Voicemail.

## Struktur einer geschützten Sprachnachricht

Jede geschützte Voicemailnachricht umfasst tatsächlich zwei Nachrichten. Die erste ist die äußere Nachricht, diese ist nicht verschlüsselt. Sie enthält eine Anlage namens "message.rpmsg". Die Anlage enthält die IRM-geschützte Sprachnachricht sowie Daten zur Steuerung der internen Rechteverwaltung. Die Daten zur Steuerung der Rechteverwaltung umfassen einen Inhaltsschlüssel sowie Rechteinformationen. Diese geben an, welche Benutzer auf die Sprachnachricht zugreifen können und in welcher Weise der Zugriff erfolgen kann.

Geschützte Sprachnachrichten werden im Suchordner **Voicemail** im Posteingang des Benutzers angezeigt. Der Benutzer kann die Sprachnachrichten mit dem eingebetteten Audioplayer abhören, ebenso wie eine reguläre Sprachnachricht abgehört wird. Bei der Wiedergabe einer geschützten Sprachnachricht ist allerdings die Schaltfläche zum Weiterleiten deaktiviert, und es wird im oberen Bereich der Nachricht ein Hinweis angezeigt, dass die Nachricht geschützt ist und nicht weitergeleitet werden kann.

Für e-Mail-Clients, die geschützte Voicemail nicht unterstützen, wird der Textkörper der äußeren Nachricht angezeigt. Administratoren können Text enthalten, wenn der Client-Software nicht geschützte Voicemail unterstützt, mithilfe von UM-Postfachrichtlinien. Sie können den Standardtext anpassen, der in der e-Mail-Nachricht durch Konfigurieren einer um-Postfachrichtlinie enthalten ist. Beispielsweise könnten Sie der um-Postfachrichtlinie mit benutzerdefinierten Text wie *Konfigurieren "Sie diese Voicemailnachricht nicht möglich, da es geschützt ist. Um anzusehen, oder diese Sprachnachricht anhören, melden Sie sich mit Ihrem Postfach am <https://mail.contoso.com> oder rufen Sie +1 (425) 555-1234 in Outlook Voice Access aufrufen."*

## Verfassen einer geschützten Voicemailnachricht

Es gibt zwei Situationen, in denen geschützte Sprachnachrichten erstellt werden können:

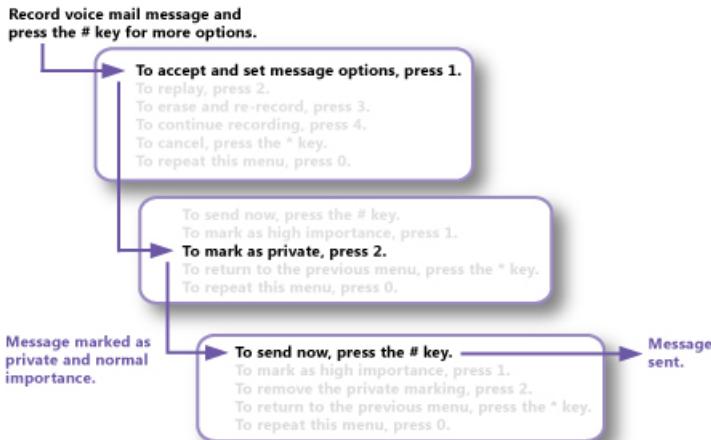
- **Mailboxansage:** Anrufbeantwortung tritt auf, wenn ein Aufrufer einen UM-aktivierten Benutzer anruft, aber der Benutzer nicht zur Verfügung, um den Anruf anzunehmen oder leitet sie direkt an die Voicemail weitergeleitet. In Anrufbeantwortung Szenarien wird das Voicemailsystem eine Reihe von Ansagen wiedergegeben, nachdem der Aufrufer eine Sprachnachricht aufgezeichnet.

Der Aufrufer kann aus verschiedenen zusätzlichen Nachrichtenoptionen wählen und die Sprachnachricht beispielsweise durch Drücken der Rautetaste (#) als privat kennzeichnen. Wenn der Aufrufer die Rautetaste (#) betätigt, kann die Nachricht gemäß den UM-Anweisungen als privat gekennzeichnet, eine solche Kennzeichnung aufgehoben oder die Sprachnachricht als wichtig gekennzeichnet werden. Das folgende Diagramm zeigt die Menüoptionen, die Aufrufern zur Verfügung stehen, wenn sie eine private Sprachnachricht für einen Benutzer hinterlassen.

#### NOTE

Bei Mailboxansagen werden von Unified Messaging die in der UM-Postfachrichtlinie des vorgesehenen Empfängers festgelegten Einstellungen für geschützte Voicemail verwendet, da der Anrufer nicht authentifiziert ist.

### Erstellen einer geschützten Voicemail über eine Mailboxansage



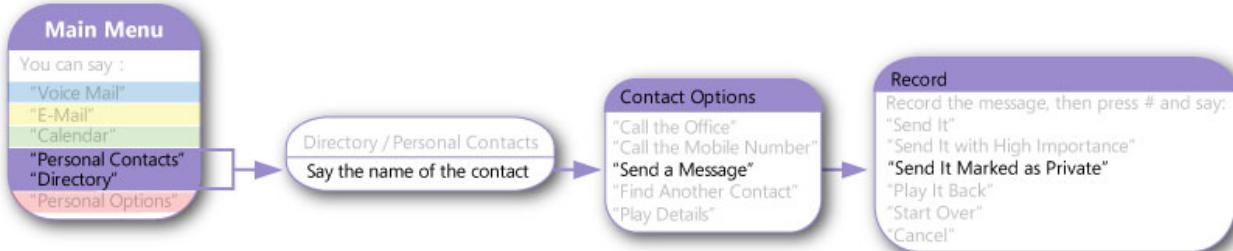
- **Outlook Voice Access:** Outlook Voice Access können UM-aktivierte Benutzer Zugriff auf ihr Postfach mithilfe von Analog, Digital oder Handys durch ihre Outlook Voice Access-Nummer zu wählen. Es gibt zwei Unified Messaging-Benutzeroberflächen für UM-aktivierten Benutzer verfügbar: der Telefon-Benutzeroberfläche (TUI) und der VoIP-Benutzeroberfläche (Benutzerschnittstelle für Spracheingabe).

Outlook Voice Access-Benutzer können im Verzeichnis nach Kontakten suchen und diesen Kontakten Sprachnachrichten senden. Wenn für die UM-aktivierten Empfänger die Funktion für geschützte Voicemail aktiviert wurde, können Anrufer die Nachrichten nach der Aufzeichnung als privat kennzeichnen. Alternativ können Administratoren eine UM-Postfachrichtlinie konfigurieren um sicherzustellen, dass alle Sprachnachrichten, die von authentifizierten Benutzern gesendet werden, UM-geschützt sind.

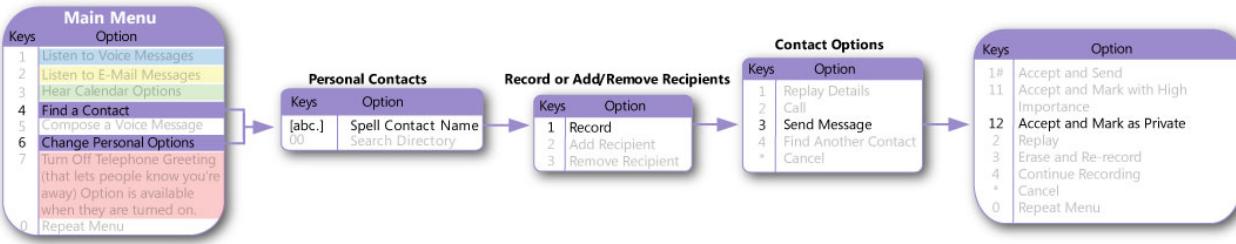
#### NOTE

Wenn es sich um einen authentifizierten Anrufer handelt, werden die in der UM-Postfachrichtlinie festgelegten Einstellungen für geschützte Voicemail angewendet, die mit dem Anrufer verknüpft sind. Dies gilt unabhängig von den UM-Postfachrichtlinieneinstellungen für den vorgesehenen Empfänger der Sprachnachricht.

### Erstellen einer geschützten Voicemailnachricht über die Benutzerschnittstelle für Spracheingabe



### Erstellen einer geschützten Voicemailnachricht über die Benutzerschnittstelle für Telefoneingabe



## UM-Postfachrichtlinien

Erstellen Sie eine Postfachrichtlinie Unified Messaging, um einen gemeinsamen Satz von UM-Richtlinieneinstellungen, wie PIN-Richtlinien, Wählvorgang Einschränkungen und geschützte Voicemail-Einstellungen für eine Auflistung von UM-aktivierten Postfächern zu übernehmen. Weitere Informationen zu UM-Postfachrichtlinien finden Sie unter [Verwalten einer um-Postfachrichtlinie](#) und [geschützte Voicemail-Prozeduren](#).

Der Exchange-Verwaltungskonsole oder über das Cmdlet **Set-UMMailboxPolicy** können in Exchange Online PowerShell Sie um geschützte Voicemail-Optionen zu konfigurieren. In der folgenden Tabelle sind die Einstellungen aufgelistet, die für geschützte Voicemail konfiguriert werden können.

### Einstellungen für geschützte Voicemail

PARAMETER	EINSTELLUNG IN DER EXCHANGE-VERWALTUNGSKONSOLE VERFÜGBAR?	BESCHREIBUNG
<i>ProtectAuthenticatedVoiceMail</i>	Ja	Der Parameter <i>ProtectAuthenticatedVoiceMail</i> gibt an, ob UM-aktivierte Benutzer beim Zugriff auf ihr Postfach mithilfe von Outlook Voice Access sind geschützte Voicemail-Nachrichten senden können. Die Standardeinstellung ist <code>None</code> . Dies bedeutet, dass kein Schutz angewendet wird, wenn Sprachnachrichten bestehen und vom Anrufer die Option Sprachnachrichten als privat markieren zu lassen. Wenn der Wert, um festgelegt ist <code>Private</code> , nur Nachrichten, die vom Anrufer als privat gekennzeichnet sind geschützt. Wenn der Wert, um festgelegt ist <code>All</code> , jede Sprachnachricht geschützt werden, unabhängig von der Option, die vom Anrufer.

PARAMETER	EINSTELLUNG IN DER EXCHANGE-VERWALTUNGSKONSOLE VERFÜGBAR?	BESCHREIBUNG
<i>ProtectUnauthenticatedVoiceMail</i>	Ja	<p>Der Parameter <i>ProtectUnauthenticatedVoiceMail</i> gibt an, ob die Mailbox-Server, die Anrufe für UM-aktivierten Benutzer, die eine um-Postfachrichtlinie zugeordnet entgegennehmen geschützte Sprachnachrichten erstellen. Diese Einstellung gilt auch, wenn eine Nachricht aus einer automatischen UM-Telefonzentrale an einen UM-aktivierten Benutzer gesendet wird. Die Standardeinstellung ist <code>None</code>. Dies bedeutet, dass kein Schutz auf Sprachnachrichten angewendet wird und der Anrufer wird nicht die Option aus, um das Markieren der Nachricht als privat angeboten. Wenn der Wert, um festgelegt ist <code>Private</code>, nur Nachrichten, die vom Anrufer als privat gekennzeichnet sind geschützt. Wenn der Wert, um festgelegt ist <code>All</code>, jede Sprachnachricht ist geschützt, unabhängig davon, ob, wenn die Nachricht vom Anrufer als privat gekennzeichnet wurden.</p>
<i>ProtectedVoiceMailText</i>	Ja	<p>Der Parameter <i>ProtectedVoiceMailText</i> gibt den Text in den Textkörper der Nachricht äußerer einer geschützte Voicemail-Nachricht enthalten sein. Dieser Text wird in allen e-Mail-Clientanwendungen angezeigt, die nicht geschützte Voicemail-Nachrichten unterstützen. Notiz, die eine Meldung immer durch UM bereitgestellt wird, wenn diese Eigenschaft, um festgelegt wird <code>Null</code> enthält oder leer ist.</p>
<i>RequireProtectedPlayOnPhone</i>	Ja	<p>Der Parameter <i>RequireProtectedPlayOnPhone</i> gibt an, ob Benutzer die um-Postfachrichtlinie zugeordnet erzwungen werden, um die geschützte Sprachnachricht über das Telefon (mithilfe der Wiedergabe über Telefon) zu überwachen. Der Standardwert lautet <code>\$false</code>. Wenn der Wert festgelegt ist <code>\$true</code>, der audio MediaPlayer auf geschützte Voicemail-Formulare in Outlook oder Outlook Web App als deaktiviert angezeigt werden. Beachten Sie, dass der Text Preview für die Sprachnachricht immer zugegriffen werden kann. Der Benutzer kann nicht die Audiodatei mit Media Player Software oder verwenden Sie den eingebetteten MediaPlayer, um die Sprachnachricht zu überwachen.</p>

PARAMETER	EINSTELLUNG IN DER EXCHANGE-VERWALTUNGSKONSOLE VERFÜGBAR?	BESCHREIBUNG
<code>AllowVoiceResponseToOtherMessageTypes</code>	Ja	Der Parameter <code>AllowVoiceResponseToOtherMessageTypes</code> gibt an, ob Anrufer, die für Outlook Voice Access Zugriff auf ihre e-Mails authentifiziert haben eine VoIP-Antwort, um e-Mail-Nachrichten und Besprechungsanfragen erstellen können.

Weitere Informationen zum Verwalten von Einstellungen für geschützte Voicemail finden Sie unter [Geschützte Voicemail-Prozeduren](#) oder [Set-UMMailboxPolicy](#).

## SMS-Benachrichtigungen und geschützte Voicemail

Benutzer, die ihr UM-Konto so konfiguriert haben, dass beim Empfang von Sprachnachrichten eine Textnachricht (SMS-Benachrichtigung) an ihr Mobiltelefon gesendet wird, empfangen im Nachrichtenteil der Textnachricht zusätzlich eine Audiotranskription (Voicemailvorschau) des Texts. Für geschützte Sprachnachrichten stellt dies jedoch ein Sicherheitsrisiko dar, da der Inhalt von Sprachnachrichten immer geschützt werden sollte.

Wenn Unified Messaging eine Textbenachrichtigung für eine Sprachnachricht erstellt, wird überprüft, ob die Sprachnachricht als privat markiert wurde. In diesem Fall wird der transkribierte Audiotext nicht der Textnachricht hinzugefügt, die an das Mobiltelefon gesendet wird. Stattdessen wird der folgende Text in die Textnachricht eingefügt: "Greifen Sie auf diese geschützte Voicemailnachricht mithilfe von Outlook Voice Access zu."

# Geschützte Voicemail-Prozeduren

18.12.2018 • 2 minutes to read

Konfigurieren von Voicemail aus authentifizierter Anrufer

Konfigurieren geschützter Voicemail von nicht authentifizierten Anrufern

Aktivieren oder Deaktivieren der Multimediameldungswiedergabe von geschützten Sprachnachrichten

Geben Sie den Text, der für e-Mail-Clients angezeigt, die Windows Rights Management nicht unterstützen

# Konfigurieren von Voicemail aus authentifizierter Anrufer

18.12.2018 • 4 minutes to read

Sie können Unified Messaging dazu konfigurieren, eingehende Anrufe entgegenzunehmen, und dann festlegen, ob Voicemailnachrichten durch Verschlüsselung geschützt werden sollen. Wenn eine Sprachnachricht geschützt ist, gilt Folgendes:

- Die Nachricht wird in Microsoft Outlook und in Outlook Web App als Privat gekennzeichnet.
- Die Sprachnachricht kann nur vom vorgesehenen Empfänger geöffnet werden.
- Der Empfänger kann auf die Sprachnachricht antworten, sie jedoch nicht an einen Empfänger weiterleiten, der nicht in der ursprünglichen Sprachnachricht enthalten war.

Diese Einstellung gilt für Sprachnachrichten, die an UM-aktivierte Benutzer gesendet werden, wenn diese ein Gespräch nicht entgegennehmen. Diese Einstellung gilt auch, wenn Anrufer sich über Outlook Voice Access bei ihrem Postfach anmelden und anschließend eine Sprachnachricht erstellen und senden.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit Verfahren für geschützte Voicemail finden Sie unter [Geschützte Voicemail-Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren von geschützten Voicemails von authentifizierten Anrufern mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Aktivieren Sie auf der Seite **UM-Postfachrichtlinie > Geschützte Voicemail** unter **Sprachnachricht von authentifizierten Anrufern schützen** eine der folgenden Optionen:
  - **None:** Verwenden Sie diese Einstellung, wenn Sie nicht, dass die angewendeten Dokumentschutztyp an alle Sprachnachrichten an UM-aktivierte Benutzer gesendet möchten.
  - **Privat:** Verwenden Sie diese Einstellung, wenn Sie möchten Unified Messaging Protection nur auf Sprachnachrichten anwenden, die vom Anrufer als privat gekennzeichnet wurden.
  - **Alle:** Verwenden Sie diese Einstellung, wenn Sie Unified Messaging Protection auf alle VoIP-Nachrichten, die nicht als privat gekennzeichnet einschließlich anwenden möchten.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie geschützte Voicemail aus authentifizierter Anrufer

In diesem Beispiel werden alle authentifizierter Anrufer auf die um-Postfachrichtlinie Sprachnachrichten verhindert **MyUMMailboxPolicy**.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy ProtectAuthenticatedVoiceMail -All
```

# Konfigurieren geschützter Voicemail von nicht authentifizierten Anrufern

18.12.2018 • 4 minutes to read

Sie können Unified Messaging für die Annahme eines eingehenden Anrufs konfigurieren und anschließend festlegen, ob Voicemailnachrichten durch Verschlüsselung geschützt werden. Eine geschützte Voicemailnachricht bedeutet Folgendes:

- Die Nachricht wird in Microsoft Outlook und in Outlook Web App als Privat gekennzeichnet.
- Die Sprachnachricht kann nur vom vorgesehenen Empfänger geöffnet werden.
- Der Empfänger kann die Sprachnachricht beantworten, er kann sie aber nicht an einen Benutzer weiterleiten, der in der ursprünglichen Sprachnachricht nicht enthalten war.

Diese Einstellung gilt für Sprachnachrichten, die an UM-aktivierte Benutzer gesendet werden, wenn diese ein Gespräch nicht entgegennehmen. Diese Einstellung gilt auch für direkt an UM-aktivierte Benutzer gesendete Sprachnachrichten, wenn der Anrufer eine automatische UM-Telefonzentrale verwendet.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit Verfahren für geschützte Voicemail finden Sie unter [Geschützte Voicemail-Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren von vor nicht authentifizierten Anrufern geschützter Voicemail mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie auf der Seite **UM-Postfachrichtlinie > Geschützte Voicemail** unter **Sprachnachrichten vor nicht authentifizierten Anrufern schützen** eine der folgenden Optionen aus:
  - **None:** Verwenden Sie diese Einstellung, wenn Sie nicht, dass die angewendeten Dokumentschutztyp an alle Sprachnachrichten an UM-aktivierte Benutzer gesendet möchten.
  - **Privat:** Verwenden Sie diese Einstellung, wenn Sie möchten Unified Messaging Protection nur auf Sprachnachrichten anwenden, die vom Anrufer als privat gekennzeichnet wurden.
  - **Alle:** Verwenden Sie diese Einstellung, wenn Sie Unified Messaging Protection auf alle VoIP-Nachrichten, die nicht als privat gekennzeichnet einschließlich anwenden möchten.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie geschützte Voicemail aus nicht authentifizierter Anrufer

In diesem Beispiel wird allen nicht authentifizierter Anrufer auf die um-Postfachrichtlinie alle Sprachnachrichten verhindert **MyUMMailboxPolicy**.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -ProtectUnauthenticatedVoiceMail -All
```

# Aktivieren oder Deaktivieren der Multimediamiedergabe von geschützten Sprachnachrichten

18.12.2018 • 5 minutes to read

Für Benutzer, die geschützte Voicemailnachrichten empfangen, kann für das Abhören der Nachrichten die Verwendung der Funktion "Wiedergabe über Telefon" erzwungen werden. Falls die Clientsoftware keine Rechteverwaltung unterstützt, müssen die Benutzer Outlook Voice Access zum Abhören von Nachrichten verwenden.

Zum Abhören von Sprachnachrichten können UM-aktivierte Benutzer (Unified Messaging) entweder die Wiedergabe über Telefon oder Multimedia-Software auf einem Computer oder Mobilgerät verwenden. Bei der Multimediamiedergabe kann ein UM-aktivierter Benutzer zum Abhören der Sprachnachricht eine Medienwiedergabe über die Computerlautsprecher oder auf einem Mobilgerät verwenden.

## NOTE

Geschützte Sprachnachrichten sind nur bei Clients verfügbar, die eine Version von Outlook mit Unterstützung der Rechteverwaltung verwenden. Falls die Clientsoftware keine Rechteverwaltung unterstützt, müssen die Benutzer Outlook Voice Access zum Abhören der Sprachnachrichten verwenden.

Standardmäßig ist der Wert der Eigenschaft **RequireProtectedPlayOnPhone** in einer UM-Postfachrichtlinie auf "False" eingestellt. Das bedeutet, dass UM-aktivierte Benutzer, die dieser UM-Postfachrichtlinie zugeordnet sind, geschützte Sprachnachrichten wie folgt abhören können:

- Verwenden von Outlook Voice Access.
- Verwenden der integrierten Medienwiedergabe oder Drücken der Schaltfläche "Wiedergabe über Telefon" in Outlook 2010 oder einer höheren Version.
- Verwenden der integrierten Medienwiedergabe oder Drücken der Schaltfläche "Wiedergabe über Telefon" in Outlook Web App.

Ist dieser Wert auf "True" eingestellt, ist die Multimediamiedergabe geschützter Sprachnachrichten nicht zulässig. UM-aktivierte Benutzer, die einer UM-Postfachrichtlinie zugeordnet sind, für die dieser Wert festgelegt ist, können geschützte Sprachnachrichten nur wie folgt abhören:

- Verwenden von Outlook Voice Access.
- Verwenden der Schaltfläche "Wiedergabe über Telefon" in Outlook 2010 oder einer höheren Version.
- Verwenden der Schaltfläche "Wiedergabe über Telefon" in Outlook Web App.

Diese Einstellung ist insbesondere dann sinnvoll, wenn UM-aktivierte Benutzer öffentliche Computer, Laptops an öffentlich zugänglichen Orten oder die Medienwiedergabe ihres Mobilgeräts zum Abhören von Sprachnachrichten verwenden, die private Informationen enthalten können.

Weitere Verwaltungsaufgaben im Zusammenhang mit Verfahren zum Schutz von Voicemail finden Sie unter [Geschützte Voicemail-Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren oder Deaktivieren der Multimediamiedergabe geschützter Sprachnachrichten mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie unter **UM-Postfachrichtlinien** wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten**
3. Aktivieren Sie auf der Seite **UM-Postfachrichtlinie > Geschützte Voicemail** das Kontrollkästchen neben "**Wiedergabe über Telefon" für geschützte Sprachnachrichten anfordern**", um diese Einstellung zu aktivieren. Deaktivieren Sie das Kontrollkästchen, um diese Einstellung zu deaktivieren.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren des geschützten Sprachnachrichten Multimediamiedergabe

In diesem Beispiel können Benutzer, die mit dem Namen der UM-Postfachrichtlinie zugeordnet sind **MyUMMailboxPolicy** um wiederzugeben geschützte Voicemail-Nachrichten mit einem MediaPlayer.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -RequireProtectedPlayOnPhone $false
```

In diesem Beispiel wird verhindert, dass Benutzer, die mit dem Namen der UM-Postfachrichtlinie zugeordnet sind **MyUMMailboxPolicy** geschützt Sprachnachrichten mit einem MediaPlayer wiedergeben.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -RequireProtectedPlayOnPhone $true
```

# Geben Sie den Text, der für e-Mail-Clients angezeigt, die Windows Rights Management nicht unterstützen

18.12.2018 • 4 minutes to read

Sie können den an Benutzer gesendeten Text angeben, wenn dieser eine geschützte Sprachnachricht empfängt, ihr E-Mail-Client aber die Verwaltung von Informationsrechten (IRM) oder Windows-Rechteverwaltung nicht unterstützt.

Der Zugriff auf geschützte Voicemail kann nur über E-Mail-Clients erfolgen, die die Windows-Rechteverwaltung unterstützen, oder wenn ein UM-aktivierter Benutzer mit Outlook Voice Access auf eine geschützte Sprachnachricht zugreift.

Geschützte Voicemail ist verschlüsselt. Wenn eine Sprachnachricht geschützt ist, gilt Folgendes:

- Die Nachricht wird in Microsoft Outlook und in Outlook Web App als Privat gekennzeichnet.
- Die Sprachnachricht kann nur vom vorgesehenen Empfänger geöffnet werden.
- Der Empfänger hat zwar die Möglichkeit, auf die Sprachnachricht zu antworten, er kann sie jedoch nicht an Benutzer weiterleiten, die nicht als Empfänger in der ursprünglichen Sprachnachricht enthalten waren.

Beim Senden einer geschützten Sprachnachricht an einen Benutzer, dessen E-Mail-Client keine Windows-Rechteverwaltung unterstützt und der nicht mit Outlook Voice Access auf die Nachricht zugreift, wird eine E-Mail-Nachricht mit dem von Ihnen angegebenen Text an diesen Benutzer gesendet. Dieser Text sollte Anweisungen zu den Schritten enthalten, die der angerufene Teilnehmer ausführen muss, um die geschützte Sprachnachricht empfangen zu können.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit Verfahren für geschützte Voicemail finden Sie unter [Geschützte Voicemail-Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Angeben des anzugegenden Texts für E-Mail-Clients, die keine Windows-Rechteverwaltung unterstützen

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  

2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten**  

3. Geben Sie auf der Seite **UM-Postfachrichtlinie > Geschützte Voicemail** unter **Nachricht, die an Benutzer gesendet werden soll, die keine Unterstützung durch Windows-Rechteverwaltung haben** den Meldungstext in das Textfeld ein.
4. Klicken Sie auf **Speichern**.

Verwenden von Exchange Online PowerShell, geben Sie den Text, der für e-Mail-Clients angezeigt, die Windows Rights Management nicht unterstützen

In diesem Beispiel gibt den Text an, der Benutzer mit dem Namen der UM-Postfachrichtlinie zugeordnet angezeigt  
**MyUMMailboxPolicy** besitzen e-Mail-Clients, die Windows Rights Management nicht unterstützen.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -ProtectedVoiceMailText "Your email client software does not support Protected Voice Mail. Please contact the Help Desk."
```

# Zulassen, dass Voice Mailbenutzer Anrufe weitergeleitet werden sollen

18.12.2018 • 11 minutes to read

Das Feature für Mailboxansageregeln wurde erstmals in Exchange 2010 vorgestellt. Mit diesem Feature können für Voicemail aktivierte Benutzer steuern, wie eingehende Anrufe behandelt werden sollen. Mailboxansageregeln werden auf ähnliche Weise auf eingehende Anrufe angewendet wie Posteingangsregeln auf eingehende E-Mails.

Mailboxansageregeln werden für einen für Voicemail aktivierten Benutzer mit Outlook oder Outlook Web App erstellt und konfiguriert. Die Regeln werden zusammen mit anderen Spracheinstellungen im Postfach des Benutzers gespeichert. Für ein UM-aktiviertes Postfach können insgesamt neun Mailboxansageregeln eingerichtet werden. Diese Regeln gelten unabhängig von den Posteingangsregeln, die vom Benutzer eingerichtet werden, und schmälern nicht das Speicherkontingent für Posteingangsregeln.

Wenn ein Benutzer für Unified Messaging (UM) und Voicemail aktiviert ist, werden standardmäßig keine Mailboxansageregeln konfiguriert. Wird ein eingehender Anruf vom Voicemailsysteem entgegengenommen, wird der Anrufer aufgefordert, eine Sprachnachricht zu hinterlassen. Aber auch wenn der Anrufer keine Aufforderung erhält, kann er eine Sprachnachricht für den Benutzer hinterlassen.

Wenn das Voicemailsysteem nur die eingehenden Anrufe der Benutzer entgegennehmen soll und die Benutzer nur eine Sprachnachricht aufzeichnen möchten, müssen Sie keine Mailboxansageregeln erstellen. Wenn Sie jedoch Bedingungen oder Aktionen einrichten möchten, können Sie dazu den Abschnitt **Mailboxansageregeln** auf der Seite **Voicemail** in Outlook Web App verwenden. Verwenden Sie zum Erstellen, Bearbeiten und Löschen von Mailboxansageregeln den Abschnitt **Mailboxansageregeln**.

## Anatomie der Mailboxansageregeln

Eine Mailboxansageregel besteht aus zwei Teilen: Bedingungen und Aktionen. Sie können eine oder mehrere Bedingungen mit einer einzelnen Mailboxansageregel verknüpfen. Die Mailboxansageregel wird nur verarbeitet, wenn alle Bedingungen für die Regel erfüllt sind. Sie können auch eine oder mehrere Aktionen mit einer einzelnen Mailboxansageregel verknüpfen. Diese Aktionen bestimmen, welche Optionen dem Anrufer bei Verarbeiten der Mailboxansageregel angeboten werden.

Mailboxansageregeln unterstützen die folgenden Bedingungen:

- Von wem der eingehende Anruf stammt
- Die Tageszeit
- Frei/Gebucht-Kalenderstatus
- Ob automatische Antworten für E-Mail aktiviert sind

Die folgenden Aktionen werden unterstützt:

- Mich anrufen
- Anrufer an eine andere Person übergeben
- Eine Sprachnachricht hinterlassen

Wenn Benutzer eine benutzerdefinierte Begrüßung für eine Mailboxansageregel aufzeichnen, müssen sie beim Konfigurieren der Mailboxansageregel die Menüoption in die benutzerdefinierte Begrüßung integrieren.

Andernfalls generiert Unified Messaging keine Menüansage, um den Anrufer darüber zu informieren, welche Optionen er wählen kann. Nachdem die benutzerdefinierte Begrüßung wiedergegeben wurde, wartet der Server auf die Eingabe des Anrufers. Ist keine Menüoption in der Begrüßung enthalten, erfolgt keine Eingabe durch den Anrufer, und dieser wird vom Server gefragt, ob er noch in der Leitung ist.

## Bedingungen

Bedingungen sind Regeln, die auf Mailboxansageregeln angewendet werden können. Durch eine Kombination von Bedingungen können Sie mehrere Mailboxansageregeln erstellen, die bei Erfüllung der Bedingungen ausgelöst werden. Wenn Sie eine Standardregel erstellen möchten, die bei jedem Anruf angewendet wird, erstellen Sie eine Regel ohne jegliche Bedingungen.

Zum Einrichten von Mailboxansageregeln können drei Bedingungen verwendet werden:

- Anrufer-ID
- Tageszeit
- Frei/Gebucht-Status

## Aktionen

Anhand von Aktionen wird definiert, was geschehen soll, wenn eine Bedingung erfüllt wird. Es gibt zwei Aktionsarten:

- Suchanruf
- Anrufweiterleitung

### Hinzufügen einer Aktion für "Mich suchen"

Wenn ein Anrufer "Mich suchen" auswählt, versucht das Voicemailsystem, Sie unter bis zu zwei verschiedenen Telefonnummern zu erreichen, und anschließend wird der Anrufer mit Ihnen verbunden (sofern Sie unter einer der Telefonnummern erreichbar sind).

- Sie können Text angeben, der dem Anrufer vorgelesen wird. Wenn Sie z. B. "In dringenden Fällen" eingeben, um Anrufer zu informieren, dass sie diese Aktion nur dann auswählen sollen, wenn Sie ein wirklich wichtiges Anliegen haben, lautet die Ansage des Voicemailsystems "Drücken Sie in dringenden Fällen die Taste 1."
- Sie müssen die Aktion für "Mich suchen" mit der Nummer auf der Telefontastatur verknüpfen, die der Anrufer zur Auswahl dieser Aktion drückt. Im obigen Beispiel ist die Nummer, die der Anrufer drücken muss, um Sie unter der oder den angegebenen Telefonnummern zu erreichen, die Taste **1**.
- Als Nächstes müssen Sie ein oder zwei Telefonnummern eingeben, die vom Voicemailsystem gewählt werden sollen. Wenn Sie zwei Telefonnummern angeben, wird die zweite Nummer gewählt, wenn Sie unter der ersten Telefonnummer nicht erreichbar sind. Jeder angegebenen Telefonnummer ist eine Dauer zugeordnet. Die Dauer ist der Zeitraum, in dem das Voicemailsystem die Telefonnummer anwählt, ehe es mit der nächsten Telefonnummer fortfährt. Alternativ kehrt das Voicemailsystem zum Optionsmenü zurück, wenn Sie nicht erreichbar sind.
- Nachdem Sie diese Informationen eingegeben haben, klicken Sie auf **Übernehmen**, um die Einstellungen für "Mich suchen" zu speichern.

### Hinzufügen von Aktionen für die Anrufweiterleitung

Durch Einrichten einer Aktion des Typs "Anrufweiterleitung" haben Anrufer die Möglichkeit, an die Telefonnummer einer anderen Person weitergeleitet zu werden. Wenn Sie einen eingehenden Anruf an eine

andere Telefonnummer oder einen anderen Kontakt weiterleiten möchten, sind verschiedene Optionen verfügbar.

- Sie können Text angeben, der dem Anrufer vorgelesen wird. Sie können z. B. "In wichtigen Fällen" eingeben, um den Anrufer zu informieren, dass er diese Option nur auswählen soll, wenn er ein wichtiges Anliegen hat, das er mit jemandem besprechen muss.
- Sie müssen die Aktion **Anrufweiterleitung** der Nummer auf der Telefontastatur zuordnen, die der Anrufer zur Auswahl dieser Aktion drückt.
- Wenn Sie die Anrufweiterleitung auswählen, müssen Sie eine Person oder Telefonnummer angeben, an die der Anrufer weitergeleitet wird. Sie können eine Telefonnummer oder einen Kontakt auswählen, die bzw. der angerufen werden soll, wenn der Anrufer die richtige Taste auf der Telefontastatur drückt. Wenn Sie einen Kontakt angeben, der sich im Unternehmensverzeichnis befindet, versucht das Voicemailsystem, den Anruf an die Durchwahl dieses Kontakts weiterzuleiten.
- Neben einer Person oder Telefonnummer, an die der Anrufer weitergeleitet wird, müssen Sie auch die Nummer der Taste auf der Telefontastatur angeben, die der Anrufer zur Auswahl der Anrufweiterleitung drückt.
- Wenn Sie diese Informationen eingegeben haben, klicken Sie auf **Übernehmen**, um die Einstellungen für die Anrufweiterleitung zu speichern.

## Auswählen einer Mailboxansageregel für jeden eingehenden Anruf

Nach dem Erstellen und Konfigurieren von Mailboxansageregeln geht Unified Messaging wie folgt vor:

1. Bestimmen, ob der Benutzer Mailboxansageregeln erstellt hat. Ist dies nicht der Fall, bietet UM dem Anrufer die Option an, eine Sprachnachricht zu hinterlassen.
2. Wurden eine oder mehrere Mailboxansageregeln konfiguriert, wertet UM jede dieser Regeln aus. Die erste Regel, deren Bedingungen erfüllt sind, wird verarbeitet.
3. Findet UM nach der Auswertung aller Regeln keine Regel, deren Bedingungen alle erfüllt sind, fordert UM den Anrufer auf, eine Sprachnachricht zu hinterlassen.

## Wählregeln

Je nach Konfiguration einer Mailboxansageregel kann ein eingehender Anruf zu einer Anrufübergabe führen. In diesem Fall unterliegt die Zieltelefonnummer für die Übergabe den Wählregeln und -einschränkungen der UM-Postfachrichtlinie, der die angerufene Partei zugeordnet ist. Weitere Informationen zu Outdialing- und Wählregeln und -einschränkungen finden Sie unter [Autorisieren von Benutzern für Anrufe](#).

### Aktivieren/Deaktivieren von Mailboxansageregeln

Standardmäßig werden Mailboxansageregeln automatisch für UM-aktivierte Benutzer aktiviert. Sie können Mailboxansageregeln jedoch für Benutzer deaktivieren, indem Sie das Feature in einer UM-Postfachrichtlinie oder im Postfach des Benutzers deaktivieren. Ausführliche Informationen zum Aktivieren oder Deaktivieren von Mailboxansageregeln finden Sie in folgenden Themen:

- [Ermöglichen Sie oder verhindern Sie, dass Benutzer in der gleichen UM-Postfachrichtlinie erstellen Aufruf von mailboxansageregeln](#)
- [Ermöglichen Sie oder verhindern Sie, dass einen Benutzer erstellen Aufruf von mailboxansageregeln](#)

# Weiterleiten von Anrufen Prozeduren

18.12.2018 • 2 minutes to read

Ermöglichen Sie oder verhindern Sie, dass einen Benutzer erstellen Aufruf von mailboxansageregeln

Ermöglichen Sie oder verhindern Sie, dass Benutzer in der gleichen UM-Postfachrichtlinie erstellen Aufruf von mailboxansageregeln

[Erstellen einer Mailboxansageregel](#)

[Anzeigen und Verwalten einer Mailboxansageregel](#)

[Aktivieren oder Deaktivieren einer Mailboxansageregel für einen Benutzer](#)

[Entfernen einer Mailboxansageregel für einen Benutzer](#)

# Ermöglichen Sie oder verhindern Sie, dass einen Benutzer erstellen Aufruf von mailboxansageregeln

18.12.2018 • 3 minutes to read

Sie können angeben, ob einzelne Benutzer in der Lage sein sollen, ihre eigenen Regeln für die Mailboxansage zu erstellen und zu verwalten, indem sie ihre Postfacheigenschaften konfigurieren. Standardmäßig können diese Benutzer Anrufbeantwortungsregeln erstellen.

Durch Konfigurieren von Mailboxansageregeln für einen UM-Wählplan oder eine UM-Postfachrichtlinie können Sie Mailboxansageregeln für mehrere Benutzer aktivieren oder deaktivieren, die für Unified Messaging (UM) aktiviert sind.

## NOTE

Diese Funktion kann nicht mit der Exchange-Verwaltungskonsole konfiguriert werden. Sie müssen zum Aktivieren oder Deaktivieren von Mailboxansageregeln die Shell verwenden.

Informationen zu weiteren Verwaltungsaufgaben zum Zulassen, dass Benutzer Anrufe weiterleiten, finden Sie unter [Weiterleiten von Anrufen Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass das Postfach des Benutzers UM-aktiviert wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen für die Verfahren in diesem Thema finden Sie unter [Tastenkombinationen in der Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Bitten Sie in den Exchange-Foren um Hilfe. Besuchen Sie die Foren unter [Exchange Server](#), [Exchange Online](#) oder [Exchange Online Protection](#)..

## Verwenden der Shell zum Aktivieren oder Deaktivieren von Regeln für die Mailboxansage für einen UM-aktivierten Benutzer

In diesem Beispiel werden für den Benutzer "tony@contoso.com" die Regeln für die Mailboxansage aktiviert.

```
Set-UMMailbox -Identity tony@contoso.com -CallAnsweringRulesEnabled $true
```

In diesem Beispiel werden für den Benutzer "thorsten@contoso.com" die Regeln für die Mailboxansage deaktiviert.

```
Set-UMMailbox -Identity tony@contoso.com -CallAnsweringRulesEnabled $false
```

# Ermöglichen Sie oder verhindern Sie, dass Benutzer in der gleichen UM-Postfachrichtlinie erstellen Aufruf von mailboxansageregeln

18.12.2018 • 3 minutes to read

Sie können das Konfigurieren von Mailboxansageregeln durch Benutzer, die einer UM-Postfachrichtlinie zugeordnet sind, zulassen oder unterbinden. Wenn die Option zum Konfigurieren von Mailboxansageregeln für einen UM-Wählplan deaktiviert ist, steht diese Funktion für UM-aktivierte Benutzer, die dieser UM-Postfachrichtlinie unterliegen, nicht zur Verfügung. Die Option ist standardmäßig aktiviert.

Informationen zu weiteren Verwaltungsaufgaben zum Zulassen, dass Benutzer Anrufe weiterleiten, finden Sie unter [Weiterleiten von Anrufen Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren oder Deaktivieren von Mailboxansageregeln für eine UM-Postfachrichtlinie mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie unter **UM-Postfachrichtlinien** wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten** .
3. Aktivieren Sie auf der Seite **UM-Postfachrichtlinien** das Kontrollkästchen neben **Konfigurieren von Mailboxansageregeln durch Benutzer zulassen**.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren von mailboxansageregeln auf einer um-Postfachrichtlinie

In diesem Beispiel können Benutzer, die die um-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy` anrufbeantwortungsregeln zu erstellen.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowCallAnsweringRules $true
```

In diesem Beispiel wird verhindert, dass Benutzer, die die um-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy` Entgegennehmen von Anrufen erstellen Regeln.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowCallAnsweringRules $false
```

# Erstellen einer Mailboxansageregel

18.12.2018 • 5 minutes to read

Exchange Online PowerShell können Sie um eine oder mehrere mailboxansageregeln für einen Benutzer zu erstellen. Sie können auch das Cmdlet **New-UMCallAnsweringRule** in einem Powershellskript verwenden, um Anruf antwortenden Regeln für mehrere Benutzer erstellen.

Mailboxansageregeln werden auf ähnliche Weise auf eingehende Anrufe angewendet wie Posteingangsregeln auf eingehende E-Mails. Wenn ein Benutzer für Unified Messaging (UM) aktiviert ist, werden standardmäßig keine Mailboxansageregeln konfiguriert. Dennoch werden eingehende Anrufe vom Voicemailsystem beantwortet, und Anrufer werden aufgefordert, eine Sprachnachricht zu hinterlassen.

## NOTE

Für Unified Messaging (UM) aktivierte Benutzer können sich bei Outlook Web App anmelden, um Mailboxansageregeln zu erstellen, zu verwalten und zu entfernen.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit Mailboxansageregeln finden Sie unter [Weiterleiten von Anrufen Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-mailboxansageregeln" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass das Postfach des Benutzers UM-aktiviert wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Sie können nur Exchange Online PowerShell verwenden, um dieses Verfahren ausführen. Gewusst wie: Öffnen Sie Exchange Online PowerShell in Ihrer lokalen Exchange-Organisation finden Sie unter **Exchange Online PowerShell öffnen**. So verwenden Sie Windows PowerShell für die Verbindung zu Exchange Online finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

Verwenden Sie Exchange Online PowerShell, um eine

## mailboxansageregel zu erstellen.

In diesem Beispiel wird die mailboxansageregel `MyCallAnsweringRule` im Postfach für Tony Smith mit der Priorität von 2.

```
New-UMCallAnsweringRule -Name MyCallAnsweringRule -Priority 2 -Mailbox tonysmith
```

In diesem Beispiel wird die mailboxansageregel `MyCallAnsweringRule` im Postfach für Tony Smith und führt die folgenden Aktionen aus:

- Die Mailboxansageregel wird auf zwei Anrufer-IDs festgelegt.
- Die Priorität der Mailboxansageregel wird auf 2 festgelegt.
- Die Mailboxansageregel wird so festgelegt, dass Anrufer die Ansage unterbrechen können.

```
New-UMCallAnsweringRule -Name MyCallAnsweringRule -CallerIds "1,4255550100,,","1,4255550123,,," -Priority 2 -CallersCanInterruptGreeting $true -Mailbox tonysmith
```

In diesem Beispiel wird die mailboxansageregel `MyCallAnsweringRule` im Postfach für Tony Smith und führt die folgenden Aktionen aus:

Die Priorität der Mailboxansageregel wird auf 2 festgelegt.

Für die Mailboxansageregel werden Tastenzuordnungen erstellt.

Wenn der Anrufer die Voicemail des Benutzers erreicht und der Status des Benutzers auf "Gebucht" gesetzt ist, hat der Anrufer folgende Möglichkeiten:

```
- <span data-ttu-id="f69a7-139">Er drückt die Taste 1 und wird an den Empfang mit der Durchwahl 45678 weitergeleitet.</span><span class="sxs-lookup"><span data-stu-id="f69a7-139">Press the 1 key and be transferred to a receptionist at extension 45678.</span></span>

- <span data-ttu-id="f69a7-140">Er drückt die Taste 2, sodass in dringenden Fällen die Suchfunktion verwendet und zuerst die Durchwahl 23456 und anschließend 45671 angerufen wird.</span><span class="sxs-lookup"><span data-stu-id="f69a7-140">Press the 2 key so the Find Me feature will be used for urgent issues, ring extension 23456 first, and then ring extension 45671.</span></span>
```

```
New-UMCallAnsweringRule -Name MyCallAnsweringRule -Priority 2 -Mailbox tonysmith -ScheduleStatus 0x4 - -KeyMappings "1,1,Receptionist,,,45678,","5,2,Urgent Issues,23456,23,45671,50,,"
```

# Anzeigen und Verwalten einer Mailboxansageregel

18.12.2018 • 5 minutes to read

Sie können Exchange Online PowerShell anzeigen oder konfigurieren Sie eine oder mehrere mailboxansageregeln für einen Benutzer. Sie können auch die Cmdlets **Get-UMCallAnsweringRule** oder **Set-umcallansweringrule** **können** in einem Powershellskript zum Anzeigen oder Anruf antwortenden Regeln für mehrere Benutzer verwalten.

Mailboxansageregeln werden auf ähnliche Weise auf eingehende Anrufe angewendet wie Posteingangsregeln auf eingehende E-Mails. Wenn ein Benutzer für Unified Messaging (UM) aktiviert ist, werden standardmäßig keine Mailboxansageregeln konfiguriert. Dennoch werden eingehende Anrufe vom Voicemailsysteem beantwortet, und Anrufer werden aufgefordert, eine Sprachnachricht zu hinterlassen.

## IMPORTANT

Für Unified Messaging (UM) aktivierte Benutzer können sich bei Outlook Web App anmelden, um Mailboxansageregeln zu erstellen, zu verwalten und zu entfernen.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit Mailboxansageregeln finden Sie unter [Weiterleiten von Anrufen Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-mailboxansageregeln" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass das Postfach des Benutzers UM-aktiviert wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Sie können nur Exchange Online PowerShell verwenden, um dieses Verfahren ausführen. Herstellen einer Verbindung mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

Verwenden Sie Exchange Online PowerShell, um eine

## mailboxansageregel anzeigen

Sie können die Eigenschaften für eine einzelne Mailboxansageregel oder für eine Liste von Mailboxansageregeln in einem UM-aktivierten Benutzerpostfach abrufen.

In diesem Beispiel wird eine formatierte Liste aller Mailboxansageregeln im UM-aktivierten Postfach eines Benutzers zurückgegeben.

```
Get-UMCallAnsweringRule-Mailbox tonysmith | Format-List
```

Dieses Beispiel zeigt die Eigenschaften der mailboxansageregel `MyUMCallAnsweringRule`.

```
Get-UMCallAnsweringRule -Identity MyUMCallAnsweringRule
```

## Verwenden Sie Exchange Online PowerShell, um eine mailboxansageregel zu konfigurieren.

Sie können eine Mailboxansageregel konfigurieren oder ändern, die im Postfach eines Benutzers gespeichert ist. Sie können folgende Bedingungen festlegen:

- Von wem der eingehende Anruf stammt
- Tageszeit
- Frei/Gebucht-Kalenderstatus
- Ob automatische Antworten für E-Mail aktiviert sind

Sie können außerdem folgende Aktionen angeben:

- Mich anrufen
- Anrufer an eine andere Person übergeben
- Eine Sprachnachricht hinterlassen

In diesem Beispiel wird die Priorität auf 2 festgelegt, in der mailboxansageregel `MyCallAnsweringRule`, die im Postfach für Tony Smith vorhanden.

```
Set-UMCallAnsweringRule -Mailbox tonysmith -Name MyCallAnsweringRule -Priority 2
```

In diesem Beispiel werden die folgenden Aktionen in der mailboxansageregel `MyCallAnsweringRule` im Postfach für Tony Smith:

- Die Mailboxansageregel wird auf zwei Anrufer-IDs festgelegt.
- Die Priorität der Mailboxansageregel wird auf 2 festgelegt.
- Die Mailboxansageregel wird so festgelegt, dass Anrufer die Ansage unterbrechen können.

```
Set-UMCallAnsweringRule -Name MyCallAnsweringRule -CallerIds "1,4255550100,,," "1,4255550123,,," -Priority 2 - CallersCanInterruptGreeting $true -Mailbox tonysmith
```

Dieses Beispiel ändert den Frei/Gebucht-Status in Abwesend in der mailboxansageregel `MyCallAnsweringRule` im Postfach für Tony Smith und die Priorität auf 2 festgelegt.

```
Set-UMCallAnsweringRule -Name MyCallAnsweringRule -Priority 2 -Mailbox tonysmith@contoso.com -ScheduleStatus  
0x8
```

# Aktivieren oder Deaktivieren einer Mailboxansageregel für einen Benutzer

18.12.2018 • 5 minutes to read

Sie können die Exchange Online PowerShell verwenden, aktivieren oder deaktivieren eine oder mehrere mailboxansageregeln für einen Benutzer. Sie können auch die Cmdlets **Enable-UMCallAnsweringRule** oder **Disable-UMCallAnsweringRule** in einem Powershellskript verwenden, aktivieren oder deaktivieren eine oder mehrere mailboxansageregeln für mehrere Benutzer.

Mailboxansageregeln werden auf ähnliche Weise auf eingehende Anrufe angewendet wie Posteingangsregeln auf eingehende E-Mails. Wenn ein Benutzer für Unified Messaging (UM) aktiviert ist, werden standardmäßig keine Mailboxansageregeln konfiguriert. Dennoch werden eingehende Anrufe vom Voicemailsystem beantwortet, und Anrufer werden aufgefordert, eine Sprachnachricht zu hinterlassen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Mailboxansageregeln finden Sie unter [Weiterleiten von Anrufen Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-mailboxansageregeln" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass das Postfach des Benutzers UM-aktiviert wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Herstellen einer Verbindung mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um eine mailboxansageregel zu aktivieren

Wenn ein Anruf erstellten mailboxansageregel an, wird es aktiviert. Sie können Exchange Online PowerShell verwenden, um eine mailboxansageregel zu aktivieren, die zuvor deaktiviert wurde. Aktivieren einen Anruf, dass mailboxansageregel an das Cmdlet **Enable-UMCallAnsweringRule** zum Abrufen der mailboxansageregel,

einschließlich der Bedingungen und Aktionen für eine angegebene mailboxansageregel aktiviert.

Dieses Beispiel aktiviert die mailboxansageregel `MyUMCallAnsweringRule` im Postfach für Tony Smith.

```
Enable-UMCallAnsweringRule -Identity MyUMCallAnsweringRule -Mailbox tonysmith
```

Im Beispiel wird die Option `WhatIf` verwendet, um zu testen, ob die Regel die Anrufbeantwortung `MyUMCallAnsweringRule` im Postfach für Tony Smith ist, kann jetzt aktiviert werden soll und ob Fehler innerhalb des Befehls vorhanden sind.

```
Enable-UMCallAnsweringRule -Identity MyUMCallAnsweringRule -Mailbox tonysmith -WhatIf
```

Dieses Beispiel aktiviert die mailboxansageregel `MyUMCallAnsweringRule` im Postfach für Tony Smith und Sie werden aufgefordert, die der Benutzer angemeldet, um sicherzustellen, dass die mailboxansageregel wird aktiviert werden soll.

```
Enable-UMCallAnsweringRule -Identity MyUMCallAnsweringRule -Mailbox tonysmith -Confirm
```

## Verwenden Sie Exchange Online PowerShell, um eine mailboxansageregel zu deaktivieren.

Durch das Deaktivieren einer Mailboxansageregel wird verhindert, dass die Regel abgerufen und verarbeitet wird, wenn ein eingehender Anruf empfangen wird. Wenn Sie eine Mailboxansageregel erstellen, sollte Sie sie während der Einrichtung von Bedingungen und Aktionen deaktivieren. Dadurch wird verhindert, dass die Mailboxansageregel beim Empfang eines eingehenden Anrufs verarbeitet wird, bevor Sie die Mailboxansageregel ordnungsgemäß konfiguriert haben.

In diesem Beispiel wird die mailboxansageregel deaktiviert `MyUMCallAnsweringRule` im Postfach für Tony Smith.

```
Disable -UMCallAnsweringRule -Identity MyUMCallAnsweringRule -Mailbox tonysmith
```

In diesem Beispiel wird die Option `WhatIf` testen, ob die Regel die Anrufbeantwortung `MyUMCallAnsweringRule` im Postfach für Tony Smith ist, kann jetzt deaktiviert werden und wenn innerhalb des Befehls Fehler aufgetreten sind.

```
Disable -UMCallAnsweringRule -Identity MyUMCallAnsweringRule -Mailbox tonysmith -WhatIf
```

In diesem Beispiel wird die mailboxansageregel deaktiviert `MyUMCallAnsweringRule` im Postfach für Tony Smith und fordert die angemeldeten Benutzers zu bestätigen, dass sie die Anrufbeantwortung Deaktivieren der Regel.

```
Disable-UMCallAnsweringRule -Identity MyUMCallAnsweringRule -Mailbox tonysmith -Confirm
```

# Entfernen einer Mailboxansageregel für einen Benutzer

18.12.2018 • 3 minutes to read

Exchange Online PowerShell können Sie um eine oder mehrere mailboxansageregeln für einen Benutzer zu entfernen. Sie können auch das Cmdlet **Remove-UMCallAnsweringRule** in einem Powershellskript verwenden, um eine entfernen oder mehr mailboxansageregeln für mehrere Benutzer.

Mailboxansageregeln werden auf ähnliche Weise auf eingehende Anrufe angewendet wie Posteingangsregeln auf eingehende E-Mails. Wenn ein Benutzer für Unified Messaging (UM) aktiviert ist, werden standardmäßig keine Mailboxansageregeln konfiguriert. Dennoch werden eingehende Anrufe vom Voicemailsystem beantwortet, und Anrufer werden aufgefordert, eine Sprachnachricht zu hinterlassen.

## NOTE

Für Unified Messaging (UM) aktivierte Benutzer können sich bei Outlook Web App anmelden, um Mailboxansageregeln zu erstellen, zu verwalten und zu entfernen.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit Mailboxansageregeln finden Sie unter [Weiterleiten von Anrufen Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-mailboxansageregeln" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass ein UM-Wählplan erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieses Verfahrens, dass das Postfach des Benutzers UM-aktiviert wurde. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Sie können nur Exchange Online PowerShell verwenden, um dieses Verfahren ausführen. Herstellen einer Verbindung mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

Verwenden Sie Exchange Online PowerShell, um eine

## mailboxansageregel zu entfernen.

Dieses Beispiel entfernt die mailboxansageregel `MyUMCallAnsweringRule` aus dem Postfach eines Benutzers. Das Postfach des Benutzers ist das Postfach des Benutzers, der das Cmdlet ausführen.

```
Remove-UMCallAnsweringRule -Identity MyUMCallAnsweringRule
```

Dieses Beispiel entfernt die mailboxansageregel `MyUMCallAnsweringRule` aus dem Postfach von Tony Smith.

```
Remove-UMCallAnsweringRule -Identity MyUMCallAnsweringRule -Mailbox tonysmith
```

# Zulassen der Anzeige von Voicemailtranskriptionen für Benutzer

18.12.2018 • 14 minutes to read

Voicemailvorschau ist ein Feature, das Benutzern zur Verfügung steht, die ihre Voicemailnachrichten Abrufen von Unified Messaging (UM) erhalten. Voicemailvorschau verbessert die vorhandene UM voicemailfunktionalität durch eine Textversion audio Aufzeichnungen bereitstellen. Der Text der e-Mail VoIP wird in e-Mail-Nachrichten in Microsoft Outlook Web App, Outlook 2010 und höher und in anderen unterstützten e-Mail-Programmen angezeigt. Weitere Informationen finden Sie unter [Microsoft Sprachtechnologien](#).

## Müssen Benutzer ein bestimmtes E-Mail-Programm verwenden?

Nein. Die Voicemailvorschau ist im Nachrichtentext eines beliebigen E-Mail-Programms (einschließlich mobiler Programme) enthalten. Wenngleich Benutzer andere E-Mail-Programme für den Empfang von Sprachnachrichten verwenden können, bieten Outlook und Outlook Web App das beste Benutzererlebnis. Wenn der Benutzer z. B. in Outlook 2010 und höheren Versionen im Voicemailvorschautext auf ein bestimmtes Wort klickt, beginnt die Wiedergabe der Sprachnachricht bei diesem Wort. Dies ist nützlich, um einen bestimmten Teil einer Sprachnachricht wiederzugeben.

## Können Benutzer nach bestimmten Voicemailnachrichten suchen?

Ja. Wörter und Sätze im Voicemailvorschautext werden automatisch indiziert, sodass Sprachnachrichten in den Suchergebnissen enthalten sind. In Outlook 2010 und höheren Versionen oder in Outlook Web App können Benutzer über das Feld **Audionotizen** ferner Text zu einer Sprachnachricht hinzufügen. Diese Notizen werden bei Suchvorgängen ebenso berücksichtigt, um das Auffinden einer Nachricht zu vereinfachen.

## Weshalb lautet der Name der Funktion "Voicemailvorschau"?

Es ist wichtig, bei den Benutzern keine falschen Erwartungen zu wecken. Bei der Voicemailvorschau stimmt der Text nicht unbedingt exakt mit der Sprachnachricht des Anrufers überein. Tatsächlich weicht der Text üblicherweise etwas ab. Wenn der Name "Transkription" lauten würde, ließe dies ein besseres Ergebnis vermuten, als im Allgemeinen erreicht werden kann. Der Begriff "Vorschau" weist jedoch darauf hin, dass der Leser einen ersten Einblick in den Inhalt der Sprachnachricht erhält, was der tatsächlichen Funktion eher entspricht.

## Wodurch wird die Zuverlässigkeit des Voicemailvorschautexts erhöht oder verringert?

Die Zuverlässigkeit des Voicemailvorschautexts hängt von einer Vielzahl von Faktoren ab, die manchmal nicht beeinflusst werden können. Die folgenden Faktoren können jedoch dazu beitragen, die Zuverlässigkeit des Voicemailvorschautexts zu erhöhen:

- Der Anrufer hinterlässt eine einfache Sprachnachricht, die keine Umgangssprache, technischen Fachwörter oder ungewöhnlichen Wörter und Sätze enthält.
- Der Anrufer spricht eine Sprache, die problemlos vom Voicemailsysteem erkannt und übersetzt werden kann. Im Allgemeinen wird die Zuverlässigkeit der Vorschau erhöht, wenn die Anrufer beim Hinterlassen von Sprachnachrichten nicht zu schnell oder zu leise und ohne starken Dialekt sprechen.
- Die Sprachnachricht enthält keine Hintergrundgeräusche, Echos oder Tonaussetzer.

# Welche Sprachen können mit der Voicemailvorschau verwendet werden?

Voicemailvorschautext ist in den folgenden Sprachen verfügbar:

- Englisch (USA) (en-US)
- Englisch (Kanada) (en-CA)
- Französisch (Frankreich) (fr-FR)
- Italienisch (it-IT)
- Polnisch (pl-PL)
- Portugiesisch (Portugal) (pt-PT)
- Spanisch (Spanien) (es-ES)

Wenn Sie über eine lokale oder Hybridbereitstellung von UM verfügen, können die UM-Sprachpakete aus dem [Microsoft Download Center](#) heruntergeladen werden.

Bei einer lokalen oder Hybridbereitstellung können nach der Installation eines UM-Sprachpaketes die Wählpläne und automatischen Telefonzentralen für die gewählte Sprache konfiguriert werden. Bei der Online-Version müssen Sie keine Sprachpakete installieren. Viele Unternehmen verfügen über nur einen UM-Wählplan. Es wird versucht, eine Voicemailvorschau in der Standardsprache des Wählplans zu erstellen. Die Standardsprache muss die Voicemailvorschau jedoch unterstützen. Ein UM-Wählplan kann lediglich zum Erstellen von Voicemailvorschauen in jeweils einer Sprache konfiguriert werden.

Um Unified Messaging für die Bereitstellung von Voicemailvorschauen in einer anderen Sprache als Englisch (USA) zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Voicemailvorschau in der gewünschten Sprache unterstützt wird.
2. Laden Sie bei einer lokalen oder Hybridbereitstellung das gewünschte UM-Sprachpaket herunter, und installieren Sie es. Durch das Herunterladen und Installieren des Sprachpaketes wird die Standardsprache des Wählplans nicht konfiguriert.
3. Konfigurieren Sie für den Wählplan die Sprache, die für die Voicemailvorschau verwendet wird. Weitere Informationen finden Sie unter [Festlegen der Standardsprache für einen Wählplan](#).

Wie Voicemailvorschautext in den unterstützten Sprachen angezeigt wird, hängt vom Typ der gesendeten Sprachnachricht ab. Es gibt zwei Typen:

- **Sprachnachrichten, die bei nicht beantworteten Anrufen aufgezeichnet werden**

Bei diesen Nachrichten wird die für die Voicemailvorschau verwendete Sprache anhand der Sprache des Anrufers und basierend darauf bestimmt, ob die Sprache unterstützt wird. Wenn der Anrufer z. B. eine Sprachnachricht auf Italienisch hinterlässt, wird der Voicemailvorschautext auf Italienisch angezeigt, wenn diese Sprache für den Wählplan konfiguriert wurde. Wenn der Anrufer jedoch eine Nachricht auf Japanisch hinterlässt, umfasst die Nachricht keinen Voicemailvorschautext, da diese Sprache nicht verfügbar ist.

- **Von einem Outlook Voice Access-Benutzer gesendete Sprachnachrichten**

Bei Nachrichten, die von einem Outlook Voice Access-Benutzer gesendet werden, wird die Sprache der Voicemailvorschau vom Voicemailadministrator bestimmt. Für den Text der Voicemailvorschau wird die Sprache des Voicemailsystems verwendet. Wenn jedoch ein Anrufer, der keine von der Voicemailvorschau unterstützte Sprache spricht, Outlook Voice Access zum Hinterlassen einer Nachricht verwendet, enthält die Nachricht keinen Voicemailvorschautext. Weitere Informationen zu Outlook Voice Access finden Sie unter

[Einrichten von Outlook Voice Access.](#)

## Erkennt UM, wenn eine Voicemailvorschau ungenau ist?

Der Zuverlässigkeitswert wird für jede Voicemailvorschau bestimmt, die in einer Sprachnachricht enthalten ist. Das Voicemailsystem misst, inwieweit der Ton in der Aufzeichnung den Wörtern, Zahlen und Ausdrücke entspricht. Wenn Entsprechungen mühelos gefunden werden, ist der Zuverlässigkeitswert hoch. Ein hoher Zuverlässigkeitswert weist üblicherweise auf eine hohe Genauigkeit der Vorschau hin.

Wenn der Zuverlässigkeitswert unter einem bestimmten Wert liegt, wird über dem Text der Voicemailvorschau der Satz **Voicemailvorschau (geringe Zuverlässigkeit)** angezeigt. Bei einem geringen Zuverlässigkeitswert ist es wahrscheinlich, dass der Voicemailvorschautext ungenau ist.

Unified Messaging verwendet zum Berechnen der Vorschauzuverlässigkeit die automatische Spracherkennung. Es kann jedoch nicht ermittelt werden, welche Wörter richtig und welche falsch wiedergegeben werden.

UM versucht jedoch, die Zuverlässigkeit der Voicemailvorschau weiter zu verbessern. Es wird beispielsweise versucht, die Telefonnummer des Anrufers (falls bereitgestellt) mit den persönlichen Kontakten des Benutzers und dem Adressbuch Ihrer Organisation sowie Kontakten in sozialen Netzwerken abzugleichen. Wenn UM eine Übereinstimmung ermittelt, werden bei der automatischen Spracherkennung für die Sprachaufzeichnung der Name des Anrufers sowie die Standardlisten mit Namen und Wörtern aufgenommen.

### Kann die Voicemailvorschau verwendet werden, wenn sie nicht absolut zuverlässig ist?

Das Benutzererlebnis bei der Voicemailvorschau wird verbessert, wenn die Benutzer nicht versuchen, die Vorschau Wort für Wort zu lesen. Stattdessen sollten sie nach Namen, Telefonnummern und Hinweisen wie "Rückruf" oder "Möchte mit Ihnen sprechen" suchen, anhand derer sich der Grund des Anrufs ermitteln lässt.

Der Zweck der Voicemailvorschau ist nicht die präzise Wiedergabe des Nachrichteninhalts, sondern die Funktion soll lediglich dazu beitragen, u. a. die folgenden Fragen zu beantworten:

- Bezieht sich diese Sprachnachricht auf meine Arbeit?
- Ist diese Sprachnachricht wichtig für mich?
- Hat der Anrufer eine Telefonnummer hinterlassen? Unterscheidet sich diese Nummer von den Telefonnummern in meiner Liste?
- Betrachtet der Anrufer diese Sprachnachricht als dringend?
- Muss ich ein Meeting verlassen, um den Anrufer zurückzurufen?
- Ich habe einen Anruf zur Bestätigung einer Anfrage erwartet. Handelt es sich um diesen Anruf?

## Kann die Voicemailvorschau aktiviert oder deaktiviert werden?

Ja. Bei aktiverter Voicemailvorschau können Benutzer die Funktion über Outlook 2010 oder eine höhere Version oder Outlook Web App aktivieren oder deaktivieren. Die Sprache des Wählplans muss die Voicemailvorschau jedoch unterstützen, und das entsprechende UM-Sprachpaket muss installiert sein.

Wenngleich bei Verwendung von Outlook 2010 oder einer höheren Version und Outlook Web App dieselben Einstellungen für die Voicemailvorschau verwendet werden, wird unterschiedlich auf diese Einstellungen zugegriffen:

### Outlook Web App

In Outlook Web App klicken Benutzer auf **Einstellungen > Telefon > Voicemail**, um auf die Einstellungen für die Voicemailvorschau zuzugreifen. Auf der Seite **Voicemail** stehen die Einstellungen unter **Voicemailvorschau** zur Verfügung.

Standardmäßig sind beide Voicemailvorschauoptionen verfügbar, wenn ein Benutzer für Unified Messaging aktiviert ist. Wenn der UM-Wählplan für die Verwendung eines UM-Sprachpakets mit Unterstützung der Voicemailvorschau konfiguriert sind, erstellt Unified Messaging in den folgenden Fällen eine Voicemailvorschau für die Benutzer:

- Ein Anrufer hinterlässt eine Voicemailnachricht, weil sein Anruf nicht entgegengenommen wird.
- Ein UM-aktivierter Benutzer meldet sich an Outlook Voice Access an und zeichnet eine Sprachnachricht für einen oder mehrere Empfänger auf.

Wenn ein Anrufer eine Sprachnachricht hinterlässt und die Option **Vorschautext in Sprachnachrichten einschließen, die ich erhalte** aktiviert ist, erstellt Unified Messaging eine Voicemailvorschau in der E-Mail-Nachricht, fügt die Audiodatei an und sendet die Nachricht an das Postfach des Empfängers. Sie können diese Option deaktivieren, wenn die für den Wählerplan konfigurierte Sprache die Voicemailvorschau nicht unterstützt und Sie keine Voicemailvorschauen in Voicemailnachrichten aufnehmen möchten.

Wenn sich Benutzer an Outlook Voice Access anmelden und eine Sprachnachricht an einen anderen Benutzer senden, können Sie das Kontrollkästchen **Vorschautext in Sprachnachrichten einschließen, die ich mit Outlook Voice Access sende** deaktivieren. Dies bietet sich beispielsweise an, wenn Sprachnachrichten in einer Sprache gesendet werden, die von der Voicemailvorschau nicht unterstützt wird, oder sie die Voicemailvorschau nicht in die Sprachnachricht einschließen möchten, da diese zu lang ist.

# Ratgeber für Voicemailvorschau

18.12.2018 • 10 minutes to read

Microsoft Exchange Unified Messaging (UM) umfasst ein Feature namens Voicemailvorschau, das Voicemailnachrichten mithilfe der automatischen Spracherkennung eine Textversion der Voicemailaudiodatei hinzufügt. Die automatische Spracherkennung ist nicht immer exakt, insbesondere wenn sie für die Aufzeichnung von Ton mit unbekannten Stimmen und Geräuschen über ein Telefon verwendet wird. Einige Organisationen benötigen konsistent fehlerfreie (oder nahezu fehlerfreie) Abschriften von Sprachnachrichten. Das Voicemailvorschau-Partnerprogramm unterstützt diese Organisationen bei der Erfüllung dieser Anforderungen.

Voicemailvorschau verwendet [Microsoft sprachtechnologien](#), um eine Textversion audio Aufzeichnungen bereitzustellen. Der Voice Mail Text wird in e-Mail-Nachrichten in Microsoft Outlook Web App, Outlook 2010 oder höher und anderen e-Mail-Programmen angezeigt.

Wenn Sie einen Benutzer in einer lokalen oder einer Hybridbereitstellung für UM aktivieren, wird standardmäßig eine Voicemailvorschau gesendet, wenn ein unterstütztes UM-Sprachpaket installiert ist. Wenn Sie einen Benutzer in Exchange Online für UM aktivieren, werden alle UM-Sprachpakete installiert. Voicemailvorschau wird jedoch nicht in allen installierten Sprachen unterstützt.

Manche Voicemailvorschau-Partner bieten erweiterte Unterstützung und Dienste für die Transkription der Voicemailvorschau an. Diese Partner beschäftigen Mitarbeiter für die Korrektur von Voicemail-Transkriptionen, die mithilfe von ASR erstellt wurden. Jeder Voicemailvorschau-Partner muss bestimmte Anforderungen erfüllen, um für die Zusammenarbeit mit Exchange UM zertifiziert zu werden.

Wenn Sie feststellen, dass die an Ihre Benutzer gesendete Voicemailvorschau nicht präzise genug ist, können Sie sich an einen der zertifizierten Voicemailvorschau-Partner wenden, die unter [Microsoft Pinpoint](#) aufgeführt sind, und sich gegen zusätzliche Kosten bei diesen anmelden.

## Übersicht

Wenn Unified Messaging den Ton einer Sprachnachricht aufzeichnet, wird die automatische Spracherkennung verwendet, um eine Vorschau des Texts in der Audiodatei zu erstellen und die gesamte Sprachnachricht zur Zustellung an den Benutzer zu übermitteln. Für jede erstellte Sprachnachricht legt Unified Messaging eine Zuverlässigkeitssstufe für die Voicemailvorschau in jeder Nachricht fest. Diese gibt an, wie genau der Ton in der Aufzeichnung den Wörtern, Zahlen und Phrasen in der Nachricht entspricht. Wenn das System problemlos Übereinstimmungen findet, ist die Zuverlässigkeitssstufe hoch. Einer höheren Zuverlässigkeitssstufe ist im Allgemeinen eine höhere Genauigkeit zugeordnet.

Die Genauigkeit des Voicemailvorschautexts hängt von vielen Faktoren ab, und manchmal können diese Faktoren nicht gesteuert werden. Der Text ist jedoch wahrscheinlich genauer, wenn:

- Es wird eine einfache Sprachnachricht hinterlassen, in der der Anrufer keine umgangssprachlichen Begriffe, technischen Jargon oder seltenen Wörter oder Ausdrücke verwendet.
- der Benutzer eine einfach zu erkennende und vom Voicemailsysteem zu konvertierende Sprache verwendet. Im Allgemeinen enthalten die Sprachnachrichten von Benutzern, die nicht zu schnell oder weich sprechen und keinen starken Akzent haben, genauere Sätze und Ausdrücke.
- Die Sprachnachricht enthält keine Hintergrundgeräusche, Echos oder Tonaussetzer.

Viele Kunden, die Unified Messaging verwenden, bestätigen, dass die Voicemailvorschau ausreichend exakt für ihre Benutzer ist. Wenn die automatische Spracherkennung jedoch auf Aufzeichnungen von unbekannten

Stimmen oder Hintergrundgeräuschen am Telefon verwendet wird, ist der Voicemailvorschau-Text nicht vollständig exakt. Wenn die Zuverlässigkeitssstufe konstant niedrig ist oder die empfangene Voicemailvorschau nicht exakt ist, können Sie die Genauigkeit der vom Benutzer empfangenen Voicemailvorschauen wie folgt erhöhen:

- Melden Sie sich für einen Sprachtranskriptionsdienst eines Voicemailvorschau-Partners an.
- Nachdem Sie sich bei einem Voicemailvorschau-Partner angemeldet haben, richten Sie den Partner für die Arbeit mit UM ein. Weitere Informationen zum Konfigurieren von UM für einen Voicemailvorschau-Partner finden Sie unter [Voicemailvorschau Partnerdienste für Benutzer konfigurieren](#).

Wenn Sie sich bei einem Voicemailvorschau-Partner anmelden, leiten die Exchange-Server in Ihrer Organisation Voicemailnachrichten mit angehängter Audiodatei an den Voicemailvorschau-Partner weiter, anstatt einen Voicemailvorschautext für Sprachnachrichten zu erstellen und die Sprachnachrichten an das Postfach des Benutzers weiterzuleiten. Die E-Mail mit dem vom Voicemailvorschau-Partner erstellten Voicemailvorschautext wird anschließend an die Exchange-Server in Ihrer Organisation übermittelt, um an das Postfach des Empfängers zugestellt zu werden.

#### **IMPORTANT**

Es wird empfohlen, dass alle Benutzer, die Unified Messaging bereitstellen möchten ein UM-Experten zu erhalten. Ein UM-Spezialisten können Sie sicherstellen, dass es ein reibungsloser Übergang zu um-WÄHLPLAN aus einem älteren Voicemail-System ist. Durchführen einer neuen bereitstellungs oder Aktualisieren von einer älteren Voicemail-Systems erfordert beträchtliche Kenntnisse über VoIP-Gateways, IP-PBX-Anlagen, Nebenstellenanlagen, Session Border Controller (SBCs) und Unified Messaging. Finden Sie weitere Informationen zur Kontaktaufnahme mit einem UM-Spezialisten [Spezialisten für Microsoft Exchange Server Unified Messaging \(UM\)](#) oder [Microsoft Hindernissen bei für Unified Messaging](#).

## Voicemail-Partnerprogramm für Exchange Unified Messaging

Um zertifizierter Voicemailpartner für die Interoperabilität mit Exchange UM zu werden, muss der Partner die in der Interoperabilitätsspezifikation für Voicemailpartner (Voice Mail Preview Interoperability Specification) enthaltenen Anforderungen implementieren, und die Partnerlösung muss von einem unabhängigen Zertifikatanbieter zertifiziert werden.

## Für Exchange Unified Messaging zertifizierte Voicemailvorschau-Partner

Wenn Sie Unified Messaging bereits in Ihrer Organisation bereitgestellt haben und einen zertifizierten Voicemailvorschau-Partner für Transkriptionsdienste suchen, finden Sie weitere Informationen unter [Microsoft PinPoint](#). Diese Softwareanbieter wurden für die Interoperabilität mit Exchange UM zertifiziert.

## Konfigurieren von Voicemailvorschau-Partnern

Nach der Konfiguration von UM werden Sprachnachrichten mit Ton an dedizierte Voicemailvorschau-Partner weitergeleitet, die dann aus der Audiodatei den Voicemailvorschautext erstellen. Damit Benutzer die Voicemailvorschau mit ihrer Sprachnachricht im Postfach erhalten können, müssen Sie jedoch eine UM-Postfachrichtlinie konfigurieren, Benutzer der UM-Postfachrichtlinie zuordnen und die Benutzer bestätigen lassen, dass sie Voicemailvorschauen in ihren Sprachnachrichten in Outlook 2010 oder höher bzw. in Outlook Web App empfangen kann. Weitere Informationen zum Konfigurieren von UM für einen Voicemailvorschau-Partner finden Sie unter [Voicemailvorschau Partnerdienste für Benutzer konfigurieren](#).

## Unterstützung für VoIP- oder Mediengateways und IP-PBX

Das Konfigurieren von VoIP-Gateways und IP-Nebenstellenanlagen für die Organisation ist eine schwierige Bereitstellungsaufgabe, die ordnungsgemäß durchgeführt werden muss, damit Unified Messaging für einen Voicemailvorschau-Partner erfolgreich bereitgestellt wird. Weitere Informationen zur Konfiguration von VoIP-Gateways und IP-Nebenstellenanlagen finden Sie unter [Telefonieratgeber für Exchange 2013](#) oder unter [Konfigurationshinweise zu unterstützten VoIP-Gateways, IP-Nebenstellenanlagen und Nebenstellenanlagen](#).

Das Testen der Interoperabilität von Exchange UM mit VoIP-Gateways wurde in das Microsoft Unified Communications Open Interoperability Program integriert. Weitere Informationen hierzu finden Sie unter [Microsoft Unified Communications Open Interoperability Program](#).

# Voice Mail Preview Prozeduren

18.12.2018 • 2 minutes to read

[Voicemailvorschau Partnerdienste für Benutzer konfigurieren](#)

[Legen Sie die Adresse des Partners Voicemailvorschau](#)

[Festlegen der ID des Voicemailvorschau-Partners](#)

[Festlegen der maximalen Nachrichtendauer für einen Voicemailvorschau-Partner](#)

[Legen Sie die maximale Verzögerung für einen Voicemailvorschau partner](#)

[Aktivieren von Voice Mail Preview für Benutzer](#)

[Deaktivieren von Voicemailvorschau für Benutzer](#)

# Voicemailvorschau Partnerdienste für Benutzer konfigurieren

18.12.2018 • 4 minutes to read

Sie können einen Voicemailvorschau-Partner für eine Unified Messaging-Postfachrichtlinie (UM) konfigurieren. Nachdem Sie die Einstellungen für den Voicemailvorschau-Partner konfiguriert haben, z. B. die ID und Adresse des Voicemailvorschau-Partners, gelten die von Ihnen konfigurierten Einstellungen für eine UM-Postfachrichtlinie für alle UM-aktivierten Benutzer, die dieser Postfachrichtlinie zugeordnet sind.

## NOTE

Sie müssen Exchange Online PowerShell verwenden, um eine Voicemailvorschau Partner zu konfigurieren.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Schritt 1: Anmelden bei einem Partnerdienst

Eine Liste zertifizierter Partner und detaillierte Anweisungen zum Anmelden finden Sie unter [Ratgeber für Voicemailvorschau](#) oder auf der Website [Microsoft PinPoint](#). Nachdem Sie sich angemeldet haben, stellt der Voicemailvorschau-Partner Ihnen eine Partner-ID und die SMTP-Adresse bereit, die Sie zum Weiterleiten von Sprachnachrichten verwenden.

In Schritt 2 wenden Sie die in Schritt 1 erhaltene Partner-ID und SMTP-Adresse auf die erforderlichen UM-Postfachrichtlinien an.

## Schritt 2: Festlegen der Adresse und ID des Voicemailvorschau-

## Partners

In diesem Beispiel wird der Partner Voicemailvorschau exumvmp@fabrikam.com-Adresse und die Partner-ID Voicemailvorschau CON123 2010 auf einem UM-Postfachrichtlinie mit dem Namen "myummailboxpolicy".

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -VoiceMailPreviewPartnerAddress exumvmp@fabrikam.com  
-VoiceMailPreviewPartnerAssignedID CON123-2010
```

## Schritt 3: Konfigurieren der erweiterten Einstellungen für den Voicemailvorschau-Partner

Wenn der Partner benutzerdefinierte Einstellungen erfordert, können Sie wie folgt zwei zusätzliche Parameter für den Voicemailvorschau-Partner festlegen:

- *VoiceMailPreviewPartnerMaxMessageDuration*
- *VoiceMailPreviewPartnerMaxDeliveryDelay*

In diesem Beispiel wird die maximale Dauer auf 300 Sekunden (5 Minuten) und die maximale Übermittlung Verzögerung auf 600 Sekunden (10 Minuten) auf einem UM-Postfachrichtlinie mit dem Namen "myummailboxpolicy".

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -VoiceMailPreviewPartnerMaxMessageDuration 300 -  
VoiceMailPreviewPartnerMaxDeliveryDelay 600
```

## Schritt 4: Zuordnen eines UM-aktivierten Benutzers zur UM-Postfachrichtlinie für einen Voicemailvorschau-Partner

Wenn Sie den Voicemailvorschau-Partnerdienst für einige, jedoch nicht für alle UM-aktivierten Benutzer in den UM-Wähleinstellungen konfigurieren möchten, müssen Sie eine neue UM-Postfachrichtlinie erstellen und die Partnereinstellungen konfigurieren. Wenn Sie diesen Vorgang abgeschlossen haben, können Sie die neue Richtlinie auf die ausgewählten UM-aktivierten Benutzer anwenden. Weitere Informationen zum Zuordnen von UM-aktivierten Benutzern zu einer UM-Postfachrichtlinie finden Sie in den folgenden Themen:

- [Zuweisen einer um-Postfachrichtlinie](#)
- [Set-UMMailbox](#)

Weitere Informationen zum Voicemailvorschau-Partnerprogramm finden Sie unter [Ratgeber für Voicemailvorschau](#).

# Legen Sie die Adresse des Partners Voicemailvorschau

18.12.2018 • 2 minutes to read

Sie können eine Partneradresse für die Voicemailvorschau für eine Unified Messaging-Postfachrichtlinie festlegen. Nachdem Sie die Partneradresse für die Voicemailvorschau für eine UM-Postfachrichtlinie festgelegt haben, wird die Einstellung auf alle UM-aktivierten Benutzer angewendet, die mit der Postfachrichtlinie verknüpft sind.

## NOTE

Sie müssen Exchange Online PowerShell verwenden, um eine Voicemailvorschau Partner Adresse festzulegen.

Weitere Informationen zum Voicemailvorschau-Partnerprogramm finden Sie unter [Ratgeber für Voicemailvorschau](#).

Weitere Verwaltungsaufgaben im Zusammenhang mit der Voicemailvorschau finden Sie unter [Voice Mail Preview Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um die Adresse des Partners Voice Mail Preview für eine um-Postfachrichtlinie festzulegen

In diesem Beispiel wird die Adresse des Partners Voicemailvorschau exumvmp@fabrikam.com auf einer um-Postfachrichtlinie "myummailboxpolicy" benannt.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -VoiceMailPreviewPartnerAddress exumvmp@fabrikam.com
```

# Legen Sie die Voicemailvorschau Partner-ID

18.12.2018 • 2 minutes to read

Sie können eine Voicemailvorschau-Partner-ID für eine Unified Messaging-Postfachrichtlinie (UM) festlegen. Nach dem Festlegen der Voicemailvorschau-Partner-ID für eine UM-Postfachrichtlinie wird die Einstellung auf alle UM-aktivierten Benutzer angewendet, die dieser UM-Postfachrichtlinie zugeordnet sind.

## NOTE

Sie müssen Exchange Online PowerShell verwenden, um die Partner-ID Voicemailvorschau einzustellen.

Weitere Informationen zum Voicemailvorschau-Partnerprogramm finden Sie unter [Ratgeber für Voicemailvorschau](#).

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit der Voicemailvorschau finden Sie unter [Voice Mail Preview Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell die Voicemailvorschau Partner-ID für eine um-Postfachrichtlinie festlegen

In diesem Beispiel wird die Partner-ID Voicemailvorschau CON123 2010 auf einem UM-Postfachrichtlinie mit dem Namen "myummailboxpolicy".

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy  
-VoiceMailPreviewPartnerAssignedID CON123-2010
```

# Legen Sie die maximale Dauer für einen Voicemailvorschau-partner

18.12.2018 • 2 minutes to read

Sie können die maximale Nachrichtendauer für einen Voicemailvorschau-Partner für eine UM-Postfachrichtlinie (Unified Messaging) festlegen. Nachdem Sie die maximale Nachrichtendauer festgelegt haben, wird die Einstellung auf alle UM-aktivierten Benutzer angewendet, die mit dieser Postfachrichtlinie verknüpft sind.

## NOTE

Sie müssen die Shell verwenden, um die maximale Nachrichtendauer für einen Voicemailvorschau-Partner festzulegen.

Weitere Informationen zum Voicemailvorschau-Partnerprogramm finden Sie unter [Ratgeber für Voicemailvorschau](#).

Weitere Verwaltungsaufgaben im Zusammenhang mit der Voicemailvorschau finden Sie unter [Voice Mail Preview Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen für die Verfahren in diesem Thema finden Sie unter **Tastenkombinationen in der Exchange-Verwaltungskonsole**.

## TIP

Liegt ein Problem vor? Bitten Sie in den Exchange-Foren um Hilfe. Besuchen Sie die Foren unter [Exchange Server](#), [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Shell zum Festlegen der maximalen Nachrichtendauer für einen Voicemailvorschau-Partner

In diesem Beispiel wird die maximale Nachrichtendauer für einen Voicemailvorschau-Partner für eine UM-Postfachrichtlinie mit dem Namen *MyUMMailboxPolicy* auf 300 Sekunden (5 Minuten) festgelegt.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -VoiceMailPreviewPartnerMaxMessageDuration 300
```

# Legen Sie die maximale Verzögerung für einen Voicemailvorschau partner

18.12.2018 • 2 minutes to read

Sie können die maximale Zustellungsverzögerung für einen Voicemailvorschau-Partner in einer Unified Messaging-Postfachrichtlinie (UM) festlegen. Nach dem Festlegen der maximalen Zustellungsverzögerung wird die Einstellung auf alle UM-aktivierten Benutzer angewendet, die dieser UM-Postfachrichtlinie zugeordnet sind.

## NOTE

Sie müssen Exchange Online PowerShell verwenden, um die maximale Verzögerung für einen Voicemailvorschau Partner festzulegen.

Weitere Informationen zum Voicemailvorschau-Partnerprogramm finden Sie unter [Ratgeber für Voicemailvorschau](#).

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit der Voicemailvorschau finden Sie unter [Voice Mail Preview Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell können Sie die maximale Verzögerung für Partner Voicemailvorschau festlegen

In diesem Beispiel wird die maximale Übermittlung Verzögerung 600 Sekunden (10 Minuten) auf einem UM-Postfachrichtlinie mit dem Namen "myummailboxpolicy".

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy - VoiceMailPreviewPartnerMaxDeliveryDelay 600
```

# Aktivieren von Voice Mail Preview für Benutzer

18.12.2018 • 2 minutes to read

Sie können die Funktion "Voicemailvorschau" für Benutzer aktivieren, die einer UM-Postfachrichtlinie (Unified Messaging) zugeordnet sind, falls diese deaktiviert wurde. Bei Aktivierung dieser Einstellung können Benutzer den Text einer Voicemailnachricht im Nachrichtentext einer E-Mail- oder Textnachricht empfangen. Die Option ist standardmäßig aktiviert.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren der Voicemailvorschau mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Aktivieren Sie auf der Seite **UM-Postfachrichtlinie > Allgemein** das Kontrollkästchen **Voicemailvorschau zulassen**.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell, Voicemailvorschau aktivieren

In diesem Beispiel können Benutzer, die die um-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy`, das

Voicemailvorschau-Feature verwenden.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowVoiceMailPreview $true
```

# Deaktivieren von Voicemailvorschau für Benutzer

18.12.2018 • 2 minutes to read

Sie können die Funktion "Voicemailvorschau" für Benutzer deaktivieren, die mit einer UM-Postfachrichtlinie verknüpft sind. Bei Deaktivierung dieser Einstellung wird verhindert, dass Benutzer den Text einer Voicemailnachricht im Nachrichtentext einer E-Mail- oder Textnachricht empfangen. Die Standardeinstellung ist "Aktiviert".

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Deaktivieren der Voicemailvorschau mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > Pläne UM-Wählpläne**, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** 
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten** 
3. Deaktivieren Sie auf der Seite **UM-Postfachrichtlinie > Allgemein** das Kontrollkästchen **Voicemailvorschau zulassen**.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell Voicemailvorschau deaktivieren

In diesem Beispiel wird verhindert, dass Benutzer, die die um-Postfachrichtlinie zugeordnet sind MyUMMailboxPolicy aus mit dem Feature Voice Mail Preview.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowVoiceMailPreview $false
```

# MWI in Exchange Online

18.12.2018 • 17 minutes to read

MWI (Message Waiting Indicator) ist eine Funktion, die sich bei den meisten Voicemailsystemen findet. Es informiert Benutzer darüber, dass Sie neue oder noch nicht abgehörte Voicemailnachrichten erhalten haben. In der Regel wird dabei durch eine Leuchtanzeige am Telefon eines Benutzers signalisiert, dass eine neue oder nicht abgehörte Voicemailnachricht vorliegt.

## Übersicht

MWI-Benachrichtigungen können alle Mechanismen beinhalten, die auf das Vorhandensein einer neuen oder nicht abgehörten Voicemail hinweisen. Die Nachricht kann in einer neuen E-Mail-Nachricht oder einer als ungelesen markierten Nachricht enthalten sein. Die MWI-Benachrichtigung kann in einer der folgenden Formen vorliegen:

- Eine von Microsoft Outlook oder Outlook Web App erkannte neue Sprachnachricht.
- Eine Leuchtanzeige an einem digitalen, analogen, USB- oder VoIP-Telefon.
- Besonderer Klingelton
- Symbole oder Schaltflächen auf dem Display eines digitalen, analogen, USB- oder VoIP-Telefons.
- Hervorgehobene Benachrichtigung in einer Softwareanwendung, wie zum Beispiel:
  - Lync 2010- und 2013-Desktopclients
  - Lync Mobile-Client-App für Windows Phone-, Microsoft Surface- und iOS-Geräte
- Eine Text- oder SMS (Short Messaging Service)-Nachricht, die an ein für den Empfang von Textnachrichten konfiguriertes Mobiltelefon gesendet wurde.

In Exchange Online wird eine Voicemail eines Benutzers in einem Postfach gespeichert. Der Zugriff kann über ein Telefon mit Outlook Voice Access, einen Desktopcomputer oder Laptop mit Outlook und Outlook Web App sowie Mobiltelefonclients erfolgen. Wenn ein Benutzer eine neue Sprachnachricht empfängt, wird diese in seinem Voicemailsuchordner angezeigt. Wird mit Outlook oder Outlook Web App auf die Sprachnachricht zugegriffen, wird die Sprachnachricht um eine E-Mail-Nachricht ergänzt.

Standardmäßig ist MWI für alle Benutzer aktiviert, die für UM (Unified Messaging) aktiviert sind. Es wird mit Einstellungen für eine UM-Postfachrichtlinie oder in den UM IP-Gateways gesteuert, die erstellt und mit einem UM-Wählplan verknüpft wurden. MWI kann auch mit geschützten Sprachnachrichten verwendet werden.

## MWI-Verwaltung

MWI kann durch Konfigurieren der Einstellungen auf zwei UM Komponenten verwaltet werden: UM-Postfachrichtlinien und UM-IP-Gateways. Für beide Komponenten UM können Sie aktivieren oder Deaktivieren von Benachrichtigungen MWI durch verwenden das Cmdlet **Set-UMMailboxPolicy** oder das Cmdlet **Set-UМИGateway** in Exchange Online PowerShell. Sie können auch die Einstellungen mithilfe der Exchange-Verwaltungskonsole (EAC) konfigurieren. Sie können den Status der Benachrichtigungen MWI anzeigen, mit dem Cmdlet **Get-UMMailboxPolicy** und das Cmdlet **Get-UМИgateway** in Exchange Online PowerShell oder indem Sie die Einstellungen in der Exchange-Verwaltungskonsole anzeigen.

### UM-Postfachrichtlinien und MWI

Sie erstellen eine UM-Postfachrichtlinie, um eine allgemeine Zusammenstellung von UM-Richtlinien und -

Einstellungen auf eine Gruppe von UM-aktivierten Postfächern anzuwenden. Mithilfe einer UM-Postfachrichtlinie können Sie beispielsweise PIN-Richtlinieneinstellungen, Wähleinschränkungen und MWI-Benachrichtigungen anwenden. Wird MWI für eine UM-Postfachrichtlinie aktiviert oder deaktiviert, werden auch alle UM-aktivierten Benutzer, die der UM-Postfachrichtlinie zugeordnet sind, aktiviert bzw. deaktiviert. Die MWI-Einstellung gilt für eine Teilmenge der Benutzer, die mit einem UM-Wählplan verknüpft sind. Weitere Informationen zu UM-Postfachrichtlinien und zum Aktivieren bzw. Deaktivieren von MWI für eine UM-aktivierte Benutzergruppe finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

Der Exchange-Verwaltungskonsole oder über das Cmdlet **Set-UMMailboxPolicy** können im Exchange Online PowerShell so konfigurieren Sie die Einstellung MWI wie in der folgenden Tabelle dargestellt.

#### **MWI-Einstellung für eine UM-Postfachrichtlinie**

PARAMETER	EINSTELLUNG IN DER EXCHANGE-VERWALTUNGSKONSOLE VERFÜGBAR?	BESCHREIBUNG
<i>AllowMessageWaitingIndicator</i>	Ja	<p>Der Parameter <i>AllowMessageWaitingIndicator</i> gibt an, ob Benutzer, die mit einer um-Postfachrichtlinie verknüpft sind MWI Benachrichtigungen empfangen können, wenn sie eine neue VoIP-Nachricht erhalten. Der Standardwert lautet <code>\$true</code>.</p> <p>Durch das Aktivieren dieser Einstellung werden den Benutzern, die einer UM-Postfachrichtlinie zugeordnet sind, bei Anrufen über ein UM-IP-Gateway MWI-Benachrichtigungen gesendet. Mit dieser Einstellung kann das UM-IP-Gateway SIP NOTIFY-Nachrichten an Telefone oder SIP-Endpunkte UM-aktivierter Benutzer empfangen oder senden.</p>

Weitere Informationen zum Verwalten von MWI-Einstellungen in einer UM-Postfachrichtlinie finden Sie in den folgenden Themen:

- [Verwalten einer UM-Postfachrichtlinie](#)
- [Aktivieren der MWI-Funktion \(Message Waiting Indicator\) für Benutzer](#)
- [Deaktivieren der Nachricht wartet Indicator \(MWI\) für Benutzer](#)
- [Set-UMMailboxPolicy](#)

#### **UM-IP-Gateways und MWI**

Wird MWI für ein UM-IP-Gateway deaktiviert, wird MWI für alle Benutzer deaktiviert, die eine Verbindung zu dem VoIP-Gateway oder der IP-Festnetztelefonanlage herstellen, das bzw. die als UM-IP-Gateway definiert ist. Wenn Sie MWI auf einem einzigen UM-IP-Gateway, das mit einem UM-Wählplan verknüpft ist, deaktivieren, werden möglicherweise MWI-Benachrichtigungen für alle UM-aktivierten Benutzer, die mit einem oder mehreren UM-Wählplänen bzw. einer oder mehreren UM-Postfachrichtlinien verknüpft sind, deaktiviert. Weitere Informationen zu UM-Postfachrichtlinien und zum Aktivieren bzw. Deaktivieren von MWI für eine UM-aktivierte Benutzergruppe finden Sie unter [Verwalten einer UM-Postfachrichtlinie](#).

Der Exchange-Verwaltungskonsole oder über das Cmdlet **Set-UMMailboxPolicy** können im Exchange Online PowerShell so konfigurieren Sie die Einstellung MWI wie in der folgenden Tabelle dargestellt.

#### **MWI-Einstellung für ein UM-IP-Gateway**

PARAMETER	EINSTELLUNG IN DER EXCHANGE-VERWALTUNGSKONSOLE VERFÜGBAR?	BESCHREIBUNG
<code>MessageWaitingIndicatorAllowed</code>	Ja	<p>Der Parameter <code>MessageWaitingIndicatorAllowed</code> gibt an, ob Sie aktivieren möchten, dass das UM-IP-Gateway benachrichtigen SIP-Nachrichten an Benutzer, die mit einem um-WÄHLPLAN gesendet werden. Der Standardwert lautet <code>\$true</code>.</p> <p>Wird diese Einstellung aktiviert, können für die vom UM-IP-Gateway empfangenen Anrufe Voicemailbenachrichtigungen an die Benutzer gesendet werden. Mit dieser Einstellung kann das UM-IP-Gateway MWI-Benachrichtigungen an UM-aktivierte Benutzer senden.</p>

Weitere Informationen zum Verwalten von MWI-Einstellungen finden Sie in den folgenden Themen:

- [Verwalten eines UM-IP-Gateways](#)
- [MWI \(Message Waiting Indicator\) für ein UM-IP-Gateway unterstützen](#)
- [Verhindern von MWI an einem UM-IP-Gateway](#)
- [Set-UMIPGateway](#)

## Textnachricht (SMS)-Benachrichtigungen für Voicemailnachrichten und entgangene Anrufe

Wie bereits erwähnt, ist eine MWI-Benachrichtigung jedes Verfahrens, mit dem die Existenz einer neuen Voicemailnachricht angegeben wird. Zusätzlich können mit den bereits erläuterten Verfahren Benutzer mit einer Textnachricht (auch als SMS (Short Message Service) bezeichnet) benachrichtigt werden, dass sie eine Sprachnachricht erhalten haben. Dabei handelt es sich um eine andere Art der MWI-Benachrichtigung bei neuen Sprachnachrichten als die bisher verwendete Anzeigeleichte oder andere Verfahren.

Wenn ein Anrufer eine neue Sprachnachricht hinterlassen hat, wird eine Textnachricht an das Mobiltelefon des Benutzers gesendet. Benutzer können auch eine Textnachricht erhalten, mit der sie informiert werden, wenn ihnen ein Anruf entgangen ist und keine Sprachnachricht hinterlassen wurde. Die Textnachricht mit der Benachrichtigung zu einem entgangenen Anruf kann zusammen mit der Benachrichtigung zu einer neuen Sprachnachricht an den Benutzer gesendet werden.

### NOTE

Die an einen Benutzer gesendete Textnachricht enthält eine Vorschau der Sprachnachricht.

Benachrichtigung Text verwenden unterschiedliche Einstellungen als die MWI-Einstellungen auf dem UM-IP-Gateway oder UM-Postfachrichtlinie. Text-Benachrichtigung für neue Voicemail und verpasste Anrufe werden für UM-Postfachrichtlinien und UM-Postfächer konfiguriert. Sie können aktivieren oder Deaktivieren von Benachrichtigungen über Textnachrichten von Text mithilfe von mit dem Cmdlet **Set-UMMailboxPolicy** und das Cmdlet **Set-UMMailbox** in Exchange Online PowerShell. Sie können den Status der Benachrichtigungen über Textnachrichten von Text mithilfe von mit dem Cmdlet **Get-UMMailboxPolicy** und das Cmdlet **Get-UMMailbox** anzeigen. Es ist nicht möglich, Text-Benachrichtigung in der Exchange-Verwaltungskonsole konfigurieren.

In der nachstehenden Tabelle sind die Parameter für ein UM-Postfach angegeben, die konfiguriert werden müssen, damit ein Benutzer Textnachrichten für Benachrichtigungen bei Sprachnachrichten und entgangenen Anrufen erhält.

### Einstellung der Benachrichtigungen per Textnachricht im Benutzerpostfach

PARAMETER	EINSTELLUNG IN DER EXCHANGE-VERWALTUNGSKONSOLE VERFÜGBAR?	BESCHREIBUNG
<i>UMSMSNotificationOption</i>	Nein	Gibt an, ob ein UM-aktivierten Benutzer Benachrichtigung für Voicemail nur Text für Voicemail und verpasste Anrufe entgegennehmen kann oder nicht, zum Empfangen von Benachrichtigungen zulässig ist. Die Werte für diesen Parameter sind: <code>VoiceMail</code> , <code>VoiceMailAndMissedCalls</code> , und <code>None</code> . Der Standardwert lautet <code>None</code> .

Weitere Informationen zum Verwalten von Einstellungen von Benachrichtigungen per Textnachricht im Benutzerpostfach finden Sie in den folgenden Themen:

- [Verwalten von Voicemail-Einstellungen für einen Benutzer](#)
- [Set-UMMailbox](#)

In der nachstehenden Tabelle ist der Parameter für eine UM-Postfachrichtlinie angegeben, der konfiguriert werden muss, damit ein Benutzer Textnachrichten für Benachrichtigungen bei Sprachnachrichten und entgangenen Anrufen erhält.

### Einstellung von Benachrichtigungen über Sprachnachrichten und verpasste Anrufe per Textnachricht in einer UM-Postfachrichtlinie

PARAMETER	EINSTELLUNG IN DER EXCHANGE-VERWALTUNGSKONSOLE VERFÜGBAR?	BESCHREIBUNG
<i>AllowSMSNotification</i>	Nein	Gibt an, ob UM-aktivierten Benutzer, deren Postfächer mit UM-Postfachrichtlinie zugeordnet sind, zum Empfangen von Text Nachricht Benachrichtigungen auf ihren Mobiltelefonen zulässig sind. Wenn dieser Parameter festgelegt ist, dass <code>\$true</code> , müssen Sie auch verwenden Sie das Cmdlet <b>Set-UMMailbox</b> und festlegen den <i>UMSMSNotificationOption</i> -Parameter für den UM-aktivierten Benutzer entweder <code>VoiceMail</code> oder <code>VoiceMailAndMissedCalls</code> . Der Standardwert lautet <code>\$true</code> .

Weitere Informationen zum Verwalten von Einstellungen für Benachrichtigungen per Textnachricht finden Sie in den folgenden Themen:

- [Verwalten einer UM-Postfachrichtlinie](#)
- [Set-UMMailboxPolicy](#)

Damit Textnachrichtbenachrichtigungen für Voicemail und entgangene Anrufe einwandfrei funktionieren, müssen

Sie die folgenden Aufgaben ausführen:

1. Verwenden Sie die Exchange-Verwaltungskonsole oder Exchange Online PowerShell zum Aktivieren des Benutzers für UM und verknüpfen sie mit der richtigen UM-Postfachrichtlinie ein.
2. Vergewissern Sie sich, dass der Parameter *AllowSMSNotification* festgelegt ist, auf die um-Postfachrichtlinie, die dem Benutzer verknüpft ist, `$true`. Den Parameter festlegen, um `$true`, führen Sie den folgenden Befehl:

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowSMSNotification $true
```

3. Aktivieren Sie auf das Postfach des Benutzers, Text-Benachrichtigung wenn der Parameter *UMSMSNotificationOption* auf `VoiceMailAndMissedCalls` oder `VoiceMail`.
4. Da die Standardeinstellung ist `None`, führen Sie den folgenden Befehl in Exchange Online PowerShell, und legen Sie die Option Text Nachricht Benachrichtigung entweder `VoiceMailAndMissedCalls` oder `VoiceMail`. Zum Beispiel:

```
Set-UMMailbox -Identity MyUMMailbox -UMSMSNotificationOption VoiceMailAndMissedCalls
```

#### IMPORTANT

Der Parameter *AllowSMSNotification* auf die um-Postfachrichtlinie und *UMSMSNotificationOption* auf das Postfach des Benutzers müssen beide festgelegt sein `$true` für SMS-Benachrichtigungen zu arbeiten.

Zusätzlich zur Konfiguration der UM-Postfachrichtlinie und des Benutzerpostfachs für die Aktivierung von Textnachrichtbenachrichtigungen bei neuen Sprachnachrichten und entgangenen Anrufen muss der Benutzer Textnachrichtbenachrichtigungen aktivieren und konfigurieren, wenn er sich bei Outlook Web App anmeldet. Zur Einrichtung und Konfiguration von Textnachrichtbenachrichtigungen müssen die folgenden Schritte ausgeführt werden:

1. Melden Sie sich bei Outlook Web App, und navigieren Sie zu **Optionen > Telefon > Voicemail**.
  2. Klicken Sie auf der Seite **Voicemail** unter **Benachrichtigungen** auf **Benachrichtigungen einrichten**.
  3. Klicken Sie auf der Seite **Text messaging** auf die Schaltfläche **Benachrichtigungen aktivieren**.
- Caution**
- Klicken Sie nicht auf **Voicemailbenachrichtigungen**. Andernfalls wird die Seite **Voicemail** wieder aufgerufen.
4. Wählen Sie auf der Seite **Text Messaging** mit der Dropdownliste unter **Gebietsschema** das Gebietsschema oder den Standort des Mobilfunknetzbetreibers für das Text Messaging aus.
  5. Wählen Sie auf der Seite **Text Messaging** unter **Mobilfunknetzbetreiber** mit der Dropdownliste den Mobilfunknetzbetreiber für das Text Messaging aus, und klicken Sie dann auf **Weiter**.
  6. Geben Sie auf der Seite **Text Messaging** im Feld **Geben Sie Ihre Telefonnummer ein, und klicken Sie auf "Weiter"** die für Textnachrichtbenachrichtigungen verwendete Mobiltelefonnummer ein, und klicken Sie auf **Weiter**. Eine sechsstellige Kennung wird an das Mobiltelefon gesendet. Haben Sie keine Kennung erhalten, klicken Sie auf **Keine Kennung empfangen, muss erneut gesendet werden**.
  7. Geben Sie die Kennung in das Feld **Kennung** ein, und klicken Sie auf **Fertig stellen**.
  8. Nach der Aktivierung der Textnachrichtbenachrichtigungen durch den Benutzer kann dieser auf der Seite **Text Messaging** auf **Voicemailbenachrichtigungen einrichten** klicken. Die Voicemailseite wird wieder

aufgerufen. Hier können sie nach unten zum Bereich **Benachrichtigungen** blättern und Optionen für Textnachrichtenbenachrichtigungen für entgangene Anrufe und Sprachnachrichten einrichten.

# Ermöglicht es Message Waiting Indicator Prozeduren

18.12.2018 • 2 minutes to read

[MWI \(Message Waiting Indicator\) für ein UM-IP-Gateway unterstützen](#)

[Verhindern von MWI an einem UM-IP-Gateway](#)

[Aktivieren der MWI-Funktion \(Message Waiting Indicator\) für Benutzer](#)

[Deaktivieren der Nachricht wartet Indicator \(MWI\) für Benutzer](#)

[Aktivieren von Benachrichtigungen über verpasste Anrufe für einen Benutzer](#)

[Deaktivieren von Benachrichtigungen über verpasste Anrufe für einen Benutzer](#)

# MWI (Message Waiting Indicator) für ein UM-IP-Gateway unterstützen

18.12.2018 • 3 minutes to read

Sie können Voicemailbenachrichtigungen an Benutzer für Anrufe zulassen oder verhindern, die von einem UM-IP-Gateway (Unified Messaging) empfangen werden. Wenn Sie diese Einstellung aktivieren, kann das UM-IP-Gateway SIP-NOTIFY-Nachrichten für Benutzer empfangen und senden. Der MWI (Message Waiting Indicator) ist standardmäßig aktiviert und ermöglicht es, dass Benachrichtigungen über wartende Nachrichten an Benutzer gesendet werden. Diese Einstellung kann jedoch gemäß Ihren Anforderungen deaktiviert werden.

Ein MWI (Message Waiting Indicator) benachrichtigt Benutzer über eine neue oder nicht abgehörte Sprachnachricht. Sie wird im Posteingang von Clients wie z. B. Outlook und Outlook Web App angezeigt. Es kann sich dabei auch um Folgendes handeln: Eine SMS, die an ein registriertes Mobiltelefon gesendet wird, ein ausgehender Anruf von einem Exchange-Server an eine Nummer, die für die Wiedergabe neuer Nachrichten konfiguriert ist, oder ein leuchtendes Lämpchen am Telefon auf dem Schreibtisch des Benutzers.

## TIP

MWI-Benachrichtigungen können auch für eine UM-Postfachrichtlinie für eine Gruppe von Benutzern aktiviert oder deaktiviert werden.

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Zulassen des Message Waiting Indicator (MWI) mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-IP-Gateways**, wählen Sie den UM-IP-Gateway Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
2. Aktivieren Sie auf der Seite **UM-IP-Gateway** das Kontrollkästchen neben **WMI (Waiting Message Indicator) zulassen**.
3. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell, Message Waiting Indicator zulassen

In diesem Beispiel wird die Anzeige für wartende Nachrichten für Benutzer angezeigt werden, die mit dem UM-IP-Gateway mit dem Namen verknüpft sind ermöglicht **MyUMIPGateway** mit der IP-Adresse 10.10.10.1.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address 10.10.10.1 -MessageWaitingIndicatorAllowed $true
```

# Verhindern von MWI an einem UM-IP-Gateway

18.12.2018 • 3 minutes to read

Sie können Voicemailbenachrichtigungen an Benutzer für Anrufe verhindern, die von einem UM-IP-Gateway (Unified Messaging) empfangen werden. Wenn Sie diese Einstellung aktivieren, kann das UM-IP-Gateway SIP-NOTIFY-Nachrichten für Benutzer empfangen und senden. Der MWI (Message Waiting Indicator) ist standardmäßig aktiviert und ermöglicht es, dass Benachrichtigungen über wartende Nachrichten an Benutzer gesendet werden. Diese Einstellung kann jedoch gemäß Ihren Anforderungen deaktiviert werden.

Ein MWI (Message Waiting Indicator) benachrichtigt Benutzer über eine neue oder nicht abgehörte Sprachnachricht. Sie wird im Posteingang von Clients wie z. B. Outlook und Outlook Web App angezeigt. Es kann sich dabei auch um Folgendes handeln: Eine SMS, die an ein registriertes Mobiltelefon gesendet wird, ein ausgehender Anruf von einem Exchange-Server an eine Nummer, die für die Wiedergabe neuer Nachrichten konfiguriert ist, oder ein leuchtendes Lämpchen am Telefon auf dem Schreibtisch des Benutzers.

## TIP

MWI-Benachrichtigungen können auch für eine UM-Postfachrichtlinie für eine Gruppe von Benutzern aktiviert oder deaktiviert werden.

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verhindern des MWI (Message Waiting Indicator) mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-IP-Gateways**, wählen Sie den UM-IP-Gateway Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

2. Deaktivieren Sie auf der Seite **UM-IP-Gateway** das Kontrollkästchen für **MWI (Message Waiting Indicator)** zulassen.

3. Klicken Sie auf **Speichern**.

Verwenden Sie Exchange Online PowerShell, um Message Waiting Indicator zu verhindern.

In diesem Beispiel wird verhindert die Anzeige für wartende Nachrichten für Benutzer, die mit dem UM-IP-Gateway mit dem Namen verknüpft sind **MyUMIPGateway** mit der IP-Adresse 10.10.10.1.

```
Set-UMIPGateway -Identity MyUMIPGateway -Address 10.10.10.1 -MessageWaitingIndicatorAllowed $false
```

# Aktivieren der MWI-Funktion (Message Waiting Indicator) für Benutzer

18.12.2018 • 3 minutes to read

Der Message Waiting Indicator (MWI) kann für Benutzer, die einer Unified Messaging-Postfachrichtlinie (UM) zugeordnet sind, aktiviert oder deaktiviert werden. Die meisten Legacy-Voicemailsysteme enthalten eine MWI-Funktion. In der Regel wird dabei durch eine LED am Telefon des Voicemail-Teilnehmers signalisiert, dass eine neue Voicemailnachricht vorliegt. Der MWI kann auch eine Textnachricht an das Mobiltelefon des UM-aktivierten Benutzers senden. Die Standardeinstellung lautet "Aktiviert".

Falls der MWI am UM-IP-Gateway deaktiviert wird, ist das Feature für UM-aktivierte Benutzer, die der UM-Postfachrichtlinie zugeordnet sind, nicht verfügbar.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

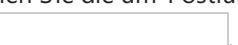
## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren des MWI mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** 
2. Klicken Sie unter **UM-Postfachrichtlinien** wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten** 
3. Aktivieren Sie auf der Seite **UM-Postfachrichtlinie** das Kontrollkästchen neben **WMI (Waiting Message Indicator) zulassen**.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell, Message Waiting Indicator aktivieren

Dieses Beispiel aktiviert die Message Waiting Indicator für Benutzer mit dem Namen der UM-Postfachrichtlinie zugeordnet `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowMessageWaitingIndicator $true
```

# Deaktivieren der Nachricht wartet Indicator (MWI) für Benutzer

18.12.2018 • 3 minutes to read

Der Message Waiting Indicator (MWI) kann für Benutzer, die einer UM-Postfachrichtlinie (Unified Messaging) zugeordnet sind, aktiviert oder deaktiviert werden. Die meisten Legacy-Voicemailsysteme umfassen eine MWI-Funktion (Message Waiting Indicator). In der Regel wird dabei durch eine LED am Telefon des Voicemail-Teilnehmers signalisiert, dass eine neue Voicemailnachricht vorliegt. Der MWI kann auch eine SMS an das Mobiltelefon eines UM-aktivierten Benutzers senden. Die Standardeinstellung ist "Aktiviert".

Falls der MWI am UM-IP-Gateway deaktiviert wird, ist das Feature für UM-aktivierte Benutzer, die der UM-Postfachrichtlinie zugeordnet sind, nicht verfügbar.

Informationen zu weiteren Verwaltungsaufgaben im Zusammenhang mit UM-Postfachrichtlinien finden Sie unter [UM-Postfachrichtlinien - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Deaktivieren von Message Waiting Indicator mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** 
2. Klicken Sie unter **UM-Postfachrichtlinien** wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten** 
3. Deaktivieren Sie auf der Seite **UM-Postfachrichtlinie** das Kontrollkästchen für **MWI (Message Waiting Indicator) zulassen**.

4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell Message Waiting Indicator deaktivieren

Dieses Beispiel deaktiviert die Message Waiting Indicator für Benutzer mit dem Namen der UM-Postfachrichtlinie zugeordnet `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowMessageWaitingIndicator $false
```

# Aktivieren von Benachrichtigungen über verpasste Anrufe für einen Benutzer

18.12.2018 • 4 minutes to read

Sie können aktivieren oder Deaktivieren von Benachrichtigungen über verpasste Anrufe für einen Unified Messaging (UM)-Postfachrichtlinie mithilfe der Exchange Online PowerShell oder der Exchange-Verwaltungskonsole. Benachrichtigung über eine verpasste Anrufe wird eine e-Mail-Nachricht, die an einen Benutzer gesendet wird, wenn der Benutzer einen eingehenden Anruf nicht beantworten und der Anrufer keine Voicemailnachricht lassen. Dies ist eine andere e-Mail-Nachricht als die Nachricht, die VoIP-Nachricht enthält, die für einen Benutzer bleibt.

Wenn Sie Benachrichtigungen über verpasste Anrufe für eine UM-Postfachrichtlinie deaktivieren, erhalten sämtliche der einer UM-Postfachrichtlinie zugeordneten Benutzer keine E-Mail-Nachricht, wenn Sie einen eingehenden Anruf nicht beantworten und der Anrufer keine Sprachnachricht hinterlässt. Standardmäßig sind Benachrichtigungen über verpasste Anrufe für alle UM-Postfachrichtlinien aktiviert, die erstellt werden. Wenn Sie einen UM-Wählplan erstellen, wird zudem standardmäßig eine UM-Postfachrichtlinie erstellt.

## NOTE

Wenn Sie Unified Messaging und Microsoft Lync Server integrieren, stehen Benachrichtigungen über verpasste Anrufe Benutzern nicht zur Verfügung, die über ein Postfach auf einem Exchange 2007- oder Exchange 2010-Postfachserver verfügen, wenn ein Benutzer sich abmeldet, bevor der Anruf an einen Postfachserver gesendet wurde, auf dem der Microsoft Exchange Unified Messaging-Dienst ausgeführt wird.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [Verwalten einer UM-Postfachrichtlinie](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren von Benachrichtigungen über verpasste Anrufe für eine UM-Telefonrichtlinie mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  
[ ]
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten** [ ].
3. Aktivieren Sie auf der Seite **UM-Postfachrichtlinie > Allgemein** das Kontrollkästchen neben **Benachrichtigungen über verpasste Anrufe zulassen**.
4. Klicken Sie auf **Speichern**.

Verwenden Sie Exchange Online PowerShell, um Benachrichtigungen über verpasste Anrufe für einen UM-Postfachrichtlinie zu aktivieren.

Dieses Beispiel aktiviert die Benachrichtigungen über verpasste Anrufe für einen UM-Postfachrichtlinie mit der Bezeichnung **MyUMMailboxPolicy**.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowMissedCallNotifications $true
```

# Deaktivieren von Benachrichtigungen über verpasste Anrufe für einen Benutzer

18.12.2018 • 4 minutes to read

Sie können aktivieren oder Deaktivieren von Benachrichtigungen über verpasste Anrufe für einen Unified Messaging (UM)-Postfachrichtlinie mithilfe der Exchange Online PowerShell oder der Exchange-Verwaltungskonsole. Benachrichtigung über eine verpasste Anrufe wird eine e-Mail-Nachricht, die an einen Benutzer gesendet wird, wenn der Benutzer einen eingehenden Anruf nicht beantworten und der Anrufer keine Sprachnachricht hinterlassen. Dies ist eine andere e-Mail-Nachricht als diejenige, die die Sprachnachricht enthält, die für einen Benutzer bleibt.

Wenn Sie Benachrichtigungen über verpasste Anrufe für eine UM-Postfachrichtlinie deaktivieren, erhalten sämtliche der einer UM-Postfachrichtlinie zugeordneten Benutzer keine E-Mail-Nachricht, wenn Sie einen eingehenden Anruf nicht beantworten und der Anrufer keine Sprachnachricht hinterlässt. Standardmäßig sind Benachrichtigungen über verpasste Anrufe für alle UM-Postfachrichtlinien aktiviert, die erstellt werden. Wenn Sie einen UM-Wählplan erstellen, wird zudem standardmäßig eine UM-Postfachrichtlinie erstellt.

## NOTE

Wenn Sie Unified Messaging und Microsoft Lync Server integrieren, stehen Benachrichtigungen über verpasste Anrufe Benutzern nicht zur Verfügung, die über ein Postfach auf einem Exchange 2007- oder Exchange 2010-Postfachserver verfügen, wenn ein Benutzer sich abmeldet, bevor der Anruf an einen Postfachserver gesendet wurde, auf dem der Microsoft Exchange Unified Messaging-Dienst ausgeführt wird.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf UM-Postfachrichtlinien finden Sie unter [Verwalten einer UM-Postfachrichtlinie](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Deaktivieren von Benachrichtigungen über verpasste Anrufe für eine UM-Telefonrichtlinie mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  
[ ]
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten** [ ].
3. Deaktivieren Sie auf der Seite **UM-Postfachrichtlinie > Allgemein** das Kontrollkästchen neben **Benachrichtigungen über verpasste Anrufe zulassen**.
4. Klicken Sie auf **Speichern**.

Verwenden Sie Exchange Online PowerShell, um Benachrichtigungen über verpasste Anrufe für einen UM-Postfachrichtlinie zu deaktivieren

Dieses Beispiel deaktiviert die Benachrichtigungen über verpasste Anrufe für einen UM-Postfachrichtlinie mit der Bezeichnung **MyUMMailboxPolicy**.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowMissedCallNotifications $false
```

# Autorisieren von Benutzern für Anrufe

18.12.2018 • 23 minutes to read

Outdialing wird der Vorgang genannt, bei dem sich Benutzer über eine Outlook Voice Access-Nummer in einen UM-Wählplan einwählen und einen Anruf einer internen oder externen Telefonnummer einleiten oder diesen weiterleiten. Unified Messaging verwendet viele Outdialingeinstellungen, um Anrufe für Benutzer zu tätigen. Zum Konfigurieren des Outdialings müssen Sie Wählregeln, Wählregelgruppen und Wählautorisierungen für Unified Messaging-Wählpläne (UM) konfigurieren und anschließend das Outdialing für UM-Wählpläne, UM-Postfachrichtlinien und automatische Telefonzentralen autorisieren. Darüber hinaus können Sie UM-Wählpläne so konfigurieren, dass sie über Kurzwahlnummern oder Zugriffscodes, ein nationales Rufnummernpräfix und ein nationales/regionales bzw. internationales Nummernformat verfügen, mit deren Hilfe Sie das Outdialing in Ihrer Organisation steuern können. In diesem Thema werden Wählregeln, Wählregelgruppen und Wählautorisierungen sowie deren Verwendung zur Autorisierung und Steuerung des Outdialings in Ihrer Organisation behandelt.

## Übersicht

Outdialing passiert, wenn:

- Ein Anruf einer externen Telefonnummer eingeleitet wird.
- Ein Anruf an eine automatische Telefonzentrale weitergeleitet wird.
- Ein Anruf an einen Benutzer in Ihrer Organisation weitergeleitet wird.
- Ein UM-aktivierter Benutzer die Funktion "Wiedergabe über Telefon" verwendet.

Damit das Outdialing ordnungsgemäß funktioniert, müssen folgende Einstellungen richtig konfiguriert sein:

- **Wählregeln:** Wählregeln definieren Sie die Nummer, die von dem UM-aktivierten Benutzer gewählt wird und die Nummer, die wird gewählt werden durch den Private Branch eXchange, (Nebenstellenanlage PBX) oder die IP-Nebenstellenanlage.
- **Wählregelgruppen:** Wählvorgang Regel Gruppen bestimmt die Arten von Anrufen, die Benutzern innerhalb einer Gruppe Wählvorgang vornehmen können.
- **Autorisierung einwählen:** Wählvorgang zu erteilenden bestimmen die Einschränkungen, die angewendet werden, um Benutzer verhindern können, dass Gebühren für unnötige Telefon anfallen oder Ferngespräche einwählen.

Zum Aktivieren des Outdialings für Benutzer, die sich in einen Wählplan oder eine automatische Telefonzentrale einwählen, führen Sie die folgenden Schritte aus.

- Vergewissern Sie sich, dass die VoIP-Gateways von einem UM-IP-Gateway abgebildet werden, das mit einem Wählplan verknüpft ist, der ausgehende Anrufe zulässt.
- Erstellen Sie Wählregelgruppen, indem Sie Wählregeln für den UM-Wählplan definieren.
- Fügen Sie Wählautorisierungen für nationale/regionale und internationale Wählregelgruppen für den UM-Wählplan, die UM-Postfachrichtlinie oder automatische Telefonzentrale hinzu, der/die demselben Wählplan wie das UM-IP-Gateway zugeordnet ist.

## Benutzertypen

Zwei Typen von Benutzern können die Outdialingfunktion in Unified Messaging verwenden: authentifizierte Benutzer und nicht authentifizierte Benutzer. Alle Benutzer, die bei einer automatischen UM-Telefonzentrale anrufen, sind nicht authentifiziert. Wenn Benutzer eine Outlook Voice Access-Nummer anrufen, gelten sie als nicht authentifiziert, weil sie nicht ihre Durchwahlnummer und PIN angegeben und sich nicht bei ihrem Postfach angemeldet haben. Benutzer sind authentifiziert, nachdem sie ihre Durchwahlnummer und PIN angegeben und sich erfolgreich bei ihrem Postfach angemeldet haben.

Wenn Benutzer eine Outlook Voice Access-Nummer anrufen, die in einem UM-Wählplan konfiguriert ist, und versuchen, einen Anruf einzuleiten oder weiterzuleiten, ohne sich bei ihrem Postfach anzumelden, werden nur die Outdialingeinstellungen des UM-Wählplans auf den Anruf angewendet. Wenn ein anonymer oder nicht authentifizierter Benutzer eine automatische UM-Telefonzentrale anruft, werden sowohl die für die automatische Telefonzentrale als auch die im der automatischen Telefonzentrale zugeordneten Wählplan konfigurierten Outdialingeinstellungen auf den Anruf angewendet.

Wenn Benutzer eine Outlook Voice Access-Nummer anrufen, die in einem Wählplan konfiguriert ist, und sich erfolgreich bei ihrem Postfach anmelden, gelten sie als authentifiziert. Nach ihrer Authentifizierung werden in den Anrufeinstellungen für das Outdialing die Wählregel- und Wählautorisierungseinstellungen in der UM-Postfachrichtlinie verwendet, die mit diesen Benutzern verknüpft ist.

## Outdialingeinstellungen

Sie müssen mehrere Einstellungen konfigurieren, um Outdialingregeln für Ihre Organisation zu aktivieren. Zusätzlich zur Konfiguration der UM-Wählpläne, automatischen UM-Telefonzentralen und UM-Postfachrichtlinien, die Sie mit den ordnungsgemäßen Wählregeln und -autorisierungen erstellt haben, müssen Sie Kurzwahlnummern, Nummernpräfixe und -formate in den UM-Wählplänen konfigurieren. Folgende Outdialingeinstellungen werden für Wählpläne, automatische Telefonzentralen und UM-Postfachrichtlinien konfiguriert:

- Amtskennziffer, nationale/regionale und internationale Zugriffscodes
- Nationales Rufnummernpräfix
- Nationale/regionale und internationale Nummernformate
- Konfigurierte nationale/regionale und internationale Wählregelgruppen
- Zulässige nationale/regionale und internationale Wählregelgruppen
- Wählregeleinträge
- Wählautorisierungen

Damit Sie das Outdialing erfolgreich für Ihre Organisation konfigurieren können, müssen Sie zunächst die Einsatzmöglichkeiten jeder Komponente beim Outdialing kennen und wissen, wie diese zu konfigurieren sind. In der folgenden Tabelle werden alle Komponenten vorgestellt, die für UM-Wählpläne, automatische UM-Telefonzentralen und UM-Postfachrichtlinien konfiguriert sein müssen, damit das Outdialing ordnungsgemäß funktioniert.

## Outdialingkomponenten

KOMPONENTE	BESCHREIBUNG
------------	--------------

KOMPONENTE	BESCHREIBUNG
Kurzwahlnummern, Rufnummernpräfixe und Nummernformate	UM verwendet beim Einleiten eines ausgehenden Anrufs Kurzwahlnummern, Rufnummernpräfixe und Nummernformate zum Bestimmen der zu wählenden Nummer. Sie können Kurzwahlnummern, Rufnummernpräfixe und Nummernformate so konfigurieren, dass ausgehende Anrufe von Benutzern, die bei einer automatischen UM-Telefonzentrale anrufen, die einem UM-Wählplan zugeordnet ist, oder von Benutzern, die die im Wählplan konfigurierte Outlook Voice Access-Nummer anrufen, eingeschränkt werden.
Wählregelgruppen	Wählregelgruppen werden erstellt, um Rufnummern ändern zu können, bevor sie bei ausgehenden Anrufen an die Nebenstellenanlage gesendet werden. Wählregelgruppen entfernen Nummern aus Rufnummern, die von UM angerufen werden, oder fügen diesen Nummern hinzu. So können Sie beispielsweise eine Wählregelgruppe erstellen, die einer 7-stelligen Rufnummer automatisch eine 0 als Präfix hinzufügt, um den Zugriff auf eine Amtsleitung zu gewähren. In diesem Beispiel müssen Benutzer, die ausgehende Anrufe tätigen, keine 0 vorwählen, um die externe Rufnummer einer Person außerhalb der Organisation zu erreichen. Jede Wählregelgruppe enthält Wählregeln, die die Arten von Inlands-, Fern- und Auslandsgesprächen bestimmen, die Benutzer innerhalb einer Wählregelgruppe tätigen können. Wählregelgruppen gelten für die Benutzer, die einem UM-Wählplan zugeordnet sind, oder für automatische UM-Telefonzentralen und UM-Postfachrichtlinien, die dem UM-Wählplan zugeordnet sind. Jede Wählregelgruppe muss mindestens eine Wählregel enthalten.
Wählregeleinträge	Mithilfe einer Wählregel wird die Art der Anrufe bestimmt, die Benutzer innerhalb einer Wählregelgruppe tätigen können. Beim Erstellen einer Wählregelgruppe konfigurieren Sie mindestens eine Wählregel. Beim Konfigurieren einer Wählregel müssen Sie deren Namen, ein umzuwendendes Nummernmuster (die Nummernmaske) und die gewählte Nummer eingeben. Zusätzlich können Sie auch einen Kommentar eingeben. Mithilfe von Kommentaren können Sie beschreiben, wie die Wählregel verwendet wird, oder eine Gruppe von Benutzern benennen, für die die Wählregel gilt. Wenn Sie einer Wählregel eine Nummernmaske und die gewählte Nummer hinzufügen, können Sie den Buchstaben "x" durch eine Ziffer einer Rufnummer ersetzen, beispielsweise 01425xxxxxx. Sie können auch ein Sternchen (*) als Platzhalterzeichen verwenden, z. B. 01425*.

KOMPONENTE	BESCHREIBUNG
Wählautorisierungen	<p>Eine Wählautorisierung verwendet Wählregelgruppen, um Wähleinschränkungen für Benutzer anzuwenden, die einer bestimmten UM-Postfachrichtlinie, einem UM-Wählplan oder einer automatischen Telefonzentrale zugeordnet sind. Wähleinschränkungen können ebenfalls verwendet werden, um Benutzern Anrufe an nationale/regionale bzw. internationale Rufnummern zu gestatten.</p> <p>Nachdem Sie die Wählregeln für einen UM-Wählplan erstellt haben, fügen Sie die Wählregelgruppe einer UM-Postfachrichtlinie, einem Wählplan oder einer automatischen Telefonzentrale hinzu. Im Anschluss an das Hinzufügen der Wählregelgruppe zu einer UM-Postfachrichtlinie gelten alle definierten Einstellungen bzw. Regeln für UM-aktivierten Benutzer, die der UM-Postfachrichtlinie zugeordnet sind.</p>

## Konfigurieren des Outdialings

Eine Wählregelgruppe ist eine Sammlung mit mindestens einer Wählregel, die für einen UM-Wählplan konfiguriert ist. Zwei Arten von Wählregelgruppen können für UM-Wählpläne konfiguriert werden: national/Regional und international. Nationale/regionale Wählregelgruppen gelten für Rufnummern, die innerhalb desselben Landes bzw. derselben Region gewählt werden. Internationale Wählregelgruppen gelten für internationale Rufnummern, die aus einem Land bzw. einer Region in einem anderen Land bzw. einer anderen Region gewählt werden.

Jeder Wählplan kann mindestens eine Wählregelgruppe enthalten. Um eine Wählregelgruppe auf eine Gruppe von Benutzern anzuwenden, müssen Sie nach dem Erstellen der Wählregelgruppe diese der Liste der zulässigen Wählregelgruppen für den UM-Wählplan und für die automatischen UM-Telefonzentralen und UM-Postfachrichtlinien hinzufügen, die dem UM-Wählplan zugeordnet sind.

Wählregelgruppen können Sie Wählregeln wird angegeben, die an eine Gruppe von UM-aktivierte Benutzer gelten, die in einer bestimmten Kategorie gehören sollen. Beispielsweise können Sie Wählregelgruppen verwenden, um anzugeben, welcher Gruppe der Benutzer Ausland telefonieren kann und welcher Gruppe nur in Bundesland oder lokalen Anrufe tätigen kann. Sie können eine Wählvorgang Regelgruppe mithilfe der Exchange-Verwaltungskonsole (EAC) oder das Cmdlet **Set-UMDialPlan** in Exchange Online PowerShell erstellen. Wenn Sie eine Nummer Regelgruppe erstellen, müssen Sie mindestens eine Wählvorgang Regel für die Gruppe definieren.

Wenn ein Benutzer eine Rufnummer wählt, gleicht UM diese Nummer mit den Wählregeln ab. Wenn eine Übereinstimmung gefunden wird, verwendet UM die Wählregel, um die zu währende Nummer zu bestimmen, indem die Telefonnummer oder Ziffern im Abschnitt **Gewählte Nummer** der Wählregel untersucht werden. Die Nummer im Feld **Gewählte Nummer** der Wählregel wird gewählt.

Die folgende Tabelle zeigt ein Beispiel der Wählregelgruppen und Wählregeln. In diesem Beispiel werden nur für die lokale Anrufe und kostengünstige Wählregelgruppen an, die erstellt wurden. Die Gruppe Wählvorgang Regel nur für die lokale Anrufe, verfügt über zwei Wählregeln: 91425\* und 91206\*, die Wählvorgang Regelgruppe kostengünstige auch hat zwei Wählregeln: 91509\* und 91360\*.

### Wählregelgruppen und Wählregeln

NAME	NUMBERMASK	DIALEDNUMBER	COMMENT
Nur Ortsgespräche	91425*	91*	Ortsgespräche
Nur Ortsgespräche	91206*	91*	Ortsgespräche

NAME	NUMBERMASK	DIALEDNUMBER	COMMENT
Billigtarif	91509*	9*	Nationale Anrufe
Billigtarif	91360*	9*	Nationale Anrufe

Wählt ein Benutzer beispielsweise die Nummer 0-1-425-555-1234, wählt UM 4255551234. UM entfernt alle nicht numerischen Zeichen (in diesem Beispiel die Bindestriche) und wendet die Nummernmaske aus dem Wählregeln an. In diesem Beispiel wendet UM die Nummernmaske 01\* an. Diese weist UM an, weder die 0 noch die 1 zu wählen, sondern alle anderen in der Rufnummer enthaltenen Ziffern, die der 1 nachgestellt sind. Hierzu gehören alle Ziffern, die durch das Sternchen (\*) dargestellt werden.

Sie können die Exchange-Verwaltungskonsole oder die Exchange Online PowerShell zum Erstellen und konfigurieren einzelne oder mehrere in nationale/regionale und internationale Wählregelgruppen und Wählregeln verwenden. Wenn Sie viele oder zu komplex Wählregelgruppen und Wählregeln erstellen, können Sie eine Datei durch Trennzeichen getrennten Werten (CSV) in Exchange Online PowerShell verwenden. Sie können importieren oder Exportieren eine Liste der Wählregelgruppen und Wählregeln.

Zum Importieren einer Liste mit Wählregelgruppen und Wählregeln, die in einer CSV-Datei definiert wurden, führen Sie das Cmdlet **Set-UMDialPlan** wie folgt aus:

```
Set-UMDialPlan "MyUMDialPlan" -ConfiguredInCountryOrRegionGroups $(IMPORT-CSV  
c:\dialrules\InCountryRegion.csv)
```

Zum Abrufen einer Liste der für einen Wählplan konfigurierten Wählregelgruppen führen Sie das Cmdlet **Get-UMDialPlan** wie folgt aus:

```
(Get-UMDialPlan -Identity "MyUMDialPlan").ConfiguredInCountryOrRegionGroups | EXPORT-CSV  
C:\incountryorregion.csv
```

Die CSV-Datei muss im richtigen Format erstellt und gespeichert werden. Jede Zeile in der CSV-Datei stellt eine Wählregel dar. Jede Wählregel wird jedoch in derselben Wählregelgruppe konfiguriert. Jede Regel in der Datei besteht aus vier Abschnitten, die durch Kommas voneinander getrennt sind. Bei diesen Abschnitten handelt es sich um den Namen, die Nummernmaske, die gewählte Nummer und einen Kommentar. Mit Ausnahme des Kommentars ist jeder Abschnitt erforderlich und muss mit richtigen Informationen ausgefüllt werden. Zwischen dem jeweiligen Texteintrag und dem Komma des nächsten Abschnitts darf kein Leerzeichen stehen. Es dürfen auch keine Leerzeilen zwischen den Regeln oder am Ende der Datei vorhanden sein. Im Folgenden sehen Sie ein Beispiel für eine CSV-Datei, die zum Erstellen von nationalen/regionalen Wählregelgruppen und Wählregeln verwendet werden kann.

#### **Name, NumberMask, DialedNumber, Kommentar**

**Low-rate,91425xxxxxxxx,9xxxxxxxx,Local call**

**Low-rate,9425xxxxxxxx,9xxxxxxxx,Local call**

**Low-rate,9xxxxxxxx,9xxxxxxxx,Local call**

**Any,91\*,91\*,Open access to in-country/region numbers**

**Long-distance,91408\*,91408\*,long distance**

Im Folgenden sehen Sie ein Beispiel für eine CSV-Datei, die zum Erstellen von internationalen Wählregelgruppen und Wählregeleinträgen verwendet werden kann.

#### **Name, NumberMask, DialedNumber, Kommentar**

**International, 901144\*, 901144\*, international call**

**International, 901133\*, 901133\*, international call**

## Anwenden konfigurierter Wählregelgruppen

Wählregelgruppen werden auf einem um-Wählplan erstellt. Sie können nationale/regionale und internationale Wählregelgruppen, die mit der Exchange-Verwaltungskonsole oder über das Cmdlet **Set-UMDialPlan** im Exchange Online PowerShell erstellen. Nachdem Sie die entsprechenden Wählregelgruppen auf einem um-Wählplan erstellen und die Wählregeln definieren, können Sie anwenden Wählregelgruppen an, denen Sie erstellt haben, einem um-Wählplan ein UM-Telefonzentrale oder für Benutzer, die eine um-Postfachrichtlinie zugeordnet sind, und autorisieren Amtswahl für, je nachdem, wie der Benutzer das Voicemailsystem zugreift.

Die für einen Wählplan erstellten Wählregelgruppen können auf Folgendes angewendet werden:

- **Dasselben Wählplans:** die Einstellungen für alle Benutzer, die in eine Outlook Voice Access-Nummer anrufen, aber nicht melden Sie sich mit ihrem Postfach angewendet werden. Anwenden eine nationale/regionale Wählvorgang Regelgruppe mit dem Namen `MyAllowedDialRuleGroup` mit dem gleichen Wählplan Exchange Online PowerShell **Set-UMDialPlan** -Cmdlet verwenden, wie folgt.

```
Set-UMDialPlan -Identity MyUMDialPlan -AllowedInCountryOrRegionGroups MyAllowedDialRuleGroup
```

- **Einzelne oder mehrere UM-Postfachrichtlinien:** die Einstellungen, die auf einer um-Postfachrichtlinie konfiguriert sind gilt für alle Benutzer, die mit dieser UM-Postfachrichtlinie verknüpft sind. Benutzer, die in eine Outlook Voice Access-Nummer anrufen, und melden Sie sich mit ihrem Postfach gelten die Einstellungen auf einem UM-Postfachrichtlinie konfiguriert ist. Anwenden eine nationale/regionale Wählvorgang Regelgruppe mit dem Namen `MyAllowedDialRuleGroup` zu einer einzelnen um-Postfachrichtlinie, verwenden Sie die Seite **Einwählen Autorisierung** auf die um-Postfachrichtlinie in der Exchange-Verwaltungskonsole oder verwenden Sie das Cmdlet **Set-UMMailboxPolicy** in Exchange Online PowerShell als folgt.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowedInCountryOrRegionGroups MyAllowedDialRuleGroup
```

- **Einzelne oder mehrere Telefonzentralen zugeordnet des UM-Wählplan:** Dies gilt für alle Benutzer, die eine automatische um-Telefonzentrale anrufen. Anwenden die nationale/regionale Wählvorgang Regelgruppe mit dem Namen `MyAllowedDialRuleGroup` zu einer einzelnen automatischen um-Telefonzentrale, verwenden Sie die Seite **Einwählen Autorisierung** auf die automatische Telefonzentrale in der Exchange-Verwaltungskonsole oder das Cmdlet **Set-UMAutoAttendant** in Exchange Online PowerShell, wie folgt.

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AllowedInCountryOrRegionGroups MyAllowedDialRuleGroup
```

Die folgende Tabelle fasst die Anwendungsmöglichkeiten von Wählregelgruppen in Unified Messaging zusammen.

### Anwendung von Outdialingregeln

ANRUFERTYP	GELTUNGSBEREICH	ANGEWENDETE OUTDIALINGEINSTELLUNGEN
Outlook Voice Access-Nummer	Der Benutzer wählt eine Outlook Voice Access-Nummer im Wählplan und meldet sich bei seinem Postfach an	UM-Postfachrichtlinie

ANRUFERTYP	GELTUNGSBEREICH	ANGEWENDETE OUTDIALINGEINSTELLUNGEN
Anonymer Anrufer	Der Benutzer wählt eine Outlook Voice Access-Nummer im Wählplan	UM-Wählplan
Anonymer Anrufer	Der Benutzer wählt sich über die Pilot- oder Durchwahlnummer einer automatischen Telefonzentrale ein	Automatische UM-Telefonzentrale
Anrufer von innerhalb der Organisation	Der Benutzer wählt sich über die Nummer für die Wiedergabe über Telefon ein	UM-Postfachrichtlinie

## Anwenden von Wählregeln

Der Outdialingprozess wird in den folgenden Fällen ausgeführt:

- Unified Messaging leitet einen Anruf einer externen Telefonnummer für einen Anrufer ein.
- Unified Messaging vermittelt einen Anruf an eine automatische Telefonzentrale.
- Unified Messaging vermittelt einen Anruf an einen Benutzer in Ihrer Organisation.
- Ein UM-aktivierter Benutzer verwendet die Funktion "Wiedergabe über Telefon".

In jedem Outdialingszenario wendet UM die konfigurierten Wählregeln an und leitet dann den Anruf für den Benutzer ein. Je nach Szenario sowie der Art der Anrufeinleitung durch den Benutzer wendet UM jedoch möglicherweise nur einige der Wählregeln auf die gewählte Rufnummer an. In anderen Outdialingszenarien wendet UM möglicherweise alle konfigurierten Outdialingregeln auf die gewählte Rufnummer an.

# Kurzwahlnummern, Rufnummernpräfixe und Nummernformate

18.12.2018 • 13 minutes to read

Sie können mehrere Kurzwahlnummern konfigurieren, die dann von einem Unified Messaging-Server (UM) zur Anwahl interner und externer Rufnummern für UM-aktivierte Benutzer verwendet werden. In vielen Fällen möchten Sie Wähleinstellungen in Verbindung mit den Kurzwahl- oder Zugriffscodes, einem nationalen Nummernprefix oder den nationalen/regionalen oder internationalen Nummernformaten konfigurieren, damit Sie das Outdialing für Benutzer in Ihrer Organisation steuern können. Dieses Thema befasst sich mit Kurzwahlnummern, Nummernpräfixen und Nummernformaten und erläutert, wie diese zum Steuern des Outdialings in Ihrer Organisation verwendet werden können.

## Übersicht

Das Outdialing ist der Prozess, mit dem sich Benutzer über einen UM-Wählplan oder bei einer automatischen UM-Telefonzentrale einwählen und dann einen Anruf bei einer internen oder externen Rufnummer tätigen. Wenn sich ein Benutzer über einen UM-Wählplan oder bei einer automatischen UM-Telefonzentrale einwählt und einen Anruf tätigt, verwendet Unified Messaging die für die Wähleinstellungen, die automatische Telefonzentrale und die UM-Postfachregel konfigurierten Einstellungen, um den Anruf durchzuführen. UM tätigt in den folgenden Situationen einen ausgehenden Anruf:

- Wenn für einen Anrufer eine externe Telefonnummer gewählt wird
- Wenn einen Anruf an eine automatische Telefonzentrale übergeben wird
- Wenn ein Anruf an einen (UM-aktivierten oder nicht UM-aktivierten) Benutzer in Ihrer Organisation übergeben wird
- Wenn ein UM-aktivierter Benutzer die Funktion "Wiedergabe über Telefon" verwendet

Zwei Typen von Benutzern verwenden Outdialing: authentifizierte Benutzer und nicht authentifizierte Benutzer. Nicht authentifizierte Benutzer rufen eine Outlook Voice Access-Nummer an, die in einem UM-Wählplan konfiguriert ist, ohne sich jedoch bei ihrem Postfach anzumelden. Nicht authentifizierte Benutzer rufen auch eine Nummer an, die in einer automatischen UM-Telefonzentrale konfiguriert ist. Authentifizierte Benutzer rufen eine Outlook Voice Access-Nummer an und melden sich erfolgreich bei ihrem Postfach an. Wenn Benutzer eine Outlook Voice Access-Nummer anrufen, gelten sie zunächst als nicht authentifiziert, weil sie nicht ihre Durchwahlnummer und PIN angegeben und sich nicht bei ihrem Postfach angemeldet haben. Benutzer sind authentifiziert, nachdem sie ihre Durchwahlnummer mit PIN angegeben und sich erfolgreich bei ihrem Postfach angemeldet haben.

Wenn ein nicht authentifizierter Benutzer bei einer UM-Telefonzentrale anruft und einen Anruf mithilfe von Outdialing tätigt, werden die Einstellungen für das Outdialing verwendet, die in den UM-Wähleinstellungen und für die Telefonzentrale konfiguriert sind. Wenn ein nicht authentifizierter Benutzer eine Outlook Voice Access-Nummer wählt, die in einem Wählplan konfiguriert ist, werden einzige die für den Wählplan konfigurierten Einstellungen verwendet. Wenn sich Benutzer jedoch erfolgreich bei ihrem Postfach angemeldet haben, werden für die authentifizierten Benutzer die Konfigurationseinstellungen des Wählplans sowie die UM-Postfachrichtlinie angewendet, die den authentifizierten Benutzern zugeordnet sind.

Sie müssen mehrere Einstellungen konfigurieren, um Outdialingregeln für Ihre Organisation zu aktivieren. Zum Steuern des Outdialings müssen Sie den UM-Wählplan, automatischen Telefonzentralen und UM-Postfachrichtlinien in Unified Messaging konfigurieren. Die folgenden Einstellungen können für UM-

Wähleinstellungen, automatische Telefonzentralen und UM-Postfachrichtlinien konfiguriert werden, um das Outdialing zu steuern:

- Amtskennziffer, nationale/regionale und internationale Zugriffscodes
- Nationales Rufnummernpräfix
- Nationale/regionale und internationale Nummernformate
- Nationale/regionale und internationale Wählregelgruppen
- Zulässige nationale/regionale und internationale Wählregelgruppen
- Wählregeleinträge

Sie konfigurieren Zugriffscodes, rufnummernpräfixe und nummernformate auf einem um-Wählplan auf der Seite **Wählen Sie eine Codes** in der Exchange-Verwaltungskonsole (EAC). Sie können auch die Einstellungen mithilfe des Cmdlets **Set-UMDialPlan** in Exchange Online PowerShell konfigurieren. Sie können auch alle Einstellungen, keine der Einstellungen oder nur einige dieser Einstellungen konfigurieren. Jede Einstellung steuert einen bestimmten Teil des Prozesses zum outdialing.

UM verwendet Zugriffscodes, Rufnummernpräfixe und Zahlenformate zur Ermittlung der richtigen zu wählenden Nummer. Sie können konfiguriert werden, um ausgehende Anrufer für Benutzer zu beschränken, die sich bei einer mit einem UM-Wählplan verknüpften automatischen UM-Telefonzentrale oder bei einer im Wählplan konfigurierten Outlook Voice Access-Nummer einwählen.

Weitere Informationen zum outdialing in Unified Messaging finden Sie unter [Kurzwahlnummern, rufnummernpräfixe, und Zahlenformate](#).

## Amtskennziffer

Sie können eine Amtskennziffer, auch als Amtsvorwahl bezeichnet, für jeden Satz Wähleinstellungen konfigurieren, den Sie erstellen. Dies ist die Nummer, die für den Zugriff auf eine Amtsleitung verwendet wird. Diese Nummer ist auch für die PBX-Anlagen (Private Branch eXchange, Nebenstellenanlage) oder die IP-PBX-Anlagen in der Organisation konfiguriert. In den meisten Telefonienetzwerken wählen die Benutzer die Nummer "9", um auf eine Amtsleitung zuzugreifen und eine externe Telefonnummer anzurufen.

Für jeden von Ihnen erstellten Wählplan sollte eine Amtskennziffer konfiguriert werden. Diese Kurzwahlnummer gilt für alle Benutzer, denen eine UM-Postfachrichtlinie zugeordnet ist, die wiederum mit dem UM-Wählplan verknüpft ist. Tätigt ein mit dem Wählplan verknüpfter Anrufer einen Anruf und wählt der Wählplan für den ausgehenden Anruf, fügt UM den Zugriffscode der Amtsleitung (üblicherweise die 9) vor der gewählten Nummernfolge hinzu, damit die PBX- oder IP PBX-Anlage die Nummer richtig wählt. Konfigurieren Sie den Amtsleitungs-Zugriffscode nicht, erkennt die PBX- oder IP-PBX-Anlage die gesendete Nummer nicht. Wie bereits erwähnt, lautet der Zugriffscode, den die Benutzer wählen, um auf eine Amtsleitung zuzugreifen, in vielen Organisationen beispielsweise "9", und diese Nummer wird auch für die PBX- oder IP-PBX-Anlage konfiguriert. Unified Messaging muss der Telefonnummernzeichenfolge für die PBX- oder IP-PBX-Anlage die Nummer "9" hinzufügen, damit die externe Nummer ordnungsgemäß gewählt wird. Wenn Sie die Kurzwahlnummer so konfigurieren, dass Unified Messaging den Zugriffscode der Amtsleitung hinzufügt, kann Unified Messaging mit diesem Zugriffscode auf eine Amtsleitung zugreifen, bevor die externe Telefonnummernfolge gewählt wird. Die von Ihnen konfigurierte Kurzwahlnummer gilt für alle Benutzer, denen eine UM-Postfachrichtlinie zugeordnet ist, die wiederum mit dem UM-Wählplan verknüpft ist.

## Rufnummernpräfix, national

Das nationale Rufnummernpräfix und die Landes-/Regionskennzahl können ebenfalls in UM-Wähleinstellungen konfiguriert werden. Unified Messaging verwendet die zum Wählen des korrekten nationalen Rufnummernprefixes bzw. der korrekten Landes-/Regionskennzahl eingegebene Nummer, wenn ein Benutzer eine

externe Rufnummer innerhalb des gleichen Landes/der gleichen Region anruft oder wenn es sich um einen internationalen Anruf handelt. Wenn ein Benutzer beispielsweise einen internationalen Anruf von Nordamerika nach Europa tätigt, stellt UM das nationale Nummernpräfix der Rufnummernfolge voran, die an die PBX- oder IP-PBX-Anlage gesendet wird, damit der ausgehende Anruf getätigst wird. Die Nummer "1" wird als nationales Nummernpräfix für Nordamerika verwendet.

## Länder-/Regionszugriffscode

In einem UM-Wählplan kann ein Länder-/Regionszugriffscode konfiguriert werden. Der Länder-/Regionszugriffscode besteht aus den Ziffern, die einem bestimmten Land oder einer Region zugeordnet sind. Der Länder-/Regionszugriffscode wird von Unified Messaging verwendet, um die richtige Telefonnummer zu wählen, wenn eine Rufnummer innerhalb des gleichen Landes oder der gleichen Region angerufen wird. UM diese Nummer der Rufnummernfolge voran, die er an die PBX- oder IP-PBX-Anlage sendet, wenn ein externer Anruf getätigst wird. Beispielsweise fügt der UM die Nummer "1" hinzu, wenn innerhalb der Vereinigten Staaten eine Rufnummer gewählt wird. Der Länder-/Regionscode für Großbritannien lautet "44".

## Internationale VAZ

In den UM-Wähleinstellungen kann eine internationale VAZ konfiguriert werden. Die internationale VAZ setzt sich aus den Ziffern zusammen, die für den Zugriff auf internationale Telefonnummern verwendet werden. Der internationale Zugriffscode wird von Unified Messaging zum Wählen des richtigen internationalen Zugriffscode verwendet, wenn ein Anruf von einer Telefonnummer innerhalb eines Landes/einer Region getätigst wird, der angerufene Anschluss sich jedoch in einem anderen Land/einer anderen Region befindet. UM diese Nummer der Rufnummernfolge voran, die er an die PBX- oder IP-PBX-Anlage sendet, wenn ein externer Anruf getätigst wird. Beispielsweise verwendet UM die Nummer "011" als internationalen Zugriffscode für die Vereinigten Staaten. Für Europa lautet die internationale VAZ "00".

## Nationale/regionale und internationale Nummernformate

Sie können die Konfiguration für eingehende Anrufe für nationale/regionale und internationale Nummernformate in einem UM-Wählplan festlegen. Nach der Konfiguration dieser Einstellungen ist Unified Messaging in der Lage, aus dem Inland/der Region und aus dem Ausland zwischen UM-Wählplänen innerhalb einer Organisation eingehende Anrufe zu erkennen. Sie können auch Zahlenformate für eingehende Anrufe hinzufügen, die in einen einzelnen Wählerplan eingefügt werden. Mit der Konfiguration dieser Optionen kann die Organisation Geld sparen, indem externe Anrufe verhindert werden, die die Benutzer nicht vom Arbeitsplatz aus tätigen dürfen. Außerdem tragen sie dazu bei, Betrug in Verbindung mit Telefongebühren zu vermeiden. UM verwendet die von Ihnen konfigurierten Informationen, um das Nummernformat des eingehenden Anrufs zu vergleichen und sicherzustellen, dass das Nummernmuster den Vorgaben entspricht, bevor der Anruf entgegengenommen wird. So können beispielsweise in einer Organisation mehrere Wählerpläne vorhanden sein. Wenn Sie über einen Wählerplan für die Vereinigten Staaten und einen weiteren für Großbritannien verfügen, möchten Sie möglicherweise dafür sorgen, dass die Benutzer im Wählerplan für die Vereinigten Staaten über UM zwar Benutzer im Wählerplan für Großbritannien anrufen können, jedoch keine direkten Anrufe zu Anschlüssen in anderen Ländern/Regionen oder von internationalen Anschlüssen tätigen können.

# Ermöglichen, dass Benutzer Anrufe Verfahren stellen

18.12.2018 • 2 minutes to read

[Aktivieren Sie ausgehende Anrufe für UM-IP-gateways](#)

[Deaktivieren ausgehender Anrufe für UM-IP-Gateways](#)

[Kurzwahlnummern konfigurieren](#)

[Erstellen von Wählregeln für Benutzer](#)

[Autorisieren von Anrufen mit Wählregeln](#)

[Autorisieren von Anrufen für Anrufer einer automatischen Telefonzentrale](#)

[Autorisieren von Anrufen für Benutzer in einem Wählplan](#)

[Autorisieren von Anrufen für eine Gruppe von Benutzern](#)

# Aktivieren Sie ausgehende Anrufe für UM-IP-gateways

18.12.2018 • 4 minutes to read

Sie können ausgehende Anrufe für ein UM-IP-Gateway (Unified Messaging) aktivieren, wenn ausgehende Anrufe deaktiviert worden sind. Wenn Sie in den Eigenschaften des UM-IP-Gateways die Option **Ausgehende Anrufe über dieses UM-IP-Gateway zulassen** aktivieren, konfigurieren Sie das UM-IP-Gateway für das Annehmen und Senden von ausgehenden Anrufen von einem/an ein VoIP-Gateway (Voice over IP), von einer/an eine Nebenstellenanlage, die für SIP (Session Initiation Protocol) aktiviert ist, von einer/an eine IP-Nebenstellenanlage oder von einem/an einen SBC (Session Border Controller). Obwohl die Einstellung **Ausgehende Anrufe über dieses UM-IP-Gateway zulassen** steuert, ob das UM-IP-Gateway ausgehende Anrufe für Benutzer initiiert kann, wirkt sie sich nicht auf Anruferübergaben oder eingehende Anrufe von einem VoIP-Gateway, einer für SIP aktivierten Nebenstellenanlage, einer IP-Nebenstellenanlage oder einem SBC aus.

Das Outdialing beschreibt eine Situation, in der ein Benutzer in einem UM-Wählplan einen UM-aktivierten Benutzer in einem anderen Wählanplan oder eine externe Telefonnummer anruft.

Um das Outdialing für UM-aktivierte Benutzer zu ermöglichen, müssen Sie die folgenden Aufgaben ausführen:

- Bestätigen, dass das UM-IP-Gateway ausgehende Anrufe zulässt.
- Erstellen von Wählregelgruppen, indem Wählregeleinträge für die UM-Wähleinstellungen erstellt werden, die dem UM-IP-Gateway zugeordnet sind.
- Hinzufügen der richtigen Wählregelgruppen zur Liste der Wähl einschränkungen unter **Wählautorisierung** im UM-Wählplan, in der automatische Telefonzentrale oder der UM-Postfachrichtlinie.

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren ausgehender Anrufe für ein UM-IP-Gateway mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-IP-Gateways**, wählen Sie den UM-IP-Gateway Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
2. Aktivieren Sie auf der Seite **UM-IP-Gateway** das Kontrollkästchen für **Ausgehende Anrufe über dieses UM-IP-Gateway zulassen**.
3. Klicken Sie auf **Speichern**.

Verwenden Sie Exchange Online PowerShell, um ausgehende Anrufe für ein UM-IP-Gateway zu aktivieren.

Dieses Beispiel aktiviert die ausgehende Anrufe auf einem UM-IP-Gateway mit dem Namen `MyUMIPGateway`.

```
Set-UMIPGateway -Identity MyUMIPGateway -OutcallsAllowed $true
```

# Deaktivieren Sie ausgehende Anrufe für UM-IP-gateways

18.12.2018 • 3 minutes to read

Sie können ausgehende Anrufe für ein UM-IP-Gateway (Unified Messaging) aktivieren oder deaktivieren. Wenn Sie das Kontrollkästchen **Ausgehende Anrufe über dieses UM-IP-Gateway zulassen** in den Eigenschaften des UM-IP-Gateways deaktivieren, konfigurieren Sie das UM-IP-Gateway so, dass ausgehende Anrufe an ein VoIP-Gateway, eine IP-Nebenstellenanlage oder einen SBC (Session Border Controller) nicht akzeptiert und gesendet werden. Obwohl die Einstellung **Ausgehende Anrufe über dieses UM-IP-Gateway zulassen** steuert, ob das UM-IP-Gateway ausgehende Anrufe für Benutzer initiiieren kann, wirkt sie sich nicht auf Anrufübergaben oder eingehende Anrufe von einem VoIP-Gateway, einer IP-Nebenstellenanlage oder einem SBC aus.

Zusätzliche Verwaltungstasks im Zusammenhang mit UM-IP-Gateways finden Sie unter [UM-IP-Gateway - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-IP-Gateways" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass ein UM-IP-Gateway erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-IP-Gateways](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Deaktivieren ausgehender Anrufe für ein UM-IP-Gateway mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-IP-Gateways**, wählen Sie den UM-IP-Gateway Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
2. Deaktivieren Sie auf der Seite **UM-IP-Gateway** das Kontrollkästchen für **Ausgehende Anrufe über dieses UM-IP-Gateway zulassen**.
3. Klicken Sie auf **Speichern**.

Verwenden Sie Exchange Online PowerShell, um ausgehende Anrufe

## für ein UM-IP-Gateway zu deaktivieren.

Dieses Beispiel deaktiviert die ausgehende Anrufe auf einem UM-IP-Gateway mit dem Namen `MyUMIPGateway`.

```
Set-UMIPGateway -Identity MyUMIPGateway -OutcallsAllowed $false
```

# Kurzwahlnummern konfigurieren

18.12.2018 • 4 minutes to read

Sie können Kurzwahlnummern, Rufnummernpräfixe und Nummernformate, die von Unified Messaging verwendet werden so konfigurieren, dass UM-aktivierte Benutzer ein- und ausgehende Anrufe einleiten können. In den meisten Fällen konfigurieren Sie einen Wählplan mit den Kurzwahlnummern, Rufnummernpräfixen und Nummernformaten, die derzeit in Ihrem Telefonienetzwerk konfiguriert sind.

Anhand der Kurzwahlnummern und Nummernpräfixe ermittelt UM die ordnungsgemäße Nummer, die bei einem Anruf gewählt werden soll, der von einem UM-aktivierten Benutzer eingeleitet wird. Outdialing ist der Begriff zum Beschreibens des Vorgangs, bei dem ein Benutzer in einem UM-Wählplan einen ausgehenden Anruf einleitet. Nummernformate werden für eingehende Anrufe in einem Land oder einer Region, internationale Anrufe oder Anrufe verwendet, die innerhalb eines Wählplans eingeleitet werden. Sie können einen Wählplan entsprechend dem Nummernformat eingehender Anrufe für nationale und internationale Nummern konfigurieren. Bei der Konfiguration der nationalen und internationalen Nummernformate können Sie eingehende Anrufe für Benutzer einschränken, die einem Wählplan zugeordnet sind.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Outdialing finden Sie unter [Ermöglichen, dass Benutzer Anrufe Verfahren stellen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren von Kurzwahlnummern, Rufnummernpräfixen und Nummernformaten über die Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. Wählen Sie aus dem um-Wählplan, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten**  

3. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
4. Füllen Sie auf der Seite **UM-Wählplan > Kurzwahlnummern** folgende Felder aus:
  - **Amtskennziffer**

- Internationale VAZ
- Rufnummernpräfix, national
- Länder-/Regionscode

5. Konfigurieren Sie unter **Nummernformate zum Wählen in Wählplänen** die folgenden Optionen:

- Nationales Nummernformat
- Internationales Nummernformat
- **Zahlenformate für eingehende Anrufe innerhalb desselben Wählplan**: Klicken Sie auf **Hinzufügen**, um ein Zahlenformat hinzuzufügen, .

6. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie einwählen, Codes, Präfixe und Zahlenformate

In diesem Beispiel wird einen um-Wählplan mit dem Namen konfiguriert `yUMDialPlan` mit ein Zahlenformat in Land oder Region, in einem internationalen Format und die folgenden Kurzwahlnummern:

- 9 für die Amtskennziffer
- 011 für die internationale VAZ
- 1 für das nationale Rufnummernpräfix
- 1 für den Länder-/Regionscode

```
Set-UMDialPlan -Identity MyUMDialPlan -OutsideLineAccessCode 9 -InternationalAccessCode 011 -
NationalNumberPrefix 1 CountryOrRegionCode 1 -InCountryOrRegionNumberFormat 1425xxxxxx -
InternationalNumberFormat 441425xxxxxx
```

# Erstellen von Wählregeln für Benutzer

18.12.2018 • 7 minutes to read

Wählregelgruppen bestehen aus Wähleinträgen. Wählregeln werden verwendet, um eine Telefonnummer zu ändern, bevor sie an die lokale Telefonanlage oder IP-Nebenstellenanlage für ausgehende Anrufe gesendet wird. Wählregeln dienen zwei Zwecken:

- Sie geben die Nummern an, die für ausgehende Anrufe gewählt werden können. Beim Erstellen einer Wählregel geben Sie die Nummernformate an, die gewählt werden können. Entspricht eine Nummer keinem der angegebenen Formate, wird sie abgelehnt. Wenn Sie keine Wählregeln festlegen, können die Anrufer zwar Anrufe innerhalb der Organisation tätigen, ausgehende Anrufe sind jedoch nicht möglich.
- Sie wandeln die gewählten Nummern um, bevor sie an die lokale Telefonanlage gesendet werden. Mit Wählregeln können Zahlen aus der gewählten Nummer entfernt oder Zahlen zur gewählten Nummer hinzugefügt werden. Sie können beispielsweise mithilfe von Wählregeln die Amtskennziffer für Ihre Telefonanlage hinzufügen oder den Länder-/Regionscode für Fern- oder Ortsgespräche hinzufügen oder entfernen.

Zum Angeben der Typen ausgehender Anrufe, die Sie für einen UM-Wählplan zulassen möchten, erstellen Sie eine Wählregelgruppe mit Wählregeln, mit denen Sie anschließend ausgehende Anrufe für Outlook Voice Access-Benutzer und Anrufer zulassen, die sich in die automatische UM-Telefonzentrale einwählen. Für nationale/regionale Anrufe und internationale Anrufe erstellen Sie gesonderte Wählregeln.

## NOTE

Wenn Sie UM mit Microsoft Lync Server integrieren, wird empfohlen, dass Sie mindestens eine Wählregelgruppe erstellen und diese in den SIP-URI-Wählplänen, UM-Postfachrichtlinien und automatischen UM-Telefonzentralen für die Weiterleitung ausgehender Anrufe an Server mit Lync autorisieren.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Outdialing finden Sie unter [Ermöglichen, dass Benutzer Anrufe Verfahren stellen](#).

## Beispiele für häufig verwendete Wählregeln

NUMMERNMUSTER	GEWÄHLTE NUMMER	MÖGLICHES Szenario FÜR DIESE WÄHLREGEL
*	*	Ermöglichen aller ausgehenden Anrufe.
1425xxxxxx	91425xxxxxx	Verhindern, dass Benutzer eine interne Durchwahl anrufen oder ein Fehler auftritt, wenn die Benutzer vergessen, die Amtskennziffer zu wählen.
1xxxxxxxxx	1xxxxxxxxx	Zulassen aller Nummern, die mit "1" beginnen.
xxxxxx	1425xxxxxx	Hinzufügen einer "1" und der Ortsvorwahl 425 zu siebenstelligen Nummern.

# Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Wenn Sie Wählregelgruppen auf UM-Postfachrichtlinien anwenden, müssen Sie bestätigen, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Wenn Sie Wählregelgruppen auf automatische UM-Telefonzentralen anwenden, müssen Sie bestätigen, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Erstellen einer Wählregel mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
3. Klicken Sie auf der Seite **UM-Wählplan > Wählregeln**, klicken Sie auf **Hinzufügen** unter **nationale/regionale Wählregeln** oder **International Wählregeln**.
4. Geben Sie auf der Seite **Neue Wählregel** die folgenden Informationen ein:
  - **Regelname einwählen:** Geben Sie den Namen der Regel Wählvorgang Gruppe, die diese Regel eines Teils werden soll. Um mit anderen Regeln zu kombinieren, verwenden Sie den gleichen Gruppennamen. Um eine neue Gruppe von Wählvorgang Regel zu erstellen, geben Sie einen neuen eindeutigen Namen ein.
  - **Nummernmuster zur Transformation von (Zahl Maske):** Geben Sie das Nummernmuster vor dem Wählen 91425xxxxxx umgewandelt. Wenn ein Anrufer eine Nummer, die mit übereinstimmt wählt, überträgt UM es auf die gewählte Nummer angerufene den Anruf entgegennehmen. Geben Sie nur Zahlen und das Platzhalterzeichen (X). Nummernmuster steht für eine Zahl Maske.
  - **Anzahl der Dialed:** Geben Sie die Nummer zu wählen. Verwenden Sie nur Zahlen und das Platzhalterzeichen (X), wie in der Zahl Muster 9xxxxxx. Platzhalter (X) werden durch die Ziffern, aus der ursprünglichen vom Benutzer gewählte Nummer ersetzt. Stellen Sie sicher, dass die Anzahl von Platzhaltern in der gewählten Nummer, die die Anzahl von Platzhaltern in das Nummernmuster identisch ist.
  - **Kommentar:** Geben Sie einen Kommentar oder eine Beschreibung für diese Wählregel. Den Kommentar

können Sie die Regel, z. B. "Add a 9, um ausgehende Anrufe." Funktionsweise beschreiben

5. Klicken Sie auf **OK**, um die Wählregel zu speichern. Geben Sie ggf. weitere Regeln ein, und verwenden Sie dabei für Regeln, die gemeinsam autorisiert werden sollen, den gleichen Namen für die Wählregelgruppe.

# Autorisieren von Anrufen mit Wählregeln

18.12.2018 • 4 minutes to read

Benutzer können standardmäßig keine ausgehenden Anrufe tätigen. Um die Arten von Anrufen festzulegen, die von Benutzern getätigt werden können, erstellen Sie zunächst Wählregeln, und autorisieren Sie dann Gruppen dieser Wählregeln in UM-Wählplänen, UM-Postfachrichtlinien oder automatischen UM-Telefonzentralen. Damit Sie Wählregelgruppen autorisieren können, müssen Wählregeln in einem UM-Wählplan definiert werden. Weitere Informationen finden Sie unter [Erstellen von Wählregeln für Benutzer](#).

Jede von Ihnen erstellte Wählregel enthält die Anruftypen oder Nummernmuster, für die Sie den Benutzern Zugriff erteilen möchten. Sie können verschiedenen Typen von Benutzern das Tätigen verschiedener Anruftypen erlauben. Die von Ihnen zugelassenen Anrufe können innerhalb eines Landes oder einer Region oder auch im Ausland liegen.

Zum Autorisieren oder Einschränken der Wählfunktion müssen die folgenden Einstellungen richtig konfiguriert werden:

- **Wählregeln:** Wählregeln definieren, die Nummer, die UM-aktivierten Benutzer wählen und die Anzahl, die durch die Private Branch eXchange, (Nebenstellenanlage PBX) oder die IP-Nebenstellenanlage gewählt und von Unified Messaging gesendet werden. Sie erstellen eine Wählvorgang Regelgruppe durch Hinzufügen einer Wählregel. Nachdem eine Gruppe der Wählvorgang Regel erstellt wurde, fügen Sie es zur Liste der autorisierten Anrufe für eine nationale/regionale und internationale Wählvorgang Regelgruppe.
- **Wählregelgruppen:** Wählvorgang Regel Gruppen bestimmt die Arten von Anrufen, die Benutzer in der Gruppe Wählvorgang vornehmen können.
- **Autorisierung einwählen:** Wählvorgang Zulassung werden verwendet, um die Einschränkungen zu ermitteln, die angewendet werden, um Benutzer verhindern können, dass Gebühren für unnötige Telefon anfallen oder Ferngespräche einwählen.

## Wie autorisiere ich eine Wählregelgruppe?

An welcher Stelle Sie Wählregelgruppen autorisieren, hängt von den Anruftypen ab, denen Sie ausgehende Anrufe erlauben möchten. Wenn Sie beispielsweise nur Outlook Voice Access-Benutzern das Tätigen ausgehender Anrufe erlauben möchten, erstellen Sie die Wählregeln und autorisieren anschließend diese Wählregelgruppen bei der UM-Postfachrichtlinie, mit der die Outlook Voice Access-Benutzer verknüpft sind. Die folgende Tabelle zeigt, wie Anrufe für verschiedene Typen von Anrufern autorisiert werden.

ANRUFERTYP	WÄHLREGELGRUPPEN HIER AUTORISIEREN
Nicht authentifizierte Anrufer, die sich bei einer Outlook Voice Access-Nummer einwählen und keine PIN eingeben	UM-Wählplan. Weitere Informationen finden Sie unter <a href="#">Autorisieren von Anrufen für Benutzer in einem Wählplan</a> .
Authentifizierte Anrufer, die sich bei einer Outlook Voice Access-Nummer einwählen und eine PIN eingeben	UM-Postfachrichtlinie für den Anrufer. Weitere Informationen finden Sie unter <a href="#">Autorisieren von Anrufen für eine Gruppe von Benutzern</a> .
Nicht authentifizierte Anrufer, die sich bei einer Telefonnummer einwählen, die für eine automatische UM-Telefonzentrale konfiguriert ist	Automatische UM-Telefonzentrale. Weitere Informationen finden Sie unter <a href="#">Autorisieren von Aufrufen für automatische Telefonzentralen Anrufer</a> .

Je nachdem, welche Benutzer Sie für das tätigen ausgehender Anrufe autorisieren, verwenden Sie die Seite

**Wählautorisierung** in der Exchange-Verwaltungskonsole für den Wählplan, die automatische Telefonzentrale oder die UM-Postfachrichtlinie.

# Autorisieren von Aufrufen für automatische Telefonzentralen Anrufer

18.12.2018 • 4 minutes to read

Sie können Wählautorisierungen für eine automatische Unified Messaging-Telefonzentrale (UM) aktivieren. Wählautorisierungen für eine automatische Telefonzentrale dienen zum Unterbinden, dass Benutzer, die sich in die automatische Telefonzentrale einwählen, Fern- oder Auslandsgespräche bzw. Outdialing-Telefonate führen. Outdialing erfolgt, wenn Unified Messaging einen ausgehenden Anruf für einen Benutzer tätigt, nachdem dieser sich bei einer Telefonnummer eingewählt hat, die für eine automatische UM-Telefonzentrale konfiguriert ist.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Outdialing finden Sie unter [Ermöglichen, dass Benutzer Anrufe Verfahren stellen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Automatische um-Telefonzentralen" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine automatische UM-Telefonzentrale erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer automatischen UM-Telefonzentrale](#).
- Bestätigen Sie, bevor Sie diese Verfahren durchführen, dass regionale/nationale und internationale Wählregeln für einen UM-Wählplan erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen von Wählregeln für Benutzer](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren von Wählautorisierungen für eine automatische UM-Telefonzentrale für nationale/regionsinterne Regelgruppen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  

2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie eine wählberechtigungen erstellen möchten, und klicken Sie dann auf

**Bearbeiten**

3. Klicken Sie auf der Seite **UM-Telefonzentrale > Autorisierung einwählen**, klicken Sie auf **Hinzufügen**  unter **nationale/regionale Wählregelgruppen autorisiert**.
4. Wählen Sie auf der Seite **Wählregelgruppen für Zulassen auswählen** die Wählregelgruppe aus, klicken Sie auf **OK** und dann auf **Speichern**.

## Aktivieren von Wählautorisierungen für eine automatische UM-Telefonzentrale für internationale Regelgruppen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** .
2. Wählen Sie auf der Seite **UM-Wählplan** unterhalb von **Automatische UM-Telefonzentralen**, UM-Telefonzentrale für die Sie eine wählberechtigungen erstellen möchten, und klicken Sie dann auf **Bearbeiten** .
3. Klicken Sie auf der Seite **UM-Telefonzentrale > Autorisierung einwählen**, klicken Sie auf **Hinzufügen**  unter **internationale Wählregelgruppen autorisiert**.
4. Wählen Sie auf der Seite **Wählregelgruppen für Zulassen auswählen** die Wählregelgruppe aus, klicken Sie auf **OK** und dann auf **Speichern**.

## Verwenden von Exchange Online PowerShell nationale/regionale und internationale Wählvorgang Autorisierung auf eine automatische um-Telefonzentrale aktivieren

Dieses Beispiel aktiviert die InCountry/RegionGroup1, InCountry/RegionGroup2, InternationalGroup1 und InternationalGroup2 Wählvorgang Autorisierung auf einem um-WÄHLPLAN automatische um-Telefonzentrale mit dem Namen .

```
Set-UMAutoAttendant -Identity MyUMAutoAttendant -AllowedInCountryOrRegionGroups  
InCountry/RegionGroup1,InCountry/RegionGroup2 -AllowedInternationalGroups  
InternationalGroup1,InternationalGroup2
```

# Autorisieren von Anrufen für Benutzer in einem Wählplan

18.12.2018 • 4 minutes to read

Sie können Wählautorisierungen für einen UM-Wählplan (Unified Messaging) aktivieren. Wählautorisierungen für einen Wählplan dienen zum Unterbinden, dass nicht authentifizierte Outlook Voice Access-Benutzer Fern- oder Auslandsgespräche bzw. Outdialing-Telefonate führen. Outdialing erfolgt, wenn Unified Messaging einen ausgehenden Anruf für einen Benutzer einleitet, nachdem dieser sich bei einer Outlook Voice Access-Telefonnummer eingewählt hat, die für einen UM-Wählplan konfiguriert ist. Wenn Sie eine Einstellung für einen UM-Wählplan konfigurieren, gilt diese für alle nicht authentifizierten Benutzer, die sich bei einer Outlook Voice Access-Nummer einwählen.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Outdialing finden Sie unter [Ermöglichen, dass Benutzer Anrufe Verfahren stellen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Bestätigen Sie, bevor Sie dieses Verfahren durchführen, dass nationale und internationale Wählregeln für einen UM-Wählplan erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen von Wählregeln für Benutzer](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Aktivieren von Wählautorisierungen für nationale Regelgruppen in einem UM-Wählplan

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
3. Klicken Sie auf der Seite **UM-Wählplan > Autorisierung einwählen**, klicken Sie auf **Hinzufügen**  
 unter **nationale/regionale Wählregelgruppen autorisiert**.

4. Wählen Sie auf der Seite **Wählregelgruppen für Zulassen auswählen** die Wählregelgruppe aus, klicken Sie auf **OK** und dann auf **Speichern**.

## Verwenden der Exchange-Verwaltungskonsole zum Aktivieren von Wählautorisierungen für internationale Wählregelgruppen in einem UM-Wählplan

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  
[ ]
2. Klicken Sie auf der Seite **UM-Wählplan** auf **Konfigurieren**.
3. Klicken Sie auf der Seite **UM-Wählplan > Autorisierung einwählen**, klicken Sie auf **Hinzufügen**  
[ ] unter **internationale Wählregelgruppen autorisiert**.
4. Wählen Sie auf der Seite **Wählregelgruppen für Zulassen auswählen** die Wählregelgruppe aus, klicken Sie auf **OK** und dann auf **Speichern**.

## Verwenden von Exchange Online PowerShell nationale/regionale und internationale Wählvorgang Autorisierung auf einem um-Wählplan aktivieren

Dieses Beispiel aktiviert die InCountry/RegionGroup1, InCountry/RegionGroup2, InternationalGroup1 und InternationalGroup2 Wählvorgang Autorisierung auf eine automatische UM-Wählplan mit dem Namen

[ ] MyUMDialPlan .

```
Set-UMDialPlan -Identity MyUMDialPlan -AllowedInCountryOrRegionGroups  
InCountry/RegionGroup1,InCountry/RegionGroup2 -AllowedInternationalGroups  
InternationalGroup1,InternationalGroup2
```

# Autorisieren von Anrufen für eine Gruppe von Benutzern

18.12.2018 • 4 minutes to read

Sie können Wählautorisierungen für eine UM-Postfachrichtlinie (Unified Messaging) aktivieren. Wählautorisierungen für eine Postfachrichtlinie dienen zum Unterbinden, dass authentifizierte Outlook Voice Access-Benutzer, die der UM-Postfachrichtlinie zugeordnet sind, nationale bzw. internationale oder Outdialing-Telefonate führen. Outdialing erfolgt, wenn Unified Messaging einen ausgehenden Anruf für einen Benutzer einleitet, nachdem dieser sich bei einer Outlook Voice Access-Telefonnummer eingewählt hat, die für einen UM-Wählplan konfiguriert ist. Die in einer UM-Postfachrichtlinie konfigurierten Einstellungen gelten für alle UM-aktivierten Benutzer, die der UM-Postfachrichtlinie zugeordnet sind.

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Outdialing finden Sie unter [Ermöglichen, dass Benutzer Anrufe Verfahren stellen](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#) .
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Ausführliche Anleitungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Bestätigen Sie, bevor Sie diese Verfahren durchführen, dass regionale/nationale und internationale Wählregeln für einen UM-Wählplan erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen von Wählregeln für Benutzer](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Aktivieren von Wählautorisierungen für regionale/nationale Wählregelgruppen in einer UM-Postfachrichtlinie

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Wählen Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, die um-Postfachrichtlinie für die Sie eine wählberechtigungen erstellen möchten, und klicken Sie dann auf **Bearbeiten**
3. Klicken Sie auf der Seite **Um-Postfachrichtlinie > Autorisierung einwählen**, klicken Sie auf

**Hinzufügen**  unter **nationale/regionale Wählregelgruppen autorisiert**.

4. Wählen Sie auf der Seite **Wählregelgruppen für Zulassen auswählen** die Wählregelgruppe aus, klicken Sie auf **OK** und dann auf **Speichern**.

Verwenden der Exchange-Verwaltungskonsole zum Aktivieren von Wählautorisierungen für internationale Wählregelgruppen in einer UM-Postfachrichtlinie

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Wählen Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, die um-Postfachrichtlinie für die Sie eine wählberechtigungen erstellen möchten, und klicken Sie dann auf **Bearbeiten**
3. Klicken Sie auf der Seite **Um-Postfachrichtlinie > Autorisierung einwählen**, klicken Sie auf **Hinzufügen**  unter **internationale Wählregelgruppen autorisiert**.
4. Wählen Sie auf der Seite **Wählregelgruppen für Zulassen auswählen** die Wählregelgruppe aus, klicken Sie auf **OK** und dann auf **Speichern**.

Verwenden von Exchange Online PowerShell um nationale/regionale und internationale Wählvorgang Autorisierung auf einer um-Postfachrichtlinie zu aktivieren

Dieses Beispiel aktiviert die InCountry/RegionGroup1, InCountry/RegionGroup2, InternationalGroup1 und InternationalGroup2 zu erteilenden auf einem UM-Postfachrichtlinie mit der Bezeichnung Wählvorgang  MyUMMailboxPolicy .

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowedInCountryOrRegionGroups  
InCountry/RegionGroup1,InCountry/RegionGroup2 -AllowedInternationalGroups  
InternationalGroup1,InternationalGroup2
```

# Einrichten von eingehenden Faxen

18.12.2018 • 14 minutes to read

Microsoft Exchange Unified Messaging (UM) verwendet zertifizierte Faxpartnerlösungen, um erweiterte Faxfunktionen bereitzustellen, z. B. ausgehende Faxe oder Faxrouting. Standardmäßig sind Exchange-Server nicht so konfiguriert, dass eingehende Faxe an einen UM-aktivierten Benutzer zugestellt werden. Stattdessen leitet ein Exchange-Server eingehende Faxanrufe an eine zertifizierte Faxpartnerlösung um. Der Server des Faxpartners empfängt die Faxdaten und sendet sie dann in einer E-Mail-Nachricht, in die das Fax als TIF-Anlage eingeschlossen ist, an das Benutzerpostfach.

Weitere Informationen zu Fax Partner finden Sie unter [Microsoft Hindernissen bei für Fax Partner](#).

## Bereitstellen und Konfigurieren von Faxfunktionen

UM leitet eingehende Faxanrufe an eine dafür vorgesehene Faxpartnerlösung weiter, die dann die Faxverbindung mit dem Faxabsender aufbaut und die Nachricht für den UM-aktivierten Benutzer empfängt. Damit UM-aktivierte Benutzer Faxnachrichten in ihren Postfächern erhalten, müssen Sie jedoch zunächst die Funktion für eingehende Faxanrufe aktivieren und den URI des Faxpartners in der UM-Postfachrichtlinie festlegen, die mit den UM-aktivierten Benutzern verknüpft ist. Eingehende Faxanrufe können in UM-Wählplänen, UM-Postfachrichtlinien und im Postfach für einen UM-aktivierten Benutzer erlaubt oder verhindert werden. Weitere Informationen finden Sie in den folgenden Themen:

- [Zulassen des Empfangs von Faxnachrichten für Benutzer mit demselben Wählplan](#)
- [Unterbinden des Empfangs von Faxnachrichten für Benutzer mit demselben Wählplan](#)
- [Aktivieren der Faxfunktion für eine Gruppe von Benutzern](#)
- [Deaktivieren der Faxfunktion für eine Gruppe von Benutzern](#)
- [Aktivieren eines Benutzers für den Faxempfang](#)
- [Verhindert, dass Benutzer empfangen von Faxnachrichten](#)

### Schritt 1: Bereitstellen von Unified Messaging

Bevor Sie können für Ihre lokale oder Hybrid Faxe einrichten Organisation, müssen Sie erfolgreich Clientzugriffs- und Postfachserver bereitstellen und Konfigurieren von Ihr unterstützten VoIP über IP (VoIP)-Gateways Faxe zulassen. Ausführliche Informationen zum Bereitstellen von UM finden Sie unter [Bereitstellen von Exchange Server UM](#). Ausführliche Informationen zur Bereitstellung von VoIP-Gateways und Nebenstellenanlagen IP Private Branch Exchange (Exchange, PBX) finden Sie unter [Connect UM to Your Telefonsystem](#).

#### IMPORTANT

Das Senden und Empfangen von Faxes mithilfe von T.38 oder G.711 wird in einer Umgebung, in der Unified Messaging und Microsoft Office Communications Server 2007 R2 oder Microsoft Lync Server integriert sind, nicht unterstützt.

### Schritt 2: Konfigurieren von Faxpartnerservern

Als Nächstes müssen Sie die Funktion für eingehende Faxanrufe aktivieren und den URI des Faxpartners in allen UM-Postfachrichtlinien festlegen, die Sie in Ihrer Organisation benötigen. Zur erfolgreichen Bereitstellung der Funktion für eingehende Faxanrufe müssen Sie eine zertifizierte Faxpartnerlösung in Exchange Unified Messaging integrieren. Weitere Informationen finden Sie unter [Faxratgeber für Exchange UM](#). Eine Liste zertifizierter

**NOTE**

Da der Faxpartnerserver außerhalb Ihrer Organisation liegt, müssen Firewallports für das Zulassen der T.38-Protokollports konfiguriert werden, die die Faxfunktion über ein IP-basiertes Netzwerk ermöglichen. Standardmäßig verwendet das T.38-Protokoll TCP-Port 6004. Es kann auch UDP-Port 6044 (User Datagram Protocol) verwenden, dies wird jedoch vom Hardwarehersteller definiert. Die Firewallports müssen für das Zulassen von Faxdaten konfiguriert werden, welche die vom Hersteller definierten TCP- oder UDP-Ports oder Portbereiche verwenden.

### Schritt 3: Aktivieren der Faxfunktion unter Unified Messaging

Drei Komponenten müssen konfiguriert werden, damit Benutzer Faxnachrichten mithilfe von Unified Messaging empfangen können:

- UM-Wähleinstellungen
- UM-Postfachrichtlinien
- UM-Postfächer

Senden von FAXen kann aktiviert oder deaktiviert für UM-Wählpläne UM-Postfachrichtlinien oder für einzelne UM-aktivierten Postfach eines Benutzers werden. UM-Postfachrichtlinien können aktiviert oder deaktiviert für das Senden von FAXen über die Exchange-Verwaltungskonsole (EAC) oder Exchange Online PowerShell werden. Aktivieren und Deaktivieren von Wähleinstellungen und einzelnen UM-aktivierten Benutzern ausgeführt werden soll von Exchange Online PowerShell. Die folgende Tabelle zeigt die Optionen, die verfügbar sind und die Cmdlets und Parameter, die zum Aktivieren und Deaktivieren von FAXen verwendet werden.

UM-KOMPONENTE	AKTIVIEREN/DEAKTIVIEREN MITHILFE DER EXCHANGE-VERWALTUNGSKONSEL?	EXCHANGE ONLINE POWERSHELL-BEISPIEL FÜR DAS SENDEN VON FAXEN AKTIVIEREN
Wählplan	Nein	<pre>Set-UMDialPlan -Identity MyUMDialPlan -faxenabled \$true</pre>
UM-Postfachrichtlinie	Ja	<pre>Set-UMMaiboxPolicy -Identity MyPolicy -AllowFax \$true</pre>
UM-aktivierter Benutzer	Nein	<pre>Set-UMMailbox -Identity tonysmith -faxenabled \$true</pre>

Obwohl der UM-Wählplan und das Postfach eines Benutzers den Empfang eingehender FAXe standardmäßig zulässt, müssen Sie zunächst den FAXeingang in der dem UM-aktivierten Benutzer zugeordneten UM-Postfachrichtlinie aktivieren und dann den URI des Faxpartnerservers eingeben.

Gehen Sie folgendermaßen vor, um den Faxempfang für UM-aktivierte Benutzer zu ermöglichen:

- Stellen Sie sicher, dass alle UM-Wähleinstellungen den Faxempfang für Benutzer, die diesen Wähleinstellungen zugeordnet sind, zulassen. Standardmäßig können alle Benutzer, die einem Satz Wähleinstellungen zugeordnet sind, Faxnachrichten empfangen. Damit UM-aktivierte Benutzer Faxnachrichten in ihrem Postfach empfangen, muss jedes VoIP-Gateway bzw. jede IP-Nebenstellenanlage für die Annahme eingehender Faxanrufe konfiguriert werden. Ferner müssen Sie ermöglichen, dass Faxnachrichten von Benutzern empfangen werden können, die mit dem Wählplan verknüpft sind. Weitere Informationen zum Ermöglichen oder Verhindern des Faxempfangs für Benutzer, die mit einem Wählplan verknüpft sind, finden Sie unter [Aktivieren eines Benutzers für den Faxempfang](#).

#### NOTE

Wenn Sie das Empfangen von Faxnachrichten für einen Wählplan deaktivieren, kann keiner der Benutzer, die diesem Wählplan zugeordnet sind, Faxnachrichten empfangen, selbst wenn Sie die Eigenschaften eines einzelnen Benutzers für den Empfang von Faxnachrichten konfigurieren. Das Aktivieren bzw. Deaktivieren von Faxnachrichten für einen Satz UM-Wähleinstellungen hat Vorrang vor den Einstellungen für einen einzelnen UM-aktivierten Benutzer.

- Konfigurieren der UM-Postfachrichtlinie, die mit dem UM-aktivierten Benutzer zugeordnet ist. Die um-Postfachrichtlinie muss für eingehende Faxe, einschließlich der faxpartner-URI und den Namen des Servers für die faxpartner konfiguriert werden. Der Parameter *FaxServerURI* muss das folgende Format verwenden: `sip:<Faxserver URI>:<Port>; <Transport>`, wobei "Faxserver URI" einen vollqualifizierten Domänennamen (FQDN) oder eine IP-Adresse des Faxservers Partner entspricht. Der "Port" ist der Port auf dem Faxserver prüft auf eingehende Faxanrufe und "Transport" ist das Transportprotokoll, das für die eingehende Faxe (UDP, TCP oder Transport Layer Security (TLS)) verwendet wird. Beispielsweise können Sie eine um-Postfachrichtlinie Empfang von Faxen wie folgt konfigurieren.

```
Set-UMMailboxPolicy MyUMMailboxPolicy -AllowFax $true -FaxServerURI  
"sip:faxserver.abc.com:5060;transport=tcp"
```

- Weitere Informationen finden Sie unter [Festlegen des Partners Faxserver URI zum Senden von Faxen zulassen](#).

#### Caution

Obwohl Sie mehrere Einträge im Format für die *FaxServerURI* hinzufügen können, indem Sie diese durch ein Semikolon voneinander, wird nur ein Eintrag verwendet werden. Mit diesem Parameter können nur einen Eingangs-, verwendet werden soll, und mehrere Einträge hinzufügen aktivieren wird nicht, Sie Laden des Lastenausgleichs für Fax Anforderungen.

- Stellen Sie sicher, dass das UM-aktivierte Postfach Faxnachrichten empfangen kann. Standardmäßig können alle Benutzer, die einem Satz Wähleinstellungen zugeordnet sind, Faxnachrichten empfangen. Es kann jedoch Situationen geben, in denen Benutzer keine Faxnachrichten empfangen können, da der Faxempfang für ihr Postfach deaktiviert wurde. Weitere Informationen zum Aktivieren von UM-aktivierten Benutzern für den Empfang von Faxnachrichten finden Sie unter [Aktivieren eines Benutzers für den Faxempfang](#).

Sie können einen einzelnen Benutzer verhindern, die mit einem Wählplan in empfangen von Faxnachrichten zugeordnet ist. Zu diesem Zweck konfigurieren Sie die Eigenschaften für den Benutzer mithilfe des **Set-UMMailbox** -Cmdlets in Exchange Online PowerShell aus. Sie können auch das Cmdlet **Set-UMMailboxPolicy** verwenden, um zu verhindern, dass mehrere Benutzer empfangen von Faxnachrichten. Weitere Informationen dazu, wie Sie verhindern, dass der Benutzer empfangen von Faxnachrichten finden Sie unter [verhindern, dass einen Benutzer empfangen von Faxnachrichten](#).

### Schritt 4: Konfigurieren der Authentifizierung

Neben den UM-Wähleinstellungen, UM-Postfachrichtlinien und UM-aktivierten Benutzern müssen Sie auch die Authentifizierung zwischen Ihren Exchange-Servern und dem Faxpartnerserver konfigurieren. Die Exchange-Server müssen den Ursprung der Nachrichten authentifizieren, die angeblich vom Server des Faxpartners stammen. Nicht authentifizierte Nachrichten, die angeblich von einem Faxpartnerserver stammen, werden von einem Exchange-Server nicht verarbeitet.

Für die Authentifizierung der Verbindung vom Faxpartnerserver zu den Exchange-Servern können Sie Folgendes verwenden:

- Mutual TLS
- Sender ID-Überprüfung

- Einen dedizierten Empfangsconnector

Ein Empfangsconnector sollte ausreichen, um die in Ihrer Organisation bereitgestellten Faxpartnerserver zu authentifizieren. Der Empfangsconnector gewährleistet, dass die Exchange-Server den gesamten vom Faxpartnerserver eingehenden Datenverkehr als authentifiziert behandeln.

Der Empfangsconnector wird auf einem Exchange-Server konfiguriert, der vom Faxpartnerserver zum Senden von SMTP-Faxnachrichten verwendet wird. Er muss mit den folgenden Werten konfiguriert werden:

- *AuthMechanism*: ExternalAuthoritative
- *PermissionGroups*: ExchangeServers, PartnersFax
- *RemoteIPRanges*: {IP-Adresse des Faxservers}
- *RequireTLS*: falsch
- *EnableAuthGSSAPI*: falsch
- *LiveCredentialEnabled*: falsch

Weitere Informationen finden Sie unter [Connectors](#).

Wenn der Faxpartnerserver Netzwerkdatenverkehr über ein öffentliches Netzwerk an einen Exchange-Server sendet, z. B. ein in der Cloud gehosteter dienstbasierter Faxpartnerserver, sollten Sie den Faxpartnerserver anhand einer Sender ID-Prüfung authentifizieren. Diese Art der Authentifizierung gewährleistet, dass die IP-Adresse, von der die Faxnachricht stammt, autorisiert ist, eine E-Mail-Nachricht im Namen der Faxpartnerdomäne zu senden, von der die Nachricht angeblich stammt. Zum Speichern der Sender ID-Datensätze (oder SPF-Datensätze (Sender Policy Framework)) wird DNS verwendet, und Faxpartner müssen ihre SPF-Datensätze in der DNS-Forward-Lookupzone veröffentlichen. Exchange überprüft die IP-Adressen durch eine DNS-Abfrage. Der Sender ID-Agent muss jedoch auf einem Postfachserver ausgeführt werden, um eine DNS-Abfrage ausführen zu können.

Sie können auch TLS zum Verschlüsseln des Netzwerkdatenverkehrs oder MTLS (Mutual TLS) für die Verschlüsselung und Authentifizierung zwischen dem Faxpartnerserver und den Exchange-Servern verwenden.

# Faxratgeber für Exchange UM

18.12.2018 • 5 minutes to read

Partnerlösungen für erweiterte Fax-Funktionen, beispielsweise Fax routing oder ausgehende Faxnachrichten zertifizierten Fax nutzt Microsoft Unified Messaging (UM). Benutzer werden nicht standardmäßig so konfiguriert, damit eingehender Faxnachrichten an einen UM-aktivierten Benutzer übermittelt werden können. Exchange Server senden die Fax-Anforderungen an eine Fax certified Partner-Lösung. Fax Partnerserver empfängt Fax-Daten, und klicken Sie dann auf das Postfach des Empfängers in einer e-Mail-Nachricht sendet, mit dem Fax als Anlage zu einer TIF enthalten. Weitere Informationen hierzu finden Sie unter [Voice E-Mail-Benutzer zum Empfangen von Faxnachrichten aktivieren.](#)

## IMPORTANT

Es wird empfohlen, dass alle Benutzer, die Unified Messaging bereitstellen möchten einen Unified Messaging-Experten zu erhalten. Unified Messaging-Spezialist wird sichergestellt, dass es ein reibungslosen Übergang zu Unified Messaging aus einem älteren Voicemail-System ist. Durchführen einer neuen bereitstellungs oder Aktualisieren von einer älteren Voicemail-Systems erfordert beträchtliche Kenntnisse über Nebenstellenanlagen und Unified Messaging. Finden Sie weitere Informationen zur Kontaktaufnahme mit einem Unified Messaging-Spezialisten [Spezialisten für Microsoft Exchange Server Unified Messaging \(UM\)](#) oder [Microsoft Hindernissen bei für Unified Messaging.](#)

## Faxpartnerprogramm für Exchange Unified Messaging

Um Faxpartner mit zertifizierter Interoperabilität mit Exchange UM zu werden, muss der Partner die in der Interoperabilitätsspezifikation für Faxpartner (Fax Partner Interoperability Specification) enthaltenen Anforderungen implementieren, und die Faxlösung muss von einem unabhängigen Zertifikatanbieter zertifiziert werden.

## Als interoperabel mit Unified Messaging zertifizierte Faxpartnerlösungen

Wenn Sie Exchange Unified Messaging bereits bereitgestellt haben und auf der Suche nach einem Faxpartner sind, der eingehende Faxe in Ihrer Organisation ermöglicht, finden Sie weitere Informationen unter [Microsoft Pinpoint für Faxpartner](#). Diesen Softwareherstellern wurde Interoperabilität mit Exchange Server zertifiziert, und sie stellen zertifizierte Softwarelösungen für Unified Messaging bereit.

## Unterstützung von VoIP, Mediengateways und IP-Nebenstellenanlagen

Bei der Konfiguration von VoIP-Gateways in Ihrer Organisation handelt es sich um eine schwierige Bereitstellungsaufgabe, deren erfolgreicher Abschluss Voraussetzung dafür ist, dass Exchange Unified Messaging erfolgreich für eingehende Faxnachrichten bereitgestellt werden kann. Unter [Telefonratgeber für Exchange 2013](#) finden Sie Antworten auf Ihre Fragen und die neuesten Informationen zur Konfiguration von VoIP-Gateways. Unter [Konfigurationshinweise zu unterstützten VoIP-Gateways, IP-Nebenstellenanlagen und Nebenstellenanlagen](#) finden Sie Hinweise zur VoIP-Gatewaykonfiguration und Dateien, die Sie für die Zusammenarbeit mit Exchange Unified Messaging ordnungsgemäß für die VoIP-Gateways, IP-Nebenstellenanlagen und SBCs in Ihrer Organisation konfigurieren müssen.

Das Testen der Interoperabilität von Exchange Unified Messaging mit VoIP-Gateways wurde in das Microsoft Unified Communications Open Interoperability Program integriert. Weitere Informationen hierzu finden Sie unter

## Microsoft Unified Communications Open Interoperability Program.

Das Qualifizierungsprogramm für VoIP-Gateways und IP-Nebenstellenanlagen gemäß dem [Microsoft Unified Communications Open Interoperability Program](#) gewährleistet eine nahtlose Setup- und Supporterfahrung für unsere Kunden, wenn sie geeignete Telefoniegateways und IP-Nebenstellenanlagen mit Microsoft Unified Communications-Software verwenden.

### **IMPORTANT**

Das Senden und Empfangen von Faxen mit T.38 oder G.711 wird nicht in Umgebungen unterstützt, in denen Unified Messaging und Communications Server 2007 R2 oder Microsoft Lync Server integriert sind.

## Bereitstellen und Konfigurieren von Faxfunktionen

UM leitet eingehende Faxanrufe an eine dafür vorgesehene Faxpartnerlösung weiter, die dann die Faxverbindung mit dem Faxabsender aufbaut und die Nachricht für den UM-aktivierten Benutzer empfängt. Damit UM-aktivierte Benutzer Faxnachrichten in ihrem Postfach empfangen können, müssen Sie den Faxpartnerserver konfigurieren. Anschließend müssen Sie die UM-Wählpläne und UM-Postfachrichtlinien konfigurieren sowie UM-aktivierte Benutzer für den Faxempfang aktivieren. Weitere Informationen finden Sie unter [Einrichten von eingehenden Faxen](#).

# Faxfunktion - Verfahren

18.12.2018 • 2 minutes to read

[Festlegen des Partners Faxserver URI zum Senden von Faxen zulassen](#)

[Enthalten Sie mit der e-Mail-Nachricht gesendet, wenn eine Faxnachricht empfangen wird text](#)

[Zulassen des Empfangs von Faxnachrichten für Benutzer mit demselben Wählplan](#)

[Unterbinden des Empfangs von Faxnachrichten für Benutzer mit demselben Wählplan](#)

[Aktivieren der Faxfunktion für eine Gruppe von Benutzern](#)

[Deaktivieren der Faxfunktion für eine Gruppe von Benutzern](#)

[Aktivieren eines Benutzers für den Faxempfang](#)

[Verhindert, dass Benutzer empfangen von Faxnachrichten](#)

# Festlegen des Partners Faxserver URI zum Senden von Faxen zulassen

18.12.2018 • 4 minutes to read

Sie können eingehende Faxe für Benutzer aktivieren oder deaktivieren, die einer UM-Postfachrichtlinie (Unified Messaging) zugeordnet sind. Beim Aktivieren von Benutzern für Unified Messaging können Benutzer Faxnachrichten erst empfangen, nachdem Sie den Faxeingang in der UM-Postfachrichtlinie aktiviert und den URI des Faxpartners des Partners eingegeben haben. Wenn die URIs in der UM-Postfachrichtlinie konfiguriert sind, aber die Option zum Zulassen eingehender Faxe im UM-Wählplan deaktiviert ist, können UM-aktivierte Benutzer, die der UM-Postfachrichtlinie zugeordnet sind, keine Faxnachrichten empfangen.

Weitere Informationen zu Faxpartnern finden Sie unter [Microsoft PinPoint für Faxpartner](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Faxnachrichten finden Sie unter [Faxfunktion - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Festlegen des Faxpartner-URI mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die Richtlinie, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** .
3. Klicken Sie auf der Seite **UM-Postfachrichtlinie > Allgemein, Partner Faxserver-URI**, geben Sie im TCP- oder TLS-URI. Beispiel: `sip:faxserver1.contoso.com:5060;transport=tcp` oder `sip:faxserver2.contoso.com:5061;transport=tls`

**NOTE**

Wenngleich das Feld mehrere Faxserver-URIs enthalten kann, wird nur einer verwendet. Wenn Sie zwei URIs eingeben, wird nur der erste verwendet.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

## Verwenden von Exchange Online PowerShell den faxpartner URI fest

In diesem Beispiel können Benutzer, die mit UM-Postfachrichtlinie verknüpft sind `UMDialPlan Default Policy` zur Verwendung von TCP mit Port 5060 für Partner Faxserver `faxserver1`.

```
Set-UMMailboxPolicy "UMDialPlan Default Policy" -FaxServerURI sip:faxserver1.contoso.com:5060;transport=tcp
```

In diesem Beispiel können Benutzer, die mit UM-Postfachrichtlinie verknüpft sind `UMDialPlan Default Policy` zur Verwendung von TLS mit Port 5061 für Partner Faxserver `faxserver2`.

```
Set-UMMailboxPolicy "UMDialPlan Default Policy" -FaxServerURI sip:faxserver2.contoso.com:5061;transport=tls
```

# Enthalten Sie mit der e-Mail-Nachricht gesendet, wenn eine Faxnachricht empfangen wird text

18.12.2018 • 4 minutes to read

Sie können zusätzlichen Text in die zu sendende E-Mail einschließen, wenn eine Faxnachricht von einem Benutzer empfangen wird, der für UM-Voicemail (Unified Messaging) und auch für den Faxempfang aktiviert ist, und wenn die UM-Postfachrichtlinie ordnungsgemäß für die Verwendung eines Faxpartneranbieters konfiguriert wurde. Standardmäßig gibt der Text, der verwendet wird, wenn ein UM-aktivierter Benutzer eine Faxnachricht empfängt, nur an, dass der Benutzer eine Faxnachricht empfangen hat. Sie können jedoch auch eine benutzerdefinierte Nachricht erstellen, indem Sie für eine UM-Postfachrichtlinie Text im Textfeld **Wenn ein Benutzer eine Faxnachricht empfängt** hinzufügen. Dieser Text kann z. B. Informationen zu Systemsicherheitsrichtlinien enthalten und das ordnungsgemäße Verfahren für den Umgang mit Faxnachrichten in Ihrer Organisation beschreiben. Nachdem Sie den Text hinzugefügt haben, wird er in jede E-Mail eingefügt, die gesendet wird, wenn UM-aktivierte Benutzer, die der UM-Postfachrichtlinie zugeordnet sind, eine Faxnachricht empfangen.

## NOTE

Der benutzerdefinierte Text, der mit einer Faxnachricht gesendet wird, darf maximal 512 Zeichen lang sein und kann einfache HTML-Text enthalten.

Weitere Informationen zu Faxpartnern finden Sie unter [Microsoft PinPoint für Faxpartner](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Faxnachrichten finden Sie unter [Faxfunktion - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern des in eine Faxnachricht eingebundenen Texts mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**  
[redacted]
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten** [redacted].
3. Geben Sie auf der Seite **UM-Postfachrichtlinie > Nachrichtentext** im Textfeld für **Wenn ein Benutzer für Unified Messaging aktiviert ist** den Text ein, der in der E-Mail enthalten sein soll, die beim Erhalt einer Faxnachricht im Postfach von Benutzern gesendet wird.
4. Klicken Sie auf **Speichern**.

## Verwenden Sie zum Ändern von Text in eine Faxnachricht enthaltene Exchange Online PowerShell

In diesem Beispiel wird es UM-aktivierten Benutzern, denen eine UM-Postfachrichtlinie zugeordnet ist, ermöglicht, weitere Anweisungen zum Öffnen von Faxnachrichten zu erhalten, die in ihrem Postfach eingehen.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -FaxMessageText "To open this fax message, double-click the file attachment."
```

# Zulassen des Empfangs von Faxnachrichten für Benutzer mit demselben Wählplan

18.12.2018 • 3 minutes to read

Sie können allen Benutzern, die einem Unified Messaging-Wählplan (UM) zugeordnet sind, das Empfangen von Faxnachrichten in ihren Postfächern erlauben. Standardmäßig können Benutzer, die für Unified Messaging aktiviert und einem UM-Wählplan zugeordnet sind, Faxnachrichten empfangen. Damit UM-aktivierte Benutzer Faxnachrichten in ihren Postfächern empfangen können, muss der Wählplan für das Akzeptieren eingehender Faxanrufe konfiguriert werden. Sie müssen den Faxbetrieb auch in der UM-Postfachrichtlinie und für den Benutzer aktivieren. Standardmäßig ist der Faxbetrieb für Wählpläne, UM-Postfachrichtlinien und Benutzer aktiviert. Es kann jedoch vorkommen, dass diese Standardeinstellungen geändert wurden und UM-aktivierte Benutzer keine Faxnachrichten empfangen können.

Wenn Sie das Empfangen von Faxnachrichten für einen Satz mit Wähleinstellungen deaktivieren, können alle Benutzer, die den Wähleinstellungen zugeordnet sind, keine Faxnachrichten empfangen. Dies gilt selbst dann, wenn Sie die Eigenschaften eines einzelnen Benutzers für den Empfang von Faxnachrichten konfigurieren. Das Aktivieren bzw. Deaktivieren von Faxnachrichten für einen Wählplan hat Vorrang vor den Einstellungen für den Faxbetrieb für eine UM-Postfachrichtlinie oder einen einzelnen UM-aktivierten Benutzer.

## NOTE

Der Exchange-Verwaltungskonsole können Sie für eine um-Postfachrichtlinie Fax Einstellungen konfigurieren. Allerdings müssen Sie Exchange Online PowerShell verwenden, um Fax-Einstellungen für Wählpläne oder für einzelne Benutzer zu konfigurieren.

Weitere Informationen zu Faxpartnern finden Sie unter [Microsoft PinPoint für Faxpartner](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Faxnachrichten finden Sie unter [Faxfunktion - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um Benutzern zu ermöglichen, die zu einem Wählplan Empfang von Faxen verknüpft sind

Dieses Beispiel aktiviert die UM-aktivierten Benutzer, die mit dem um-Wählplan mit dem Namen verknüpft sind `MyUMDialPlan` eingehende Faxe empfangen.

```
Set-UMDialPlan -Identity MyUMDialPlan -FaxEnabled $true
```

# Verhindern, dass Benutzer in den gleichen Wöhleinstellungen empfangen von Faxnachrichten

18.12.2018 • 3 minutes to read

Sie können verhindern, dass UM-aktivierte Benutzer, die mit einem Unified Messaging-Wählplan (UM) verknüpft sind, Faxnachrichten empfangen. Standardmäßig können Benutzer, die für Unified Messaging aktiviert und mit einem UM-Wählplan verknüpft sind, Faxnachrichten empfangen. Unter gewissen Umständen kann es jedoch notwendig sein, den Empfang von Faxnachrichten für Benutzer, die bestimmten UM-Wöhleinstellungen zugeordneten sind, zu unterbinden.

Sie können den Faxempfang für UM-aktivierte Benutzer unterbinden, indem Sie den UM-Wählplan, die UM-Postfachrichtlinie oder das Postfach des UM-aktivierten Benutzers konfigurieren. Wenn Sie die Zustellung eingehender Faxnachrichten in UM-Wöhleinstellungen deaktivieren, wird der Empfang von Faxnachrichten für alle Benutzer unterbunden, die den Wöhleinstellungen zugeordnet sind. Das Aktivieren bzw. Deaktivieren von Faxnachrichten in Wöhleinstellungen hat Vorrang vor den Einstellungen für einen einzelnen UM-aktivierten Benutzer.

## NOTE

Der Exchange-Verwaltungskonsole können Sie für eine um-Postfachrichtlinie Fax Einstellungen konfigurieren. Allerdings müssen Sie Exchange Online PowerShell verwenden, um Fax-Einstellungen für Wöhlpäne oder für einzelne Benutzer zu konfigurieren.

Weitere Informationen zu Faxpartnern finden Sie unter [Microsoft PinPoint für Faxpartner](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Faxnachrichten finden Sie unter [Faxfunktion - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wöhlpäne" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wöhleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wöhlpans](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

Verwenden von Exchange Online PowerShell verhindert, dass Benutzer, die zu einem Wöhlp plan aus empfangen von Faxnachrichten

## verknüpft sind

In diesem Beispiel wird verhindert, dass die UM-aktivierten Benutzer, die mit dem Namen der UM-Wählplan zugeordnet `MyUMDialPlan` aus empfangen von Faxnachrichten.

```
Set-UMDialPlan -Identity MyUMDialPlan -FaxEnabled $false
```

# Aktivieren von Faxen für eine Gruppe von Benutzern

18.12.2018 • 3 minutes to read

Sie können eingehende Faxe für Benutzer aktivieren, die einer Unified Messaging-Postfachrichtlinie (UM) zugeordnet sind. Beim Aktivieren von Benutzern für Unified Messaging können Benutzer Faxnachrichten standardmäßig erst empfangen, nachdem Sie den URI für den Server des Faxpartners angegeben, einen Server des Faxpartners für die Organisation bereitgestellt und den Faxbetrieb in einer UM-Postfachrichtlinie aktiviert haben. Wenn die Option zum Zulassen eingehender Faxnachrichten im UM-Wählplan deaktiviert ist, können Benutzer, die der UM-Postfachrichtlinie zugeordnet sind, keine Faxnachrichten empfangen. Wenn die Option zum Zulassen eingehender Faxnachrichten für einen einzelnen Benutzer deaktiviert ist, kann dieser Benutzer keine Faxnachrichten empfangen.

Weitere Informationen zu Faxpartnern finden Sie unter [Microsoft PinPoint für Faxpartner](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Faxnachrichten finden Sie unter [Faxfunktion - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren des Eingangs von Faxnachrichten über die Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** 
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die Postfachrichtlinie Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** 
3. Aktivieren Sie auf der Seite **UM-Postfachrichtlinie > Allgemein** das Kontrollkästchen neben **Eingehende Faxe zulassen**.

4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

## Verwenden von Exchange Online PowerShell, aktivieren Sie eingehende Faxe

In diesem Beispiel können Benutzer, die mit UM-Postfachrichtlinie verknüpft sind `MyUMMailboxPolicy` eingehende Faxe verwenden.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowFax $true
```

# Deaktivieren von Faxen für eine Gruppe von Benutzern

18.12.2018 • 3 minutes to read

Sie können eingehende Faxe für Benutzer deaktivieren, die einer UM-Postfachrichtlinie (Unified Messaging) zugeordnet sind. Beim Aktivieren von Benutzern für Unified Messaging können Benutzer Faxnachrichten erst empfangen, nachdem Sie den URI für den Server des Faxpartners angegeben, einen Server des Faxpartners für die Organisation bereitgestellt und die Faxfunktion in einer UM-Postfachrichtlinie aktiviert haben. Wenn die Option zum Zulassen eingehender Faxe im UM-Wählplan deaktiviert ist, können UM-aktivierte Benutzer, die der UM-Postfachrichtlinie zugeordnet sind, dennoch keine Faxnachrichten empfangen. Ebenso kann ein Benutzer keine Faxnachrichten empfangen, wenn die Option zum Zulassen eingehender Faxe für diesen einzelnen Benutzer deaktiviert ist.

Weitere Informationen zu Faxpartnern finden Sie unter [Microsoft PinPoint für Faxpartner](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Faxnachrichten finden Sie unter [Faxfunktion - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Deaktivieren eingehender Faxnachrichten mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die Postfachrichtlinie Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**
3. Deaktivieren Sie auf der Seite **UM-Postfachrichtlinie > Allgemein** das Kontrollkästchen **Eingehende**

**Faxe zulassen.**

4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

## Verwenden Sie Exchange Online PowerShell, um eingehende Faxe deaktivieren

In diesem Beispiel wird verhindert, dass Benutzer, die mit UM-Postfachrichtlinie verknüpft sind `MyUMMailboxPolicy` eingehende Faxe verwenden.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -AllowFax $false
```

# Aktivieren eines Benutzers für den Faxempfang

18.12.2018 • 3 minutes to read

Sie können einen Benutzer für Unified Messaging (UM) aktivieren, damit dieser Faxnachrichten empfangen kann. Wenn Sie einen Benutzer für Unified Messaging aktivieren, kann dieser standardmäßig Faxnachrichten empfangen, wenn Sie den Faxbetrieb aktivieren und einen Faxpartner-URI für die UM-Postfachrichtlinie konfigurieren, die mit dem Benutzer verknüpft ist. Die Faxfunktion kann in den UM-Wähleinstellungen, in den UM-Postfachrichtlinien oder im UM-aktivierten Benutzerpostfach aktiviert oder deaktiviert werden.

Standardmäßig lassen das Postfach des Benutzers und der Wählplan, der dem Benutzer zugeordnet ist, den Faxeingang zu. Damit ein Benutzer jedoch Faxnachrichten empfangen kann, müssen Sie zunächst den Faxeingang in der mit dem UM-aktivierten Benutzer verknüpften UM-Postfachrichtlinie aktivieren und den URI des Faxpartners eingeben.

## NOTE

Der Exchange-Verwaltungskonsole können Sie für eine um-Postfachrichtlinie Fax Einstellungen konfigurieren. Allerdings müssen Sie Exchange Online PowerShell verwenden, um Fax-Einstellungen für Wählpläne oder für einzelne Benutzer zu konfigurieren.

Weitere Informationen zu Faxpartnern finden Sie unter [Microsoft PinPoint für Faxpartner](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Faxnachrichten finden Sie unter [Faxfunktion - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Bevor Sie dieses Verfahren ausführen, vergewissern Sie sich, dass in der dem Benutzer zugewiesenen UM-Postfachrichtlinie der Faxbetrieb aktiviert und die URI des Faxpartners ordnungsgemäß konfiguriert ist.
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass der Benutzer für Unified Messaging aktiviert ist. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie zum Aktivieren eines Benutzers UM Empfang von Faxen Exchange Online PowerShell

In diesem Beispiel wird der Empfang eingehender Faxnachrichten für Tony Smith aktiviert.

```
Set-UMMailbox -Identity tonysmith@contoso.com -FaxEnabled $true
```

# Unterbinden des Faxempfangs für einen Benutzer

18.12.2018 • 3 minutes to read

Verhindern Sie, dass einen Benutzer für Unified Messaging (UM) empfangen von Faxnachrichten. Erfahren Sie, wie Sie Fax modifizieren für neue und vorhandene UM-Benutzer.

In der Standardeinstellung Wenn Sie einen Benutzer für Unified Messaging aktivieren werden sie Faxe empfangen, wenn Sie Faxen aktivieren und konfigurieren einen faxpartner URI auf die um-Postfachrichtlinie, die dem Benutzer verknüpft ist. Faxen kann aktiviert oder deaktiviert auf UM einwählen, Pläne, UM-Postfachrichtlinien oder das UM-aktivierten Postfach des Benutzers.

Standardmäßig lassen das Postfach des Benutzers und der Wählplan, der dem Benutzer zugeordnet ist, den Faxeingang zu. Damit ein Benutzer jedoch Faxnachrichten empfangen kann, müssen Sie zunächst den Faxeingang in der mit dem UM-aktivierten Benutzer verknüpften UM-Postfachrichtlinie aktivieren und den URI des Faxpartners eingeben.

## NOTE

Der Exchange-Verwaltungskonsole können Sie um Fax-Einstellungen für eine Unified Messaging-Postfachrichtlinie zu konfigurieren. Allerdings müssen Sie Exchange Online PowerShell verwenden, um Fax-Einstellungen für Wählpläne oder für einzelne Benutzer zu konfigurieren.

Weitere Informationen zu Faxpartnern finden Sie unter [Microsoft PinPoint für Faxpartner](#).

Informationen zu weiteren Verwaltungsaufgaben in Bezug auf Faxnachrichten finden Sie unter [Faxfunktion - Verfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 2 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass der Benutzer für Unified Messaging aktiviert ist. Ausführliche Anleitungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um zu verhindern, dass einen UM-aktivierten Benutzer empfangen von Faxnachrichten

In diesem Beispiel wird verhindert, dass der UM-aktivierte Benutzer Tony über sein Postfach Faxnachrichten empfangen kann.

```
Set-UMMailbox -Identity tony@contoso.com -FaxEnabled $false
```

# Festlegen von Outlook Voice Access-PIN-Sicherheit

18.12.2018 • 10 minutes to read

Wenn Unified Messaging-Benutzer (UM) sich per Telefon mit dem Voicemailsysteem verbinden, nutzen sie für die Navigation durch das Menüsystem Outlook Voice Access. Bevor Benutzer jedoch auf das Voicemailsysteem zugreifen können, werden sie vom System zur Eingabe ihrer PIN aufgefordert. Als Administrator können Sie PIN-Einstellungen und -Vorgaben konfigurieren sowie PIN-Verwaltungsaufgaben durchführen. Nachdem ein Benutzer für Voicemail aktiviert und eine PIN für ihn generiert wurde, wird diese PIN verschlüsselt im Postfach des Benutzers gespeichert.

## NOTE

Zum Eingeben der PIN für den Zugriff auf ein UM-aktiviertes Postfach müssen Outlook Voice Access-Benutzer ein Tastaturwahl- oder DTMF-Telefon (Dual-Tone Multi-Frequency) verwenden. Die Spracherkennung ist für die PIN-Eingabe nicht verfügbar.

## PIN-Übersicht

Eine PIN ist eine numerische Zeichenfolge, die in bestimmten Systemen verwendet wird, damit ein Benutzer authentifiziert werden kann und Zugriff erhält. PINs werden am häufigsten für Geldautomaten verwendet. PINs werden auch für Voicemailsysteme anstelle alphanumerischer Kennwörter verwendet. Die Sicherheit einer PIN hängt von ihrer Länge, von der Stufe des Schutzes sowie davon ab, wie schwer sie zu erraten ist.

In Unified Messaging geben Outlook Voice Access-Benutzer ihre PIN über ein analoges, digitales oder Mobiltelefon ein, damit sie in ihrem Exchange Server-Postfach auf E-Mail-, Voicemail-, Kontakt- und Kalenderinformationen zugreifen können.

In Unified Messaging werden PIN-Richtlinien in einer UM-Postfachrichtlinie festgelegt und konfiguriert. Je nach Ihren Anforderungen können Sie mehrere UM-Postfachrichtlinien erstellen. Wenn Sie einen Benutzer für Voicemail aktivieren, verknüpfen Sie den Benutzer mit einer vorhandenen UM-Postfachrichtlinie. Die UM-PIN-Richtlinien, die in der UM-Postfachrichtlinie konfiguriert werden, müssen auf den Sicherheitsanforderungen Ihrer Organisation basieren.

## PIN-Vorgaben

Es folgen verschiedene PIN-Konfigurationseinstellungen, die Sie für eine UM-Postfachrichtlinie festlegen können.

### Minimale PIN-Länge

Die Einstellung **Minimale PIN-Länge** gibt die Mindestanzahl der Stellen an, die eine Postfach-PIN aufweisen muss. Der Wertebereich ist 4 bis 24, die Standardeinstellung lautet 6. Bei Eingabe von 0 werden die Benutzer nicht zur Eingabe einer PIN aufgefordert.

## IMPORTANT

Das Konfigurieren dieser Einstellung mit Null wird nicht empfohlen. Wenn Sie die Einstellung mit Null konfigurieren, verringern Sie die Sicherheitsstufe Ihres Netzwerk erheblich.

Wenn Sie die minimale PIN-Länge in einen höheren Wert ändern, werden derzeitige Outlook Voice Access-Benutzer aufgefordert, eine neue PIN mit der neuen Mindestanzahl von Stellen einzugeben, bevor sie fortfahren

können.

#### NOTE

Durch das Erhöhen dieses Werts wird die Sicherheit der UM-Umgebung gesteigert. Ein zu hoher Wert kann allerdings dazu führen, dass die Benutzer ihre PIN vergessen.

### **PIN-Gültigkeitsdauer (Tage) erzwingen**

Die Einstellung **PIN-Gültigkeitsdauer (Tage) erzwingen** bestimmt den Zeitraum in Tagen ab dem Datum, an dem ein Outlook Voice Access-Benutzer seine PIN zuletzt geändert hat, bis zum Datum, an dem er gezwungen wird, diese erneut zu ändern. Der Wertebereich ist 0 bis 999, der Standardwert lautet 60 Tage. Bei Eingabe von 0 läuft die PIN nicht ab.

#### NOTE

Unified Messaging benachrichtigt Benutzer nicht, wenn ihre PIN in Kürze abläuft.

### **Anzahl der Anmeldefehler vor dem Zurücksetzen der PIN**

Die **Anzahl der Anmeldefehler vor dem Zurücksetzen der PIN** gibt die Anzahl der aufeinander folgenden erfolglosen Anmeldeversuche an, bevor die Postfach-PIN automatisch zurückgesetzt wird. Um diese Einstellung zu deaktivieren, legen Sie sie auf Unbegrenzt fest. Andernfalls muss der Wert dieser Einstellung niedriger als der Wert der Einstellung **Anzahl der Anmeldefehler vor dem Sperren** sein. Der Wertebereich ist 1 bis 998, der Standardwert lautet 5.

#### NOTE

Um die Sicherheit für UM-aktivierte Benutzer zu erhöhen, geben Sie einen Wert unter 5 ein.

### **Anzahl der Anmeldefehler vor dem Sperren**

Die Einstellung **Anzahl der Anmeldefehler vor dem Sperren** gibt an, wie viele PIN-Eingabefehler Outlook Voice Access-Benutzer bei aufeinander folgenden Anrufen begehen dürfen, ehe der Zugriff auf ihr Postfach gesperrt wird. Nach 5 Versuchen wird die PIN standardmäßig automatisch zurückgesetzt. Der Wertebereich ist 1 bis 999, der Standardwert lautet 15.

#### NOTE

Verringern Sie zum Erhöhen der Sicherheit die zulässige Anzahl der Fehlversuche. Bei Festlegung auf einen Wert, der wesentlich kleiner als der Standardwert ist, werden Benutzer jedoch ggf. unnötigerweise am Zugriff gehindert. Unified Messaging generiert Warnereignisse, die mithilfe der Ereignisanzeige angezeigt werden können, wenn ein Fehler bei der PIN-Authentifizierung für einen UM-aktivierten Benutzer auftritt oder der Anmeldeversuch des Benutzers am System nicht erfolgreich ist.

### **Gängige PIN-Muster zulassen**

Die Einstellung **Gängige Muster in PIN zulassen** dient zum Aktivieren oder Deaktivieren der Verwendung gängiger Muster bei der PIN-Erstellung. Diese Einstellung ist standardmäßig deaktiviert und hindert Benutzer von Outlook Voice Access an der Eingabe der folgenden Muster:

- **Fortlaufende Zahlen:** PIN-Werte, die vollständig aus aufeinander folgenden Zahlen bestehen. Beispiele für sequenzielle Zahlen für eine PIN sind 1234 und 65432.
- **Wiederholte Zahlen:** PIN-Werte, die aus bestehen wiederholt Zahlen. Beispiele für wiederholte Zahlen sind 11111 und 22222.

- **Suffix des Postfachdurchwahl:** PIN-Werte, die das Suffix eines Benutzers Postfachdurchwahl bestehen.

Wenn die Postfachdurchwahl 36697 ist, kann nicht die PIN 6697 sein.

## Anzahl der PIN-Wiederverwendungen

Die Einstellung **Anzahl der PIN-Wiederverwendungen** legt die Anzahl der unterschiedlichen PINs fest, die ein Benutzer verwenden muss, bevor zuvor verwendete PINs erneut verwendet werden dürfen. Der Wertebereich ist 1 bis 20, der Standardwert lautet 5.

## Verwalten von Outlook Voice Access-PINs

Bei der Planung von Outlook Voice Access-PINs müssen Sie die geeigneten Sicherheitsstufen für Ihre Organisation wählen. Sie müssen die Outlook Voice Access-PIN-Vorgaben sorgfältig untersuchen und prüfen, ob Ihre PIN-Sicherheitseinstellungen die Sicherheitsanforderungen Ihrer Organisation erfüllen bzw. übererfüllen.

### IMPORTANT

Aus Sicherheitsgründen empfiehlt es sich, strenge PIN-Anforderungen für Outlook Voice Access-Benutzer zu implementieren. Dazu empfiehlt sich das Erstellen von Unified Messaging-PIN-Richtlinien, die mindestens sechs Stellen für PINs vorsehen und die Sicherheitsstufe des Netzwerks erhöhen.

Nachdem Sie die Outlook Voice Access-PIN-Vorgaben festgelegt haben, müssen Sie eine UM-Postfachrichtlinie erstellen und konfigurieren, um die PIN-Vorgaben der Organisation durchzusetzen. Details zum Erstellen einer UM-Postfachrichtlinie finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#). Weitere Informationen zum Verwalten von UM-Postfachrichtlinien finden Sie unter [Verwalten einer UM-Postfachrichtlinie](#).

### NOTE

Nachdem Sie die um-Postfachrichtlinie erstellt haben, müssen Sie die UM-aktivierten Benutzer oder Benutzer mit der entsprechenden UM-Postfachrichtlinie verknüpfen. Dies ist das Cmdlet **Enable-UMMailbox** in Exchange Online PowerShell oder mithilfe der Exchange-Verwaltungskonsole (EAC) möglich. Weitere Informationen zu Exchange Online PowerShell-Cmdlet finden Sie unter [Enable-UMMailbox](#).

Es gibt Situationen, in denen Outlook Voice Access-Benutzer ihre PIN vergessen oder ihr Voicemailzugriff gesperrt wird. In beiden Fällen müssen Sie ggf. die PIN eines UM-aktivierten Benutzers zurücksetzen. Weitere Informationen finden Sie unter [Zurücksetzen einer Voicemail-PIN](#).

Sie können PIN-Informationen für einen Benutzer abrufen, der für Unified Messaging (UM) aktiviert ist. Die zurückgegebenen Informationen werden mithilfe der verschlüsselten PIN-Daten berechnet, die im Postfach des Benutzers gespeichert sind. So können Sie PIN-Informationen für den Benutzer anzeigen. Außerdem wird angegeben, ob der Benutzer für sein Postfach gesperrt wurde. Weitere Informationen finden Sie unter [Abrufen von PIN-Informationen für Voicemail](#).

# PIN-Sicherheit – Verfahren

18.12.2018 • 2 minutes to read

Festlegen von Outlook Voice Access-PIN-Richtlinien

Zurücksetzen einer Voicemail-PIN

Abrufen von PIN-Informationen für Voicemail

Enthalten Sie mit der e-Mail-Nachricht gesendet, wenn ein Zurücksetzen PIN-Nummer ist text

Legen Sie die PIN-Mindestlänge für Voicemail

Legen Sie die PIN-Gültigkeitsdauer für Voicemail

Festlegen Sie die Anzahl der vorherigen Voicemail PINs Recycling

Deaktivieren Sie gängige PIN Muster für Voicemail

Aktivieren Sie für Voicemail-gängiger PIN-Muster

Festlegen Sie die Anzahl der Anmeldung Fehler vor einer Voicemail, die PIN zurücksetzen,

Festlegen Sie die Zahl der ungünstigen-Anmeldung, bevor ein Voice Mail-Benutzer gesperrt ist

# Festlegen von Outlook Voice Access-PIN-Richtlinien

18.12.2018 • 4 minutes to read

Sie können PIN-Richtlinien für eine Unified Messaging-Postfachrichtlinie (UM) festlegen. UM-Postfachrichtlinien können konfiguriert werden, um die Sicherheitsstufe für UM-aktivierte Benutzer zu erhöhen, die Outlook Voice Access verwenden, indem von Benutzern verlangt wird, dass sie die vordefinierten PIN-Richtlinien für Ihre Organisation einhalten.

Wenn Sie PIN-Richtlinien für Outlook Voice Access-Benutzer festlegen möchten, können Sie entweder eine neue UM-Postfachrichtlinie erstellen oder eine vorhandene UM-Postfachrichtlinie ändern. Nach dem Erstellen einer neuen UM-Postfachrichtlinie können Sie die UM-Postfachrichtlinie konfigurieren, indem Sie die folgenden PIN-Einstellungen konfigurieren:

- `MinPasswordLength`
- `PINLifetime`
- `LogonFailuresBeforePINReset`
- `MaxLogonAttempts`
- `AllowCommonPatterns`
- `PINHistoryCount`

Aus Sicherheitsgründen empfiehlt es sich, strenge PIN-Anforderungen für UM-Benutzer zu implementieren. Dies wird erreicht, indem Sie UM-PIN-Richtlinien erstellen, die PINs mit 6 oder mehr Stellen erfordern und den Grad an Sicherheit für das Netzwerk erhöhen.

Wenn Sie die PIN-Richtlinie ändern, wird die neue PIN-Einstellung auf die Benutzer angewendet, die zurzeit der UM-Postfachrichtlinie zugeordnet sind. Wenn Sie z. B. die UM-Postfachrichtlinie ändern und die PIN-Mindestlänge von 7 auf 10 Stellen erhöhen, werden Benutzer bei ihrer nächsten Anmeldung gezwungen, ihre PIN zu ändern, um der geänderten PIN-Anforderung zu genügen.

Informationen zu weiteren Aufgaben im Zusammenhang mit der Outlook Voice Access-PIN-Sicherheit finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

#### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Festlegen von PIN-Richtlinien für Outlook Voice Access-Benutzer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, klicken Sie auf dem um-Wählplan, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf der Seite **UM-Postfachrichtlinie** auf **PIN-Richtlinien**.
5. Konfigurieren Sie auf der Seite **PIN-Richtlinien** die PIN-Einstellungen für Outlook Voice Access-Benutzer, die einer UM-Postfachrichtlinie zugeordnet sind, und klicken Sie dann auf **Speichern**.

## Verwenden von Exchange Online PowerShell zum Festlegen von PIN-Richtlinien für Outlook Voice Access-Benutzer

In diesem Beispiel wird die PIN-Einstellungen für Benutzer, die um-Postfachrichtlinie zugeordnet

`MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 8 -MaxLogonAttempts 12 -MinPINLength 8 -PINHistoryCount 10 -PINLifetime 60 -ResetPINText "The PIN used to allow you access to your mailbox using Outlook Voice Access has been reset."
```

# Zurücksetzen einer Voicemail-PIN

18.12.2018 • 6 minutes to read

Wenn ein UM-aktivierter (Unified Messaging) Voicemailbenutzer sein Postfach durch mehrfache Anmeldeversuche bei Outlook Voice Access mit einer falschen PIN gesperrt oder seine PIN vergessen hat, kann seine PIN mithilfe eines der folgenden Verfahren zurückgesetzt werden. Beim Zurücksetzen der Outlook Voice Access-PIN eines Benutzers können Sie Unified Messaging für die automatische PIN-Generierung konfigurieren oder die PIN manuell angeben. Die neue PIN wird per E-Mail an den Benutzer gesendet. Sie können weitere PIN-Optionen angeben, z. B. den Benutzer auffordern, bei der ersten Anmeldung seine PIN zurückzusetzen. Benutzer können außerdem ihre UM-PIN mithilfe von Outlook oder Outlook Web App zurücksetzen.

## NOTE

Für den Zugriff auf UM-aktivierte Postfächer müssen Outlook Voice Access-Benutzer mit Tastaturwahl- bzw. DTMF-Eingaben (Dual Tone Multi-Frequency) arbeiten. Die Spracherkennung ist für die PIN-Eingabe nicht verfügbar.

Informationen zu weiteren Aufgaben im Zusammenhang mit der Outlook Voice Access-PIN-Sicherheit finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Zurücksetzen einer Unified Messaging-PIN mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger**. Wählen Sie in der Listenansicht das Benutzerpostfach aus, das angezeigt werden soll.
2. Klicken Sie im Detailbereich unter **Telefon- und Sprachfunktionen** unter **Unified Messaging** auf **Details anzeigen**.
3. Klicken Sie auf der Seite **UM-Postfach** auf **UM-Postfacheinstellungen** und dann auf **PIN zurücksetzen**.
4. Wählen Sie auf der Seite **UM-Postfach-PIN zurücksetzen** die folgenden Optionen, um die PIN des UM-aktivierten Benutzers zurückzusetzen:

- **Eine PIN automatisch generieren:** mit dieser Option können Sie automatisch die PIN generieren, die vom Benutzer verwendet wird, um auf ihr Postfach mithilfe von Outlook Voice Access zuzugreifen. Diese Einstellung ist standardmäßig aktiviert.

Die automatisch generierte PIN wird in einer E-Mail-Nachricht an das Postfach des Benutzers gesendet. Nachdem der Benutzer die PIN erhalten und sich an seinem Postfach angemeldet hat, wird er aufgefordert, die PIN in eine leichter zu merkende PIN zu ändern.

Outlook Web App und Microsoft Outlook ermöglichen Benutzern ebenfalls das Zurücksetzen der PIN. Die PIN wird automatisch auf Basis der PIN-Richtlinien generiert, die für die UM-Postfachrichtlinie konfiguriert sind, die dem Postfach des Benutzers zugeordnet ist. Es wird empfohlen, die PINs für Outlook Voice Access-Benutzer automatisch zu generieren.

- **Eine PIN eingeben:** mit dieser Option können Sie eine PIN für eine Outlook Voice Access-Benutzer manuell angeben. Diese Einstellung ist standardmäßig deaktiviert.

Wenn Sie eine PIN für einen Benutzer angeben, wird die PIN in einer E-Mail-Nachricht an das Postfach des Benutzers gesendet. Nachdem er die PIN erhalten und sich beim Postfach angemeldet hat, kann er die PIN durch Konfigurieren persönlicher Optionen in Outlook Voice Access ändern. In Outlook Web App und Microsoft Outlook ist jedoch keine Option für die manuelle Angabe einer PIN verfügbar.

- **Muss der Benutzer ihre PIN-Nummer der ersten Anmeldung zurückzusetzen:** mit dieser Option können Sie, dass der Benutzer ihre PIN zurückgesetzt, wenn sie sich zuerst bei Outlook Voice Access anmelden. Diese Option ist standardmäßig aktiviert.

Wenn Sie die Option zum automatischen Generieren einer PIN für einen Benutzer aktivieren, können Sie mithilfe dieser Option anfordern, dass der Benutzer seine PIN beim erstmaligen Anmelden bei Outlook Voice Access ändert. Dies erhöht die Sicherheit für die Benutzer-PIN.

5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell einen Unified Messaging-PIN zurücksetzen

In diesem Beispiel wird die Voicemail-PIN für Tony Smith auf 1985848 zurückgesetzt. Diese PIN muss jedoch beim erstmaligen Anmelden des Benutzers bei Outlook Voice Access geändert werden.

```
Set-UMMailboxPIN -Identity tonysmith@contoso.com -PIN 1985848 -PinExpired $true
```

# Abrufen von PIN-Informationen für Voicemail

18.12.2018 • 3 minutes to read

Sie können PIN-Informationen für einen Benutzer abrufen, der für Unified Messaging (UM) aktiviert ist.

Nachdem ein Benutzer für UM aktiviert wurde und eine PIN generiert oder erstellt wurde, wird die PIN verschlüsselt und im Postfach des Benutzers gespeichert.

Wenn Sie PIN-Informationen für einen UM-aktivierten Benutzer abrufen, werden die Informationen, die an Sie zurückgegeben werden, mithilfe der verschlüsselten PIN-Daten im Postfach des Benutzers berechnet. Mit diesem Task können Sie Informationen aus dem Postfach des Benutzers anzeigen. Er gibt außerdem an, ob der Benutzer für sein Postfach gesperrt wurde.

Weitere Aufgaben im Zusammenhang mit PIN-Sicherheit finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Wählpläne" im Thema [Unified Messaging Permissions](#).
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfächer" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass das Postfach des Benutzers UM-aktiviert wurde. Genaue Anweisungen finden Sie unter [Aktivieren eines Benutzers für Voicemail](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Abrufen von PIN-Informationen für einen UM-aktivierten Benutzer

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger**. Wählen Sie in der Listenansicht das Benutzerpostfach aus, das angezeigt werden soll.
2. Klicken Sie im Detailbereich unter **Telefon- und Sprachfunktionen** auf **Details anzeigen**.
3. Lassen Sie auf der Seite **UM-Postfach > UM-Postfacheinstellungen** den **PIN-Status** für den Benutzer

anzeigen. Auf dieser Seite können Sie außerdem die Voicemail-PIN für den Benutzer zurücksetzen.

## Verwenden von Exchange Online PowerShell zum Abrufen von PIN-Informationen für einen UM-aktivierten Benutzer

In diesem Beispiel wird die Benutzer-ID angezeigt sowie die Information, ob eine PIN abgelaufen ist, ob das UM-Postfach gesperrt wurde und ob Thorsten zum ersten Mal als Benutzer auftritt.

```
Get-UMMailboxPIN -identity tony@contoso.com
```

# Enthalten Sie mit der e-Mail-Nachricht gesendet, wenn ein Zurücksetzen PIN-Nummer ist text

18.12.2018 • 4 minutes to read

Sie können zusätzlichen Text in die E-Mail-Nachricht aufnehmen, die Benutzer erhalten, wenn ihre UM (Unified Messaging)- oder Voicemail-PIN zurückgesetzt wird. Geben Sie dazu in einer UM-Postfachrichtlinie in das Feld **Wenn die Outlook Voice Access-PIN eines Benutzers zurückgesetzt wird** benutzerdefinierten Text ein. Der benutzerdefinierte Text kann z. B. sicherheitsrelevante Informationen für UM-aktivierte Benutzer enthalten.

Eine für Outlook Voice Access verwendete PIN wird vom Unified Messaging- oder Voicemailsyste standardmäßig nach 5 fehlgeschlagenen Anmeldeversuchen zurückgesetzt. Benutzer können ihre PINs auch über die UM-Funktionen in Outlook Web App bzw. Outlook 2010 oder höher oder von einem Telefon aus über Outlook Voice Access zurücksetzen.

## NOTE

Die Texteingabe in das Feld ist auf 512 Zeichen beschränkt und kann einfachen HTML-Text umfassen.

Weitere Aufgaben im Zusammenhang mit der Sicherheit von Outlook Voice Access-PINs finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Hinzufügen von Text zur E-Mail-Nachricht, die Benutzer erhalten, wenn ihre PIN zurückgesetzt wird, mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-  
Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf **Bearbeiten**
3. Geben Sie auf der Seite **UM-Postfachrichtlinie > Nachrichtentext** in das Textfeld für **Wenn die  
Outlook Voice Access-PIN eines Benutzers zurückgesetzt wird** den Text ein, der in die E-Mail  
aufgenommen werden soll, die Benutzern beim Zurücksetzen ihrer PIN zugesendet wird.
4. Klicken Sie auf **Speichern**.

Verwenden von Exchange Online PowerShell zum Hinzufügen von Text  
in der e-Mail-Nachricht an Benutzer gesendet werden, wenn seine PIN  
zurückgesetzt wird

In diesem Beispiel enthält die weiteren Text umfasst, die "Ihre PIN nicht für andere Benutzer freigeben.  
Möglicherweise Disziplinarmaßnahmen, in der e-Mail-Nachricht führen"an Benutzer gesendet, die UM-  
Postfachrichtlinie zugeordnet sind  wenn seine PIN zurückgesetzt wird.

```
Set-UMMailboxPolicy -identity MyUMMailboxPolicy -ResetPINText "Do not share your PIN with other users. Doing  
so may result in disciplinary action."
```

# Legen Sie die PIN-Mindestlänge für Voicemail

18.12.2018 • 4 minutes to read

Sie können die minimale PIN-Länge für Ihre Outlook Voice Access-Benutzer konfigurieren, die für Unified Messaging (UM) aktiviert sind. Die PIN-Einstellungen, die Sie für eine UM-Postfachrichtlinie konfigurieren, gelten für alle UM-aktivierten Benutzer, die der UM-Postfachrichtlinie zugeordnet sind.

Mithilfe von Outlook Voice Access können UM-aktivierte Benutzer auf die Voicemail-, E-Mail-, Kalender- und persönlichen Kontaktinformationen in ihrem Postfach zugreifen. Bevor sie auf ihr Postfach zugreifen können, müssen sie jedoch eine PIN eingeben, damit sie vom Voicemailsysteem authentifiziert werden können.

## NOTE

Wenn Sie die minimale PIN-Länge ändern, werden vorhandene Outlook Voice Access-Benutzer aufgefordert, eine neue PIN mit der neuen Mindestanzahl von Stellen einzugeben, bevor sie fortfahren können. Der Standardwert ist 6.

Informationen zu weiteren Aufgaben im Zusammenhang mit der Outlook Voice Access-PIN-Sicherheit finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der minimalen PIN-Länge für Outlook Voice Access mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. Klicken Sie in der Listenansicht auswählen die Wähleinstellungen, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

4. Klicken Sie auf **PIN-Richtlinien**, und geben Sie neben **PIN-Mindestlänge** einen Wert von 4 bis 24 ein.

5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell zum Konfigurieren der PIN-Mindestlänge für Outlook Voice Access

In diesem Beispiel wird die minimale PIN-Länge von 8 Stellen für Outlook Voice Access-Benutzer, die mit dem Namen der UM-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -MinPINLength 8
```

In diesem Beispiel legt die minimale PIN-Länge 8 Ziffern und die Anzahl der Häufigkeit, mit die einer Anmeldung ausgeführt werden kann, bevor der Benutzer PIN auf 3 zurückgesetzt wird. Dies gilt für UM-aktivierten Benutzer, die mit dem Namen der UM-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 3 -MinPINLength 8
```

# Legen Sie die PIN-Gültigkeitsdauer für Voicemail

18.12.2018 • 4 minutes to read

Sie können die PIN-Gültigkeitsdauer für UM-aktivierte (Unified Messaging) Benutzer konfigurieren. Die PIN-Gültigkeitsdauer ist der maximale Zeitraum, den eine Outlook Voice Access-PIN für UM-aktivierte Empfänger gültig ist. Die PIN-Gültigkeitsdauereinstellung wird für eine UM-Postfachrichtlinie konfiguriert und gilt für alle UM-aktivierten Benutzer, die der UM-Postfachrichtlinie zugeordnet sind.

Für eine UM-Postfachrichtlinie können mehrere PIN-bezogene Einstellungen konfiguriert werden. Die PIN-Gültigkeitsdauer bestimmt den Zeitraum in Tagen ab dem Datum, an dem ein Outlook Voice Access-Benutzer seine PIN zuletzt geändert hat, bis zum Datum, an dem er gezwungen wird, diese erneut zu ändern. Der Wertebereich ist 0 bis 999, der Standardwert 60 Tage. Bei Eingabe von 0 läuft die PIN nicht ab. Diese Einstellung sollte nicht auf 0 festgelegt werden, da dadurch die Sicherheit Ihres Netzwerks stark gefährdet wird.

## IMPORTANT

Unified Messaging benachrichtigt Benutzer nicht, wenn ihre PIN in Kürze abläuft.

Informationen zu weiteren Aufgaben im Zusammenhang mit der Outlook Voice Access-PIN-Sicherheit finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der PIN-Gültigkeitsdauer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

3. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie auf **PIN-Richtlinien**, und geben Sie neben **PIN-Gültigkeitsdauer (Tage) erzwingen** einen Wert von 0 bis 999 ein.
5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell so konfigurieren Sie die PIN-Lebensdauer

In diesem Beispiel wird die Anzahl der Tage, die eine PIN für Outlook Voice Access-Benutzer verwendet werden können, die mit dem Namen einer UM-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy` auf 30.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -PINLifetime 30
```

Das folgende Beispiel konfiguriert die folgenden PIN-bezogene Einstellungen für Outlook Voice Access-Benutzer, die mit dem Namen einer UM-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy`:

- Legt die Anzahl von Anmeldefehlern vor dem Zurücksetzen der Benutzer-PIN auf 3 fest.
- Legt die maximale Anzahl von Anmeldeversuchen auf 5 fest.
- Legt die minimale PIN-Länge auf 9 Ziffern fest.
- Legt eine PIN-Gültigkeitsdauer von 40 Tagen fest.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 3  
-MaxLogonAttempts 5 -MinPINLength 9 -PINLifetime 40
```

# Festlegen Sie die Anzahl der vorherigen Voicemail PINs Recycling

18.12.2018 • 4 minutes to read

Wenn sich Benutzer von Outlook Voice Access bei einer Outlook Voice Access-Nummer einwählen, werden sie aufgefordert, ihre PIN einzugeben, damit das Voicemailsysteem sie authentifizieren kann. Nachdem sie authentifiziert wurden, können sie auf die Voicemail-, E-Mail-, Kalender- und persönlichen Kontaktinformationen in ihrem jeweiligen Postfach über jedes beliebige Telefon zugreifen.

Für eine UM-Postfachrichtlinie (Unified Messaging) können mehrere PIN-bezogene Einstellungen konfiguriert werden. Verwenden Sie die Einstellung **Anzahl der PIN-Wiederverwendungen**, um die Anzahl der eindeutigen PINs festzulegen, die Benutzer verwenden müssen, bevor eine alte PIN erneut verwendet werden darf. Sie können diese Einstellung auf einen Wert von 1 bis 20 festlegen. In den meisten Organisationen sollte dieser Wert auf die Standardeinstellung (fünf PINs) festgelegt werden. Wenn Sie diesen Wert zu hoch festlegen, kann dies die Benutzer verärgern, weil sie zu häufig neue PINs erstellen und sich merken müssen. Wird er zu niedrig festgelegt, kann dies eine Sicherheitsbedrohung für Ihr Netzwerk bedeuten.

## IMPORTANT

Die Anzahl der PIN-Wiederverwendungen kann nicht deaktiviert werden.

Informationen zu weiteren Aufgaben im Zusammenhang mit der Outlook Voice Access-PIN-Sicherheit finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Ändern der Anzahl der PIN-Wiederverwendungen mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. Klicken Sie in der Listenansicht auswählen die Wähleinstellungen, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** [ ] .
3. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um- Postfachrichtlinie Sie ändern möchten, und klicken Sie dann auf **Bearbeiten** [ ].
4. Klicken Sie auf **PIN-Richtlinien**, und geben Sie neben **Anzahl der PIN-Wiederverwendungen** einen Wert von 1 bis 20 ein.
5. Klicken Sie auf **Speichern**.

## Verwenden Sie zum Ändern der Anzahl der PIN Recycle Exchange Online PowerShell

In diesem Beispiel wird die Anzahl der PIN Recycle auf die um-Postfachrichtlinie **MyUMMailboxPolicy** bis 10.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -PINHistoryCount 10
```

# Deaktivieren Sie gängige PIN Muster für Voicemail

18.12.2018 • 4 minutes to read

Sie können gängige UM-PIN-Muster (Unified Messaging) für Outlook Voice Access-Benutzer aktivieren oder deaktivieren. Wenn Sie die Einstellung gängiger PIN-Muster für eine UM-Postfachrichtlinie aktivieren oder deaktivieren, gilt die Einstellung für alle UM-aktivierten Benutzer, die der UM-Postfachrichtlinie zugeordnet sind. Standardmäßig können UM-aktivierte Benutzer beim Erstellen einer PIN keine gängigen Muster verwenden.

Sie können mehrere PIN-bezogene Einstellungen für eine UM-Postfachrichtlinie konfigurieren. Die Einstellung **Gängige PIN-Muster zulassen** dient zum Aktivieren oder Deaktivieren der Verwendung gängiger Muster bei der PIN-Erstellung. Diese Einstellung ist standardmäßig deaktiviert und hindert Benutzer an der Verwendung der folgenden Zahlenmuster:

- **Fortlaufende Zahlen:** Diese PIN-Werte, die nur aufeinander folgende Zahlen enthalten sind. Beispiele für fortlaufende Nummern für eine PIN sind 1234 und 65432.
- **Wiederholte Zahlen:** Diese PIN-Werte, die nur wiederholte Zahlen enthalten sind. Beispiele für wiederholte Zahlen sind 11111 und 22222.
- **Suffix des Postfachdurchwahl:** Diese PIN-Werte, die das Suffix des Postfachdurchwahl eines Benutzers enthalten sind. Beispielsweise ist ein Benutzer Postfachdurchwahl 36697, PIN des Benutzers 3669712 nicht möglich.

## NOTE

Wenn die Einstellung **Gängige PIN-Muster zulassen** aktiviert ist, wird nur das Suffix der Postfachdurchwahl zurückgewiesen.

Weitere Aufgaben im Zusammenhang mit der Sicherheit von Outlook Voice Access-PINs finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Deaktivieren gängiger PIN-Muster

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf der Symbolleiste auf **Bearbeiten** 
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf der Symbolleiste auf **Bearbeiten** 
3. Deaktivieren Sie auf der Seite **UM-Postfachrichtlinie** unter **PIN-Richtlinien** das Kontrollkästchen neben **Gängige PIN-Muster zulassen**.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell gängiger Muster der PIN deaktivieren

In diesem Beispiel wird verhindert, dass Benutzer mit dem Namen der UM-Postfachrichtlinie zugeordnet **MyUMMailboxPolicy** aus mithilfe von PINs, die gängiger Muster enthalten.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowCommonPatterns $false
```

# Aktivieren Sie für Voicemail-gängiger PIN-Muster

18.12.2018 • 4 minutes to read

Sie können gängige UM-PIN-Muster (Unified Messaging) für Outlook Voice Access-Benutzer aktivieren oder deaktivieren. Wenn Sie die Einstellung gängiger PIN-Muster für eine UM-Postfachrichtlinie aktivieren oder deaktivieren, gilt die Einstellung für alle UM-aktivierten Benutzer, die der UM-Postfachrichtlinie zugeordnet sind. Standardmäßig können UM-aktivierte Benutzer beim Erstellen einer PIN keine gängigen Muster verwenden.

Sie können mehrere PIN-bezogene Einstellungen für eine UM-Postfachrichtlinie konfigurieren. Die Einstellung **Gängige PIN-Muster zulassen** dient zum Aktivieren oder Deaktivieren der Verwendung gängiger Muster bei der PIN-Erstellung. Diese Einstellung ist standardmäßig deaktiviert und hindert Benutzer an der Verwendung der folgenden Zahlenmuster:

- **Fortlaufende Zahlen:** Diese PIN-Werte, die nur aufeinander folgende Zahlen enthalten sind. Beispiele für fortlaufende Nummern für eine PIN sind 1234 und 65432.
- **Wiederholte Zahlen:** Diese PIN-Werte, die nur wiederholte Zahlen enthalten sind. Beispiele für wiederholte Zahlen sind 11111 und 22222.
- **Suffix des Postfachdurchwahl:** Diese PIN-Werte, die das Suffix des Postfachdurchwahl eines Benutzers enthalten sind. Beispielsweise ist ein Benutzer Postfachdurchwahl 36697, PIN des Benutzers 3669712 nicht möglich.

## NOTE

Wenn die Einstellung **Gängige PIN-Muster zulassen** aktiviert ist, wird nur das Suffix der Postfachdurchwahl zurückgewiesen.

Weitere Aufgaben im Zusammenhang mit der Sicherheit von Outlook Voice Access-PINs finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

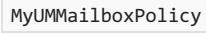
## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Aktivieren gängiger PIN-Muster

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf der Symbolleiste auf **Bearbeiten** 
2. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie, die Sie verwalten möchten, und klicken Sie dann auf der Symbolleiste auf **Bearbeiten** 
3. Aktivieren Sie auf der Seite **UM-Postfachrichtlinie** unter **PIN-Richtlinien** das Kontrollkästchen neben **Gängige PIN-Muster zulassen**.
4. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell, gängiger Muster der PIN aktivieren

In diesem Beispiel können Benutzer mit dem Namen der UM-Postfachrichtlinie zugeordnet  PINs verwenden, die gängiger Muster enthalten.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -AllowCommonPatterns $true
```

# Festlegen Sie die Anzahl der Anmeldung Fehler vor einer Voicemail, die PIN zurücksetzen,

18.12.2018 • 4 minutes to read

Sie können konfigurieren, welche Anzahl von Anmeldefehlern vor dem Zurücksetzen der PIN für einen Outlook Voice Access-Benutzer zulässig ist. Die möglichen Werte liegen in einem Bereich von 1 bis 998, der Standardwert ist 5. Die maximal zulässige Anzahl von fehlerhaften Anmeldeversuchen vor dem Zurücksetzen eines Postfachs wird in einer UM-Postfachrichtlinie konfiguriert und gilt für alle Outlook Voice Access-Benutzer, die der UM-Postfachrichtlinie zugeordnet sind.

## NOTE

Sie erhöhen die Sicherheit, indem Sie die Einstellung **Anzahl der Anmeldefehler vor dem Zurücksetzen der PIN** mit einem kleineren Wert als 5 konfigurieren. Sie verringern die Sicherheit, wenn Sie diese Einstellung mit einem größeren Wert als 5 konfigurieren.

Informationen zu weiteren Aufgaben im Zusammenhang mit der Outlook Voice Access-PIN-Sicherheit finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Konfigurieren der Anzahl von Anmeldefehlern, bevor eine PIN zurückgesetzt wird, mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-

Postfachrichtlinie Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**

4. Klicken Sie auf **PIN-Richtlinien** und dann auf **Anzahl der Anmeldefehler vor dem Zurücksetzen der PIN:**, und geben Sie einen Wert zwischen 0 und 999 ein.
5. Klicken Sie auf **Speichern**.

**Verwenden von Exchange Online PowerShell so konfigurieren Sie die Anzahl der Anmeldung Fehler, bevor Sie eine PIN wird zurückgesetzt.**

In diesem Beispiel wird die Zahl der ungünstigen-Anmeldung auf, bevor der Benutzer PIN auf 3 für UM-aktivierte Benutzer zurückgesetzt wird, die mit dem Namen einer UM-Postfachrichtlinie zugeordnet sind .

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 3
```

In diesem Beispiel wird die Zahl der ungünstigen-Anmeldung auf, bevor der Benutzer PIN zurückgesetzt wird, auf 3, die maximale Anzahl der Anmeldeversuche auf 5, und die PIN-Mindestlänge bis 9 für UM-aktivierten Benutzer, die mit dem Namen einer UM-Postfachrichtlinie zugeordnet sind .

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 3 -MaxLogonAttempts 5 -MinPINLength 9
```

# Festlegen Sie die Zahl der ungünstigen-Anmeldung, bevor ein Voice Mail-Benutzer gesperrt ist

18.12.2018 • 4 minutes to read

Sie können konfigurieren, welche Anzahl fehlerhafter Anmeldeversuchen zulässig ist, bevor das Postfach eines Outlook Voice Access-Benutzers gesperrt wird. Die maximal zulässige Anzahl fehlerhafter Anmeldeversuche vor dem Sperren eines Postfachs wird in einer UM-Postfachrichtlinie konfiguriert und gilt für alle UM-aktivierten Benutzer, die der UM-Postfachrichtlinie unterliegen. Die Standardeinstellung ist 15.

Verringern Sie zum Erhöhen der Sicherheit die maximale Anzahl der Fehlversuche. Bei Festlegung auf einen Wert, der wesentlich kleiner als der Standardwert ist, werden Benutzerpostfächer jedoch gegebenenfalls unnötigerweise gesperrt. Wenn Fehler bei der PIN-Authentifizierung von UM-aktivierten Benutzern auftreten oder Anmeldeversuche von Benutzern beim System fehlschlagen, erzeugt Unified Messaging Warnereignisse, die Sie in der Ereignisanzeige anzeigen können. Diese Einstellung muss höher als die Einstellung für die Anzahl fehlerhafter Anmeldeversuche sein, ehe die PIN zurückgesetzt wird.

Informationen zu weiteren Aufgaben im Zusammenhang mit der Outlook Voice Access-PIN-Sicherheit finden Sie unter [PIN-Sicherheitsverfahren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: Weniger als 1 Minute.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM-Postfachrichtlinien" im Thema [Unified Messaging Permissions](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass UM-Wähleinstellungen erstellt wurden. Ausführliche Anleitungen finden Sie unter [Erstellen eines UM-Wählplans](#).
- Vergewissern Sie sich vor dem Ausführen dieser Verfahren, dass eine UM-Postfachrichtlinie erstellt wurde. Genaue Anweisungen finden Sie unter [Erstellen einer UM-Postfachrichtlinie](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Konfigurieren der maximalen Anzahl fehlerhafter Anmeldeversuche vor dem Sperren eines Voicemailbenutzers

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > UM-Wählpläne**.
2. In der Listenansicht, wählen Sie den UM-Wählplan, die Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

3. Klicken Sie auf der Seite **UM-Wählplan** unter **UM-Postfachrichtlinien**, wählen Sie die um-Postfachrichtlinie Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie auf **PIN-Richtlinien**, und geben Sie neben **Anzahl der Anmeldefehler vor dem Sperren** einen Wert von 1 bis 999 ein.
5. Klicken Sie auf **Speichern**.

Verwenden von Exchange Online PowerShell so konfigurieren Sie die Anzahl der Anmeldung Fehler, bevor ein Voice Mail-Benutzer ist gesperrt.

In diesem Beispiel wird die maximale Anzahl Anmeldeversuche bis 10 für UM-aktivierten Benutzer, die mit dem Namen einer UM-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -MaxLogonAttempts 10
```

In diesem Beispiel wird die Zahl der ungünstigen-Anmeldung an, bevor der Outlook Voice Access-Benutzer PIN zurückgesetzt wird, auf 3, die maximale Anzahl von Anmeldeversuchen auf 5 und eine PIN-Mindestlänge bis 9 für UM-aktivierten Benutzer, die mit dem Namen einer UM-Postfachrichtlinie zugeordnet sind `MyUMMailboxPolicy`.

```
Set-UMMailboxPolicy -Identity MyUMMailboxPolicy -LogonFailuresBeforePINReset 3  
-MaxLogonAttempts 5 -MinPINLength 9
```

# Erstellen von Berichten für Sprachanrufe mail

18.12.2018 • 3 minutes to read

Unified Messaging-Anrufberichte (UM) enthalten Informationen zu den Anrufen, die an UM weitergeleitet oder von UM durchgeführt wurden. Verwenden Sie diese Berichte zur Überwachung, Fehlerbehebung und Berichterstellung zu UM für die Organisation. Sie können auf Berichte mit Unified Messaging-Anrufstatistiken über das Tool "Anrufstatistik" und auf Anrufprotokolle für UM-aktivierte Benutzer über das Tool "Benutzeranrufprotokolle" zugreifen.

Diese Berichte enthalten aggregierte Statistikinformationen zu Anrufen für Exchange-Server und zu Anrufen für UM-aktivierte Benutzer in Ihrer Organisation. Diese Berichte ermöglichen Folgendes:

- Erfassen von Statistiken zu UM-Diensten und UM-aktivierten Benutzern in den jeweiligen Organisationen durch die Administratoren von lokalen, hybriden und Onlineorganisationen.
- Sie stellen Zusammenfassungen der erfassten Daten bereit. Diese Daten können bis zu 90 Tage gespeichert und bis zu zwei Jahre archiviert werden, um Aufbewahrungsanforderungen zu erfüllen.
- Überprüfen der allgemeinen Audioqualität für eingehende Anrufe bei bereitgestellten Exchange-Servern.
- Einfaches Überprüfen der Verfügbarkeit des Voicemailsystems und der UM-Dienste in der Organisation während eines bestimmten Zeitraums.
- Planen der Unified Messaging-Serverkapazität für eine lokale oder eine Hybridorganisation.
- Überprüfen, wie in einer Organisation bereitgestellte UM-Dienste während eines bestimmten Zeitraums verwendet werden.

Die folgenden Themen helfen Ihnen dabei, Anrufstatistiken und Berichte zu erfassen und diese Ergebnisse zu interpretieren, um UM-Dienste in der Organisation zu überwachen und Probleme damit zu behandeln:

- [Überprüfen Sie die e-Mail-Sprachanrufe in Ihrer Organisation](#) Mithilfe der UM-Anrufstatistik können Sie die Verfügbarkeit und die Audioqualität von UM überwachen und die Nutzung nachverfolgen, um sie in der Kapazitätsplanung zu berücksichtigen.
- [Überprüfen Sie die e-Mail-Sprachanrufe für einen Benutzer](#) Die Benutzeranrufprotokolle enthalten ausführliche Informationen zu den Anrufen für einen Benutzer innerhalb der letzten 90 Tage.
- [Überprüfen Sie die Audioqualität VoIP-Anrufe in Ihrer Organisation](#) Sollten in der Organisation Probleme mit der Audioqualität von UM-Anrufen auftreten, können Sie die Ursache des Problems mithilfe der Audioqualitätsdetails der UM-Anrufstatistik ermitteln.
- [Durchführen einer Überprüfung der Audioqualität von Sprachanrufen für Benutzer](#) Werden von einem Benutzer Probleme mit der Audioqualität der UM-Anrufe festgestellt, können Sie mithilfe der Informationen zur Audioqualität aus den Benutzeranrufprotokollen die Ursache der Probleme ermitteln.
- [Interpretieren von Voice Mail-anrufdatensätzen](#) Exportieren Sie ausführlichere Daten, um Probleme mit der Audioqualität oder mit abgelehnten Anrufen zu diagnostizieren sowie um Informationen für Überwachungen oder Berichte zum UM-Dienst bereitzustellen.

# UM Berichte Prozeduren

18.12.2018 • 2 minutes to read

Überprüfen Sie die e-Mail-Sprachanrufe in Ihrer Organisation

Überprüfen Sie die e-Mail-Sprachanrufe für einen Benutzer

Überprüfen Sie die Audioqualität VoIP-Anrufe in Ihrer Organisation

Durchführen einer Überprüfung der Audioqualität von Sprachanrufen für Benutzer

Interpretieren von Voice Mail-anrufdatensätze

# Überprüfen Sie die e-Mail-Sprachanrufe in Ihrer Organisation

18.12.2018 • 7 minutes to read

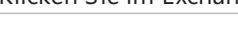
Mithilfe des Berichts "Anrufstatistik" können Sie Informationen zu Typ und Status von eingehenden Anrufen anzeigen, die von den Exchange-Servern in Ihrer Organisation verarbeitet wurden. Der Bericht enthält statistische Informationen zu den Anrufen, die an UM weitergeleitet oder von UM für die Organisation erfasst wurden. Anhand dieser Informationen können Sie für die Kapazitätsplanung, Überwachung und Behandlung von UM-Verfügbarkeits- und Audioqualitätsproblemen sowie nicht erfolgreicher Anrufe die Nutzung nachverfolgen.

In diesem Thema werden diese Fragen beantwortet:

- [Wie rufe ich Anrufstatistiken für UM ab?](#)
- [Wie werte ich UM-Anrufstatistiken aus?](#)

Informationen zu weiteren Aufgaben im Zusammenhang mit UM-Berichten finden Sie unter [UM Berichte Prozeduren](#).

## Wie rufe ich Anrufstatistiken für UM ab?

1. Klicken Sie im Exchange Administrationscenter (EAC) auf **Unified messaging > Weitere Optionen**  **> Statistiken aufrufen**.
2. Wählen Sie die Informationen aus, die in den Bericht eingeschlossen werden soll. Der Bericht wird automatisch aktualisiert, wenn Sie eine der folgenden Optionen auswählen:
  - **Anzeigen:** Wählen Sie den Anrufstatistiken anzeigen:
  - **Täglich (90 Tage):** täglich wählen Sie in der letzten 90 Tage für alle Anrufe angezeigt.
  - **Monatlich (12 Monate):** monatliche wählen, um eine Zusammenfassung der Anrufe nach Monat für die letzten 12 Monate anzuzeigen.
  - **Alle:** Wählen Sie alle die kombinierte Statistik für alle Anrufe, die seit dem Start UM Bearbeiten der Anrufe empfangen zu sehen.
  - **UM-Wähleinstellungen:** Wenn Sie die Daten im Bericht nur Anrufe in einem bestimmten um-Wählplan beschränken möchten, wählen Sie dieses Gateway. Wenn Sie einen um-Wählplan zuerst auswählen, werden nur die UM-IP-Gateways, die dem ausgewählten um-Wählplan zugeordnet in der Liste aufgeführt.
3. Wenn Sie für eine Zeile des Berichts ausführlichere Informationen zur Audioqualität anzeigen möchten, markieren Sie die Zeile, und klicken Sie auf **Details zur Audioqualität**. Weitere Informationen zum Interpretieren der Audioqualität finden Sie unter [Überprüfen Sie die Audioqualität VoIP-Anrufe in Ihrer Organisation](#).
4. Wenn Sie den Bericht in die Zwischenablage kopieren möchten, klicken Sie auf **Kopieren**.
5. Für tägliche Berichte können Sie Details für einen bestimmten Tag in eine CSV-Datei exportieren.
6. Wählen Sie den Tag aus, und klicken Sie auf **Tag exportieren**.

## 7. Klicken Sie im Bestätigungsdialogfeld **Dateidownload** auf **Öffnen** oder **Speichern**.

Die exportierte Datei wird Um\_cdr\_ *YYYY-MM-TT.csv*, heißen, wobei *YYYY-MM-TT* ist, das Jahr, Monat und Tag, die der Bericht ausgeführt wurde. Weitere Informationen finden Sie unter [interpretieren Voice Mail-anrufdatensätze](#).

### NOTE

Auf der Berichtsseite können Sie eine Microsoft Excel-Vorlage herunterladen, mit der Sie die CSV-Datei für einen bestimmten Tag importieren können.

[Return to top](#)

## Wie werte ich UM-Anrufstatistiken aus?

Der Bericht für die UM-Anrufstatistik enthält die folgenden Informationen:

- **Datum:** der UTC-Datum für die Anrufdaten. Das Datumsformat hängt von den Typ des Berichts, den Sie ausgewählt haben und Ihr Gebietsschema. Sie können aus den folgenden Optionen wählen:
  - ---: Alle Anrufe werden angezeigt.
  - **MMM/JJ:** den Monat die Anrufe. Beispielsweise Jan/13.
  - **MM/TT/JJ:** den Tag der Aufrufe. Beispiel 6/23/13.
- **Insgesamt:** die Gesamtzahl der Aufrufe für die ausgewählten UM-Wähleinstellungen oder das UM-IP-Gateway für das Datum.
- **SPRACHNACHRICHT:** der Prozentsatz eingehender Anrufe entgegen UM im Namen von Benutzern in welche Aufrufer links eine Sprachnachricht.
- **Verpasste:** der Prozentsatz eingehender Anrufe, die durch UM im Namen von Benutzern in der Aufrufer keine Sprachnachricht hinterlassen, wodurch eine Benachrichtigung über verpasste Anrufe beantwortet.
- **OUTLOOK VOICE ACCESS:** der Prozentsatz eingehender Anrufe, in dem Benutzer zu um-WÄHLPLAN angemeldet (und authentifiziert wurden) auf ihre e-Mail-Nachrichten, Kalender und Sprachnachrichten zuzugreifen.
- **AUSGEHEND:** authentifiziert, oder der Prozentsatz der Anrufe, die getätigt wurden oder Übertragen von UM im Auftrag von nicht authentifizierten Benutzern. Diese Statistik enthält suchen mich, am Telefon wiedergeben und Wiedergabe über Telefon Ansage Anruftypen.
- **Automatische TELEFONZENTRALE:** der Prozentsatz eingehender Anrufe, die von automatischen UM-Telefonzentralen beantwortet wurden.
- **FAX:** der Prozentsatz eingehender Anrufe, die an einen faxpartner umgeleitet wurden.
- **OTHER:** der Prozentsatz der alle anderen ein- oder platzierten Anrufe, die nicht in einem der oben genannten Kategorien fallen. Bei diesen anrufen enthalten Aufrufe an Outlook Voice Access Zahlen, in dem der Benutzer nicht anmelden und wurden nicht authentifiziert.
- **Fehler bei oder abgelehnt:** der Prozentsatz der Anrufe, die entweder Fehler verursacht haben oder vom UM abgelehnt wurden. Beachten Sie, dass fehlerhafte Anrufe werden nicht doppelt gezählt. Beispielsweise wenn ein Anruf an Outlook Voice Access ein Fehler auftritt, wird er nur als fehlgeschlagen Anruf und nicht auch als ein Anruf Outlook Voice Access gezählt.
- **AUDIOQUALITÄT:** die allgemeine Audioqualität für den ausgewählten Zeitraum für die Organisation grafisch dargestellt.

[Return to top](#)

## Weitere Informationen

[Überprüfen Sie die Audioqualität VoIP-Anrufe in Ihrer Organisation](#)

[Interpretieren von Voice Mail-anrufdatensätze](#)

# Überprüfen Sie die e-Mail-Sprachanrufe für einen Benutzer

18.12.2018 • 5 minutes to read

Mithilfe von Benutzeranrufprotokollen können die folgenden Informationen zu bestimmten UM-Benutzern (Unified Messaging) angezeigt werden:

- Details zu den UM-Anrufen für einen Benutzer innerhalb der letzten 90 Tage.
- Audioqualität der einzelnen Anrufe. Die Audioqualitätsmetrik ist unter Umständen nicht für alle Anrufe verfügbar, da die Metrik von mehreren Faktoren (wie Art und die Dauer des Anrufs) abhängt.

Informationen zu weiteren Aufgaben im Zusammenhang mit UM-Berichten finden Sie unter [UM Berichte Prozeduren](#).

## Wie rufe ich Anrufprotokolle für einen UM-aktivierten Benutzer ab?

1. In der Exchange-Verwaltungskonsole (EAC), wählen Sie **Unified messaging > Weitere Optionen**  
 > **Benutzer Anruflisten**.
2. Klicken Sie auf **Benutzer auswählen**, und wählen Sie den Benutzer aus, für den Sie Daten abrufen möchten.
3. Wenn Sie für eine Zeile des Berichts ausführlichere Informationen zur Audioqualität anzeigen möchten, markieren Sie die Zeile, und klicken Sie auf **Details zur Audioqualität**. Weitere Informationen zum Interpretieren der Audioqualität finden Sie unter [Durchführen einer Überprüfung der Audioqualität von Sprachanrufen für Benutzer](#).
4. Wenn Sie den Bericht in die Zwischenablage kopieren möchten, klicken Sie auf **Alle Zeilen in die Zwischenablage kopieren**.

## Wie interpretiere ich das UM-Benutzeranrufprotokoll?

Das Benutzeranrufprotokoll enthält zu jedem Anruf folgende Informationen:

- **Datum und Uhrzeit:** Datum und Uhrzeit des Anrufs, in der Zeitzone, die der ausgewählte Benutzer in Microsoft Outlook Web App festgelegt wurde.
- **Dauer:** wie lange in Minuten (MM) und Sekunden (SS), im folgenden Format Anrufs: mm: ss.
- **CALL TYPE:** den Anruftyp:
  - **Entgegennehmen von Anrufen:** der Aufruf war nicht beantwortet und an die Mailbox-Server weitergeleitet wurde, und der Aufrufer links auf einer Sprachnachricht.
  - **Rufen Sie Entgegennehmen von Anrufen entgangene:** der Aufruf war nicht beantwortet und an die Mailbox-Server weitergeleitet wurde, und der Aufrufer eine Sprachnachricht hinterlassen haben.
  - **Teilnehmerzugriff:** ein Anruf wurde versucht, die Teilnehmerzugriffsnummer. Der Aufrufer angemeldet und wurde authentifiziert, UM mit deren Erweiterung und das Kennwort für den e-Mail-Nachrichten, Kalender und Sprachnachrichten über das Telefon Zugriff auf.
  - **Automatische Telefonzentralen:** der Anruf entgegengenommen wurde, durch eine automatische

um-Telefonzentrale. Bei diesen anrufen sind in der Regel Anrufe in dem der Aufrufer Haupttelefonnummer des Unternehmens gewählt.

- **Fax:** ein Anruf wurde empfangen, in dem ein Fax-Ton erkannt wurde. Wenn Sie Fax Partner konfiguriert haben, wurde dieser Aufruf an den Partner gesendet.
  - **PlayonPhone:** wurde durch UM ein Anruf getätigt, da der Benutzer auf die Schaltfläche Telefon in einer Sprachnachricht in Microsoft Outlook Web App oder Outlook wiedergeben geklickt hat.
  - **FindMe:** ein ausgehender Anruf platziert wurde UM als Ergebnis einer mich Regel in eine mailboxansageregel zu suchen.
  - **Anzahl von nicht authentifizierten Pilot:** ein Anruf an die Outlook Voice Access getätigt wurde. Der Anrufer nicht anmelden und wurde nicht authentifiziert.
  - **Aufzeichnung Ansage:** UM aufzeichnen persönliche Begrüßung für einen Benutzer ein Anruf platziert wurde.
  - **None:** ein Anruf getätigt wurde, aber der Typ wurde nicht definiert.
- **Anzahl aufrufen:** die Telefonnummer oder die SIP-Adresse des Anrufers.
  - **Anzahl AUFGERUFEN:** die Telefonnummer oder die SIP-Adresse (für Benutzer in SIP-Wählplänen, wie beispielsweise Microsoft Office Communications Server 2007 R2 oder Microsoft Lync Server-Benutzer) der eigentliche Empfänger des Anrufs.
  - **UM-IP-GATEWAY:** die UM-IP-Gateways, die den Anruf ausgeführt wurden.
  - **AUDIOQUALITÄT:** die allgemeine Audioqualität des Anrufs. Weitere Informationen zur Audioqualität wählen Sie die Zeile aus, und klicken Sie auf **Audio Qualität Details**.

# Überprüfen Sie die Audioqualität VoIP-Anrufe in Ihrer Organisation

18.12.2018 • 6 minutes to read

Sollten in der Organisation Probleme mit der Audioqualität von UM-Anrufen und Voicemailnachrichten auftreten, verwenden Sie den Bericht Anrufstatistik, um die Ursache der Probleme zu ermitteln.

## NOTE

Die Audioqualität eines Anrufs kann durch Faktoren beeinträchtigt werden, die nicht in den Berichten behandelt werden. Liegt auf Ihren Exchange-Servern beispielsweise eine hohe Arbeitsspeicher- oder CPU-Auslastung vor, melden die Benutzer unter Umständen eine schlechte Anrufqualität, obwohl die Audioqualität den Berichten zufolge ausgezeichnet ist.

Weitere Aufgaben im Zusammenhang mit Anrufstatistiken finden Sie unter [UM Berichte Prozeduren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM rufen Sie Daten und Zusammenfassungsbericht Cmdlets" im Thema [Unified Messaging Permissions](#) .
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Abrufen von Statistiken zur Audioqualität in Ihrer Organisation mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified messaging > Weitere Optionen**  
[ ] > **Statistiken aufrufen**.
2. Wählen Sie die Anrufstatistik aus, die in den Bericht eingeschlossen werden soll. Der Bericht wird automatisch aktualisiert, wenn Sie beliebige der folgenden Optionen auswählen:
  - **Anzeigen:** Wählen Sie den Anrufstatistiken anzeigen:
  - **Täglich (90 Tage):** tägliche wählen Sie in der letzten 90 Tage für alle Anrufe angezeigt.
  - **Monatlich (12 Monate):** monatliche wählen, um eine Zusammenfassung der Anrufe nach Monat für die letzten 12 Monate anzuzeigen.
  - **Alle:** Wählen Sie alle die kombinierte Statistik für alle Anrufe, die seit dem Start UM Bearbeiten der Anrufe empfangen zu sehen.
  - **UM-Wähleinstellungen:** Wenn Sie die Daten im Bericht nur Anrufe in einem bestimmten um-Wählplan

beschränken möchten, dass Wähleinstellungen auswählen.

- **UM-IP-Gateway:** Wenn Sie die Daten im Bericht nur Anrufe in einer bestimmten UM-IP-Gateway einschränken möchten, wählen Sie aus, UM-IP-Gateway. Wenn Sie einen um-Wählplan zuerst auswählen, werden nur die UM-IP-Gateways, die dem ausgewählten um-Wählplan zugeordnet in der Liste aufgeführt.

3. Wenn Sie für eine Zeile des Berichts ausführlichere Informationen zur Audioqualität anzeigen möchten, markieren Sie die Zeile, und klicken Sie auf **Details zur Audioqualität**. Die folgenden Informationen sind verfügbar:

- **Datum und Uhrzeit:** der UTC-Datum und Uhrzeit, die die Anruf Statistiken erfasst wurden.
- **Um-WÄHLPLAN:** die Wähleinstellungen für die Anrufe in die Statistiken enthalten.
- **UM-IP-GATEWAY:** die UM-IP-Gateway, die die Anrufe in die Statistik einbezogenen ausgeführt wurden.
- **NMOS:** das Netzwerk Mean Opinion Score (NMOS) für den Anruf. Die NMOS gibt an, wie gut die Audioqualität für den Aufruf als Zahl auf einer Skala von 1 bis 5, mit 5 wird hervorragende wurde.

**NOTE**

Das bestmögliche NMOS-Ergebnis eines Anrufs hängt vom verwendeten Audio-Codec ab. Das NMOS-Ergebnis steht ggf. für Anrufe, die kürzer als 10 Sekunden sind, nicht zur Verfügung.

- **NMOS-Beeinträchtigung:** der Betrag audio Verschlechterung der Abweichung des NMOS vom oberen Wert möglich, dass der Audiocodec verwendet wird. Angenommen, wenn der Wert des NMOS-Beeinträchtigung für einen Anruf 1.2 wurde und die Abweichung des NMOS für den Anruf gemeldet 3.3 wurde, wäre die maximale NMOS für diesen bestimmten Aufruf 4.5 (1.2 + 3.3).
  - **JITTER:** die durchschnittliche Abweichung in den Empfang von Datenpaketen für den Anruf.
  - **PAKETVERLUST:** der durchschnittliche Prozentsatz der Daten Paketverlust für den ausgewählten Anruf. Paketverlust ist ein Hinweis auf die Zuverlässigkeit der Verbindung.
  - **ROUNDTrip:** die durchschnittliche Roundtrip Faktor, in Millisekunden für Audio auf den ausgewählten Anruf. Die Round-Trip Bewertung misst Wartezeit für die Verbindung.
  - **Spitzen-Verlust Dauer:** die durchschnittliche Dauer an Paketverlusten bei Bursts von Verlusten für den ausgewählten Anruf.
  - **Anzahl der Beispiele:** die Anzahl der Anrufe, die als Stichprobe verwendet wurden, um die Durchschnittswerte berechnen.
4. Eine ausführliche Audioqualitätsmetrik zu bestimmten Anrufen finden Sie unter [Durchführen einer Überprüfung der Audioqualität von Sprachanrufen für Benutzer](#).

# Durchführen einer Überprüfung der Audioqualität von Sprachanrufen für Benutzer

18.12.2018 • 4 minutes to read

Werden von einem Benutzer Probleme mit der Audioqualität der UM-Anrufe (Unified Messaging) gemeldet, können Sie den Bericht für Benutzeranrufprotokolle verwenden, um die Ursache der Probleme zu klären.

## NOTE

Die Audioqualität eines Anrufs kann durch Faktoren beeinträchtigt werden, die nicht in den Berichten behandelt werden. Liegt auf Ihren Exchange-Servern beispielsweise eine hohe Arbeitsspeicher- oder CPU-Auslastung vor, melden die Benutzer unter Umständen eine schlechte Anruflqualität, obwohl die Audioqualität den Berichten zufolge ausgezeichnet ist.

Informationen zu weiteren Aufgaben im Zusammenhang mit UM-Berichten finden Sie unter [UM Berichte Prozeduren](#)

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "UM rufen Sie Daten und Zusammenfassungsbericht Cmdlets" im Thema [Unified Messaging Permissions](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Abrufen von Anruflisten für einen UM-aktivierten Benutzer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified Messaging > Weitere Optionen**  
[ ] > **Benutzer Anruflisten**.
2. Klicken Sie auf **Benutzer auswählen**, und wählen Sie den Benutzer aus, für den Sie Daten abrufen möchten.
3. Wenn Sie für eine Zeile des Berichts ausführlichere Informationen zur Audioqualität anzeigen möchten, markieren Sie die Zeile, und klicken Sie auf **Details zur Audioqualität**. Die folgenden Informationen sind verfügbar:
  - **Datum und Uhrzeit:** Datum und Uhrzeit des Anrufs, in der Zeitzone, die der ausgewählte Benutzer in Outlook Web App festgelegt wurde.
  - **Benutzer:** den ausgewählten Benutzer.

- **Um-WÄHLPLAN**: die Wähleinstellungen für den Anruf.
- **UM-IP-GATEWAY**: die UM-IP-Gateway, das für den Anruf verwendet wurde.
- **AUDIOCODEC**: Audiocodec, die während des Anrufs verwendet wurde.
- **NMOS**: das Netzwerk Mean Opinion Score (NMOS) für den Anruf. Die NMOS gibt an, wie gut die Audioqualität für den Aufruf als Zahl auf einer Skala von 1 bis 5, mit 5 wird hervorragende wurde.

**NOTE**

Der maximal mögliche NMOS-Wert für einen Anruf hängt vom verwendeten Audio codec ab. Für sehr kurze Anrufe von weniger als 10 Sekunden ist möglicherweise kein NMOS-Wert verfügbar.

- **NMOS-Beeinträchtigung**: der Betrag audio Verschlechterung der Abweichung des NMOS vom oberen Wert möglich, dass der Audio codec verwendet wird. Angenommen, wenn der Wert des NMOS-Beeinträchtigung für einen Anruf 1.2 wurde und die Abweichung des NMOS für den Anruf gemeldet 3.3 wurde, wäre die maximale NMOS für diesen bestimmten Aufruf 4.5 (1.2 + 3.3).
- **JITTER**: die durchschnittliche Abweichung in den Empfang von Datenpaketen für den Anruf.
- **PAKETVERLUST**: der durchschnittliche Prozentsatz der Daten Paketverlust für den ausgewählten Anruf. Paketverlust ist ein Hinweis auf die Zuverlässigkeit der Verbindung.
- **ROUNDTRIP**: die durchschnittliche Roundtrip Faktor, in Millisekunden für Audio auf den ausgewählten Anruf. Die Round-Trip Bewertung misst Wartezeit für die Verbindung.
- **Spitzen-Verlust Dauer**: die durchschnittliche Dauer an Paketverlusten bei Bursts von Verlusten für den ausgewählten Anruf.

# Interpretieren von Voice Mail-anrufdatensätze

18.12.2018 • 13 minutes to read

Um ausführliche Informationen zu Anrufen anzuzeigen, die an einem bestimmten Tag von den Exchange-Servern behandelt wurden, exportieren Sie die Anrufdaten für diesen Tag aus dem Anrufstatistikbericht. Tägliche Anrufdaten, die für die vergangenen 90 Tage verfügbar sind, helfen Ihnen beim Diagnostizieren von Problemen mit der Audioqualität oder abgelehnten Anrufen und stellen Informationen für Überwachungen oder Berichte zu Exchange-Servern in der Organisation bereit.

Informationen zu weiteren Aufgaben im Zusammenhang mit UM-Berichten finden Sie unter [UM Berichte Prozeduren](#).

## Exportieren täglicher UM-Anrufdatensätze mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Unified messaging > Weitere Optionen** > **Statistiken aufrufen**.
2. Klicken Sie unter **Anzeigen** auf **Täglich (90 Tage)**, und wählen Sie dann den UM-Wählplan oder das UM-IP-Gateway oder ggf. beides aus. Der Bericht wird automatisch aktualisiert, wenn Sie Optionen auswählen.
3. Wählen Sie den Tag aus, für den Sie Anrufdatensätze exportieren möchten, und klicken Sie auf **Tag exportieren**.
4. Klicken Sie im Bestätigungsdialogfeld **Dateidownload** auf **Öffnen** oder **Speichern**.

Die exportierte Datei wird Um\_cdr\_ JJJJ-MM-TT.csv, heißen, wobei JJJJ-MM-TT ist, das Jahr, Monat und Tag, die der Bericht ausgeführt wurde.

### NOTE

Auf der Berichtsseite können Sie eine Microsoft Excel-Vorlage herunterladen, mit der Sie die CSV-Datei für einen bestimmten Tag importieren können.

5. Verwenden Sie eine Anwendung wie Excel, um die CSV-Datei zu verarbeiten und eigene benutzerdefinierte Berichte zu erstellen.

## Interpretieren von UM-Anrufdaten

Die exportierten UM-Anrufdaten enthalten die folgenden detaillierten Informationen zu jedem Anruf, der an diesem Tag von UM behandelt wurde.

### NOTE

Im Anrufstatistikbericht werden die Tage in der UTC-Zeit angezeigt.

- **CallStartTime:** Datum und Uhrzeit, die den Anruf in UTC UM behandelt. Das Datum und die UTC-Zeit wird in folgendem Format dargestellt: JJJJ-MM-TT ssZ, in dem YYYY = Jahr, MM = Monat, DD = Tag, Hh Stunde im 24-Stunden, mm == Minuten, ss = Sekunden. Z bedeutet Zulu, die eine Möglichkeit zum

Kennzeichnen von UTC ist (wie *+Hh:mm* oder *-Hh:mm*, der aus UTC in die Uhrzeit-Offset können). Da alle Anrufzeiten in diesem Bericht in UTC-Zeit sind, wird diese Z verwendet werden.

Für einen Anruf am 23.06.13 um 14:23 Uhr wird die Anrufstartzeit z. B. als 23.06.2013 14:23:11Z angezeigt.

- **Call Type:** den Anruftypt:

- **Rufen Sie beantworten Sprachnachricht:** der Aufruf war nicht beantwortet und an die Exchange-Server weitergeleitet wurde, und der Aufrufer links auf einer Sprachnachricht.
  - **Rufen Sie Entgegennehmen von Anrufen entgangene:** der Aufruf war nicht beantwortet und an die Exchange-Server weitergeleitet wurde, und der Aufrufer eine Sprachnachricht hinterlassen haben.
  - **Teilnehmerzugriff:** ein Anruf wurde versucht, die Teilnehmerzugriffsnummer. Der Aufrufer angemeldet und wurde authentifiziert, UM mit deren Erweiterung und das Kennwort für den e-Mail-Nachrichten, Kalender und Sprachnachrichten über das Telefon Zugriff auf.
  - **Automatische Telefonzentralen:** der Anruf entgegengenommen wurde, durch eine automatische um-Telefonzentrale. Bei diesen anrufen sind in der Regel Anrufe in dem der Aufrufer Haupttelefonnummer des Unternehmens gewählt.
  - **Fax:** ein Anruf wurde empfangen, in dem ein Fax-Ton erkannt wurde. Wenn Sie Fax Partner konfiguriert haben, wurde dieses Anrufs an den faxpartner gesendet.
  - **PlayOnPhone:** wurde durch UM ein Anruf getätigt, da der Benutzer auf die Schaltfläche Telefon in einer Sprachnachricht in Microsoft Outlook Web App oder Outlook wiedergeben geklickt hat.
  - **Hier finden Sie mich:** ein ausgehender Anruf platziert wurde UM als Ergebnis einer mich Regel in eine mailboxansageregel zu suchen.
  - **Anzahl von nicht authentifizierten Pilot:** ein Anruf an die Outlook Voice Access getätigt wurde. Der Aufrufer nicht anmelden und wurde nicht authentifiziert.
  - **Aufzeichnung Ansage:** UM aufzeichnen persönliche Begrüßung für einen Benutzer ein Anruf platziert wurde.
  - **None:** ein Anruf getätigt wurde, aber der Typ wurde nicht definiert.
- **CallIdentity:** der SIP-Anruf-Identität, von dem UM-IP-Gateway bereitgestellt werden.
  - **ParentCallIdentity:** der SIP-Sitzung Identität der Sitzung, die dieses Anrufs ausgelöst hat. In diesem Feld wird verwendet, wenn Sie den Anruf entgegennehmen Regeln Find Me Feature oder Anruf stellen Sie Anrufe, einschließlich Call gehandelt zwischen automatischen UM-Telefonzentralen verwenden.
  - **UMServerName:** der Name des Postfachservers, der den Anruf behandeln, sofern vorhanden. Diese Informationen nur, wenn Sie über einen lokalen Postfachserver verfügen.
  - **Wählplannamens:** der UM-Wählplan, die der Anruf verarbeitet.
  - **Rufen Sie Dauer:** die gesamte Dauer des Anrufs.
  - **IPGatewayAddress:** den vollqualifizierten Domänenamen (FQDN) des IP-Gateways, die der Anruf verarbeitet.
  - **CalledPhoneNumber:** die angegebene Rufnummer oder SIP-Adresse des Empfängers des Anrufs (für Benutzer in SIP-Wählplänen mit Microsoft Office Communications Server 2007 R2 oder Microsoft Lync Server).
  - **CallerPhoneNumber:** die angegebene Rufnummer oder SIP-Adresse des Anrufers.

- **OfferResult:** der Status des Anrufs:
  - **Antwort:** UM erfolgreich beantwortet haben oder einen Anruf platziert. Der Anruf wurde weder übertragen noch umgeleitet. Bei diesen anrufen abgeschlossenen Aufrufe Outlook Voice Access, Wiedergabe über Telefon oder UM-Telefonzentralen und aufruft, UM, wenn die gewählte Erweiterung Antworten nicht behandelt.
  - **Fehler:** UM angenommen oder getätigter einen Aufruf, jedoch ist fehlgeschlagen. Bei diesen anrufen umfassen Anrufe, in dem die gewählte Nummer oder Adresse ist überlastet, nicht annehmen, oder ist nicht vorhanden. in dem der Aufrufer die Verbindung trennt, bevor die Verbindung hergestellt wurde; Der UM-Wählplan oder UM postfachrichtlinieneinstellungen verhindert, in dem den Anruf; oder, in dem die VoIP-Gateway oder IP-PBX auf Ihrem Telefonsystem konnte nicht erreicht werden.
  - **Abgelehnt:** UM den Anruf in der Regel aufgrund eines Konfigurationsfehlers abgelehnt. Bei diesen anrufen enthalten Aufrufe, wenn das UM-IP-Gateway einem um-Wählplan zugeordnet ist, nicht oder Inkompatibilitätsprobleme vorhanden sind.
  - **Umgeleitet:** UM den Anruf angenommen, aber es auf einen anderen Postfachserver umgeleitet. Bei diesen anrufen enthalten Aufrufe, wenn der Aufrufer im Menü UM verwendet, um einen Kontakt in das Verzeichnis oder persönliche Kontakte aufrufen oder der Aufrufer aufgerufen eine Outlook Voice Access-Nummer verwenden eine Telefonnummer ein, die das Postfach des Benutzers zugeordnet ist. In diesen Fällen wird UM den Anruf an den Exchange-Server, der mit dem Konto des Benutzers verbunden ist.
  - **None:** der Status des Anrufs ist unbekannt.
- **DropCallReason:** die Ursache der Anruf beendet wurde, wenn UM den Grund zu ermitteln konnte. Wenn der Anrufer die Verbindung trennt, wird dies beispielsweise ordnungsgemäßes Auflegen.
- **ReasonForCall:** wie die Verbindung hergestellt wurde:
  - **Direkte:** der Anrufer die gewählte Nummer direkt gewählt.
  - **DivertForward:** der Anrufer eine Telefonnummer gewählt und der angerufene den Anruf an Voicemail UM umgeleitet.
  - **DivertBusy:** der Anrufer eine Telefonnummer gewählt und das Telefon wurde beschäftigt, damit der Anruf an Voicemail UM umgeleitet wurde.
  - **DivertNoAnswer:** der Anrufer eine Telefonnummer gewählt und die Person nicht annehmen möchten, damit der Anruf an Voicemail UM umgeleitet wurde.
  - **Ausgehend:** der Anruf wurde von getätigter UM, beispielsweise zur Wiedergabe einer Sprachnachricht mithilfe von am Telefon wiedergeben.
  - **None:** keinen Grund für den Anruf gemeldet wurde.
- **DialedString:** die Anzahl Adresse oder Telefonnummer der Person ein, denen dieser Aufruf wurde entweder bezeichnet wird, oder übertragen. Dieser Wert bezieht sich auch an die Adresse oder Telefonnummer für die Wiedergabe für Telefonanrufe aufgerufen.
- **CallerMailboxAlias:** die Postfach-Alias (der Teil der e-Mail-Adresse, die vor dem @-Zeichen) des Anrufers. Dieser Wert ist nur verfügbar, wenn der Anrufer bei Outlook Voice Access angemeldet.
- **CallerMailboxAlias:** der Postfachalias, der den Empfänger des Anrufs, wenn der Empfänger einen UM-aktivierten Benutzer ist.
- **Name der automatischen Telefonzentrale:** der Name der automatischen Telefonzentrale im Zusammenhang mit diesem Anruf.

- **NMOS Score:** das Netzwerk Mean Opinion Score (NMOS) für den Anruf. Die NMOS gibt an, wie gut die Audioqualität für den Aufruf als Zahl auf einer Skala von 1 bis 5, mit 5 wird hervorragende wurde.

**NOTE**

**Hinweis:** die maximale NMOS möglichen für einen Anruf hängt von der Audiocodec verwendet wird. Die NMOS möglicherweise nicht zur Verfügung für sehr Anrufe, die weniger als 10 Sekunden sind.

- **NMOSDegradation:** der Betrag audio Verschlechterung der Abweichung des NMOS vom oberen Wert möglich, dass der Audiocodec verwendet wird. Angenommen, wenn der Wert des NMOS-Beeinträchtigung für einen Anruf 1.2 wurde und die Abweichung des NMOS für den Anruf gemeldet 3.3 wurde, wäre die maximale NMOS für diesen bestimmten Aufruf 4.5 (1.2 + 3.3).
- **NMOSDegradation Jitter:** insgesamt NMOS-Beeinträchtigung aufgrund von Jitter.
- **NMOSDegradation PacketLoss:** insgesamt NMOS-Beeinträchtigung aufgrund von Paketverlust.
- **Jitter:** die durchschnittliche Abweichung in den Empfang von Datenpaketen für den Anruf.
- **PacketLoss:** der durchschnittliche Prozentsatz der Daten Paketverlust für den ausgewählten Anruf. Paketverlust ist ein Hinweis auf die Zuverlässigkeit der Verbindung.
- **Roundtrip:** der durchschnittliche Roundtrip in Millisekunden für Audio auf den ausgewählten Anruf. Die Round-Trip Bewertung misst Wartezeit für die Verbindung.
- **BurstDensity:** der Prozentsatz der Pakete verloren und binnen (hoch Verlust Rate) Bursts verworfen.
- **Spitzen-lückendauer:** die durchschnittliche Dauer an Paketverlusten bei Bursts von Verlusten für den ausgewählten Anruf.
- **Audiocodec:** während des Anrufs verwendete Audiocodec.

# UM und Voice Mail Terminologie

18.12.2018 • 21 minutes to read

In der folgenden Tabelle sind die Begriffe und Definitionen enthalten, die beim Microsoft Unified Messaging verwendet werden.

## Audiocodec

Eine digitale Codierung eines analogen Sprachsignals. Die meisten Audiocodes bieten eine Datenkomprimierung, die bei der Wiederherstellung der Daten zu gewissen Einbußen bei der Wiedergabetreue führt. Audiocodecs können in der Soundqualität, der für ihre Nutzung erforderlichen Bandbreite und den Systemanforderungen, die für die Codierung benötigt werden, variieren.

## Audionotizen

Textbasierte Notizen, die zu einer Voicemailnachricht hinzugefügt werden können, die in Outlook oder Outlook Web App empfangen wurde.

## Automatische Telefonzentrale

Ein Softwaresystem, das Anrufe beantwortet, Ansagen oder Anweisungen wiedergibt und dann Eingaben des Anrufers als Wältöne oder Sprache erfasst. Automatische Telefonzentralen können einen Anruf an vom Anrufer angegebene Telefonnummern bzw. benannte Benutzer oder Entitäten (z. B. Abteilungen) ohne manuellen Eingriff eines Mitarbeiters der Vermittlungsstelle weiterleiten.

## ASR (Automatic Speech Recognition, Automatische Spracherkennung)

Eine Technologie, mit der ein Computer die menschliche Sprache mit einem vordefinierten Satz von Wörtern oder Begriffen abgleichen kann.

## Anrufannahme

Der Prozess der Interaktion eines Anrufers mit einem Voicemailsysteem, wenn unter der ursprünglich gewählten Nummer nicht geantwortet wird. Normalerweise wird vom System eine Begrüßung oder Ansage wiedergegeben und dem Anrufer die Möglichkeit geboten, eine Sprachnachricht aufzuzeichnen.

## Mailboxansageregeln

Eine Form der Mailboxansage, bei der der Benutzer, für den der Anruf angenommen wird, Regeln festlegen kann, um das dem Anrufer entgegengesetzte Verhalten zu bestimmen. Der Benutzer kann auszuwertende Bedingungen, Begrüßungen und dem Anrufer bereitzustellende Auswahlmöglichkeiten sowie Aktionen angeben (z. B. das Durchstellen oder Hinterlassen einer Nachricht), die als Reaktion auf die Auswahl des Anrufers ausgeführt werden.

## Leitungsvermitteltes Netzwerk

Ein Netzwerk mit einer dedizierten Verbindung. Eine dedizierte Verbindung ist ein Schaltkreis oder eine Leitung, der/die zwischen zwei Knoten eingerichtet wird, um diesen die Kommunikation untereinander zu ermöglichen.

## Bedingte Anrufweiterleitung

Eine Reihe von Bedingungen, die von einem Benutzer ausgewählt und verwendet werden, wenn ein eingehender Anruf empfangen wird. Der Anruf wird auf Basis der festgelegten Bedingungen weitergeleitet.

## Wahl nach Namen

Eine Funktion, die einem Anrufer die Eingabe des Namens einer Person über die Tastatur eines Telefons ermöglicht (ABC=2, DEF=3 usw.).

## Wähleinstellungen

Für Unified Messaging sind dies eine Reihe von telefonfähigen Endpunkten, die einen gemeinsamen Rufnummerplan teilen. Die Details des Plans werden vom Telefonsystem bestimmt, über das das UM verbunden ist. Im einfachsten Fall kann dies eine PBX-Anlage (Private Branch Exchange) mit ihren Durchwahlnummern sein, wobei jede eine eindeutige Nummer mit fester Länge besitzt.

## Wählregelgruppe

Zum Aktivieren von Telefonnummern an geändert werden, bevor sie mit einer herkömmlichen oder SIP-aktivierte PBX oder IP-PBX für ausgehende Anrufe gesendet werden, werden Wählregelgruppen erstellt. Wählregelgruppen möglicherweise Ziffern von entfernen oder hinzufügen Ziffern Telefonnummern, die zum Anrufen von einem Unified Messaging-Server verwendet werden. Jeder Wählvorgang Regelgruppe enthält wählregeleinträge, die die Typen der nationale/regionale und internationale Anrufe zu bestimmen, die Benutzer in einer Wählvorgang Regelgruppe vornehmen können. Jeder Wählvorgang Regelgruppe muss mindestens ein Wählvorgang Regel Eintrag enthalten.

## Faxpartner

UM-Faxpartner stellen Anwendungen oder Dienste bereit, die Anrufe annehmen können, die von UM bei der Faxtonerkennung übergeben werden. Das Produkt oder der Dienst des Partners empfängt dann die Faxdaten, erstellt eine Nachricht und stellt diese dem UM-aktivierten Benutzer als E-Mail-Nachricht mit TIF-Anlage zu. Diese Nachrichten werden im Faxsuchordner in Outlook und Outlook Web App angezeigt.

## Sammelanschluss

Ein Satz von Durchwahlnummern, die in einer Gruppe zusammengefasst sind, die von der traditionellen oder SIP-aktivierten PBX- oder IP-PBX-Anlage durchsucht wird, um eine verfügbare Durchwahlnummer zu finden. Ein Sammelanschluss wird verwendet, um Anrufe an Endpunkte mit identischen Funktionsumfängen oder an eine Anwendung wie Voicemail weiterzuleiten.

## Nationales Nummernformat

Das Zahlenformat nationale/regionale gibt an, wie Telefonnummer des Benutzers mit Unified Messaging aus einem Wählplan zu einem anderen Wählplan gewählt werden sollte, die den gleichen Ländercode hat. Dies wird durch eine automatische Telefonzentrale und verwendet, wenn ein Benutzer Outlook Voice Access sucht und versucht, den Benutzer im Verzeichnis aufzurufen. Bei diesem Eintrag besteht aus einem Rufnummernpräfix und einer Variablen Anzahl von Zeichen (beispielsweise 020xxxxxx).

## Informationsansage

Eine Audionachricht, die wiedergegeben wird, wenn sich ein Anrufer zum ersten Mal bei einem

Voicemailsystem einwählt und die einen Belang beschreiben kann.

#### Internationale Kennung

Die Vorwahl, die für internationale Anrufe verwendet wird. Die internationale Kennung ist innerhalb der Vereinigten Staaten "011" und sonst weltweit häufig "00".

#### Internationales Nummernformat

Die Ziffernfolge, mit der definiert wird, wie jemand angewählt wird, der sich außerhalb eines bestimmten Landes befindet.

#### IP-PBX-Anlagen (Internet Protocol Private Branch eXchange)

Eine Telefonvermittlung, die eine systemeigene Unterstützung für VoIP (Voice over IP) bietet. Eine IP-PBX-Anlage verwendet VoIP-basierte Protokolle für die Kommunikation mit IP-basierten Hosts (z. B. VoIP-Telefone) über ein paketvermitteltes Netzwerk. Einige IP-PBX-Anlagen können auch die Verwendung herkömmlicher analoger und digitaler Telefone unterstützen.

#### Auswahlmethode für zugeordnete Namen

Der Mechanismus, der verwendet wird, um einem Anrufer bei der Unterscheidung zwischen Benutzern zu helfen, deren Namen der Tonwahl- oder Spracheingabe entsprechen.

#### MWI (Message Waiting Indicator)

Ein Signal, das die Existenz mindestens einer nicht abgehörten Sprachnachricht anzeigen. Bei Voicemailsystemen ist dies häufig ein Leuchtsignal am Telefon oder ein unterbrochener Wählton.

#### Microsoft Exchange Unified Messaging-Dienst für die Anrufweiterleitung

Ein Dienst, mit dem eingehende Anrufe für UM-aktivierte Benutzer an den Microsoft Exchange Unified Messaging-Dienst weitergeleitet werden.

#### Microsoft Exchange Unified Messaging-Dienst

Ein Dienst, der Unified Messaging-Funktionen für UM-aktivierte Benutzer implementiert.

#### Benachrichtigung über verpasste Anrufe

Eine E-Mail-Nachricht, die an einen UM-aktivierten Benutzer geschickt wird und anzeigt, dass jemand angerufen, aber keine Nachricht hinterlassen hat.

#### Rufnummernpräfix, national

Die Vorwahl, die für nationale Anrufe verwendet wird. In den Vereinigten Staaten ist dies das Präfix 1. In Großbritannien und dem größten Teil der restlichen Welt ist das Präfix 0.

#### Nummernmaske

Eine Reihe von Zahlen und Platzhalterzeichen, mit dem Telefon bestimmen, Zahl, die das Postfach Server einwählen. Eine "X" stellt eine einzelne Ziffer (0 bis 9). Ein Sternchen (\*) stellt eine beliebige Anzahl von solchen

Ziffern.

## Numerische Durchwahl

Eine Ziffernfolge, die kein "+" oder keinen Länder-/Regionalcode enthält. In Wähleinstellungen müssen Durchwahlnummern eine bestimmte Länge besitzen.

## Outdialing

Ein Prozess, in dem Unified Messaging (UM) eine Telefonnummer wählt oder Anrufe vermittelt. Anrufe werden von Unified Messaging grundsätzlich empfangen, doch manchmal wählt UM auch Telefonnummern für Anrufe. So kommt es beispielsweise zum Outdialing, wenn eine automatische Unified Messaging-Telefonzentrale einen Anruf an die Durchwahl eines Benutzers vermittelt oder wenn ein UM-aktivierter Benutzer die "Wiedergabe über Telefon" in Outlook verwendet.

## Outlook Voice Access

Eine Reihe von Sprachansagen, mit denen der authentifizierte Anrufer über ein analoges, digitales oder Mobiltelefon auf E-Mail, Voicemail, den Kalender und die Kontaktinformationen zugreifen kann. Outlook Voice Access ermöglicht authentifizierten Anrufern außerdem mithilfe von MFV-Tasten- oder Spracheingaben die Navigation durch ihre persönlichen Informationen, das Tätigen von Anrufen, das Auffinden von Benutzern sowie das Navigieren durch die Systemansagen und Menüs.

## Amtskennziffer

Das von UM (oder einer Person mit interner Durchwahl in der PBX- oder IP-PBX-Anlage) für den Zugriff auf eine Amtsleitung verwendete Präfix. Diese Vorwahl ist häufig "0" oder "9".

## Paketvermittlung

Die Paketvermittlung ist ein Verfahren, mit dem eine Datennachricht in kleinere Einheiten aufgeteilt wird, die als Pakete bezeichnet werden. Pakete werden über die beste verfügbare Route an ihr Ziel gesendet, wo sie dann beim Empfänger wieder zusammengesetzt werden.

## Pilot-ID

Eine Telefonnummer, die auf einen Sammelanschluss verweist und die Zugriffsnummer für Anrufe ist, die an Unified Messaging weitergeleitet werden. Diese wird manchmal auch als Pilotnummer bezeichnet.

## PIN

Eine Kennung, den ein Benutzer auf dem Telefon eingibt, um auf sein Postfach zuzugreifen.

## Wiedergabe über Telefon

Eine Unified Messaging-Funktion, die Benutzer verwenden können, um ihre Sprachnachrichten abzuspielen oder um personalisierte Voicemailansagen über ein Telefon abzuspielen und aufzuzeichnen.

## PBX-Anlagen (Private Branch eXchange)

Ein privates Telefonnetzwerk in einer Organisation. Einzelne Telefonnummern bzw. Durchwahlen werden unterstützt. An diese werden Anrufe automatisch vermittelt. Benutzer können sich gegenseitig über

Durchwahlnummern anrufen, auch über verteilte Standorte hinweg.

## Ansage

Eine Audionachricht, die am Telefon wiedergegeben wird, um dem Benutzer gültige Optionen zu erläutern.

## Geschützte Voicemail

Eine UM-Funktion, die die Informationsrechteverwaltung zum Verschlüsseln der Inhalte von Sprachnachrichten verwendet und die für diese Sprachnachrichten zulässigen Operationen angibt. Der Schutz kann über eine Anruferaktion (Markierung der Nachricht als "privat") oder durch eine Systemrichtlinie ausgelöst werden.

## Telefonfestnetzanbindung (Public Switched Telephone Network, PSTN)

PSTN ist ein internationaler Zusammenschluss der leitungsvermittelten Telefonnetzwerke. Dieser Zusammenschluss ähnelt dem Internet, das ein internationaler Zusammenschluss der öffentlichen IP-basierten paketvermittelten Netzwerke ist.

## Zurücksetzen

Wenn eine PIN oder ein Kennwort zurückgesetzt wird, wählt das System wahllos eine neue temporäre PIN oder ein Kennwort aus. Der Benutzer muss die temporäre PIN bei der nächsten Anmeldung an Outlook Voice Access ändern.

## Umgekehrte Nummersuche (Reverse Number Lookup, RNL)

Eine Methode, mit der der Name einer Person auf Basis einer Telefonnummer aus einem Verzeichnis oder einem anderen Informationsspeicher ermittelt wird.

## RTAudio-Codec

Ein erweiterter Sprachcodec, der für Zweiwege-VoIP-Echtzeitanwendungen (Voice over IP) wie Spiele, Audiokonferenzen oder drahtlose Anwendungen über IP entwickelt wurde. RTAudio ist der von Microsoft bevorzugte Audiocodec und der Standardcodec für Microsoft Lync Server-Plattformen.

## SIP-aktivierte PBX-Anlage

Eine SIP-aktivierte PBX-Anlage ist ein Telefoniegerät, das in einem Telefonie- oder leitungsvermittelten Netzwerk als Netzwerkvermittlungsstelle oder Vermittlungsstelle für Anrufe fungiert. Der Unterschied zwischen einer SIP-aktivierten PBX-Anlage und einer traditionellen PBX-Anlage besteht jedoch darin, dass mit der SIP-aktivierten PBX-Anlage eine Verbindung mit dem Internet hergestellt werden kann und das SIP-Protokoll für Anrufe über das Internet verfügbar ist.

## SIP-Benachrichtigung

Eine SIP-Benachrichtigung ist eine SIP-Nachricht, die von einem SIP-Peer an einen anderen gesendet wird, um diesen über eine Änderung zu informieren.

## SIP-Peer

Ein SIP-aktiviertes Gerät, mit dem Telefoniekommunikation zwischen einem VoIP-Gateway, IP-PBX-Anlagen,

SIP-aktivierten PBX-Anlagen, Microsoft Lync-Server oder VoIP-Telefonen und UM-Diensten bereitgestellt wird.

#### Unterbrechung durch Sternaste

Eine Aktion, die ein Anrufer ausführen kann, wenn er sich bei einer automatischen Unified Messaging-Telefonzentrale eingewählt hat, aber auf Outlook Voice Access zugreifen möchte, um seine E-Mail und Voicemail abzurufen. Dazu drückt er während der Wiedergabe der Ansagen der automatischen Telefonzentrale auf die Sternaste (\*).

#### Zugriffsnummer des Teilnehmers (Outlook Voice Access-Nummer)

Eine Nummer, die in einer traditionellen oder SIP-aktivierten PBX-Anlage oder IP-PBX-Anlage und in einem UM-Wählplan konfiguriert ist, die den Benutzern den Zugriff auf ihr Outlook-Postfach mithilfe von Voice Access gestattet. In einigen Fällen kann hierfür dieselbe Nummer wie die Zugriffsnummer des Teilnehmers oder Pilotnummer (auch als Pilot-ID bezeichnet) in der traditionellen oder SIP-aktivierten PBX- oder IP-PBX-Anlage und im UM-Sammelanschluss konfiguriert sein.

#### Systemansage

Eine kurze Audioaufzeichnung für Unified Messaging, die vom Server für Anrufer abgespielt wird. Mithilfe von Systemansagen werden Anrufer begrüßt und über ihre Optionen informiert, wenn sie das Voicemailsysteem verwenden.

#### Benutzerschnittstelle für Telefoneingabe (TUI)

Eine Schnittstelle, die zum Navigieren der Menüs eines Voicemailsystems mithilfe von DTMF- oder Tonwahleingaben verwendet wird.

#### Text-to-Speech (TTS, Text-zu-Sprache)

Technologien zum Übersetzen oder Umwandeln von nicht handschriftlichem Text in Sprachausgabe.

#### UM-IP-Gateway

(Siehe IP-Gateway.) Ein UM-IP-Gateway ist die Exchange Unified Messaging-Darstellung eines beliebigen SIP-Peers, mit dem die Kommunikation mithilfe von VoIP-Protokollen möglich wird. Es kann ein Gerät dargestellt werden, das mit einer traditionellen oder SIP-fähigen PBX- oder IP-PBX-Anlage oder mit Microsoft Lync Server kommuniziert.

#### UM-Arbeitsprozesse

Ein Prozess, der während des Starts des Microsoft Exchange Unified Messaging-Diensts erstellt wird. Der UM-Dienst leitet beim Empfangen einer Anforderung zur Bearbeitung eines eingehenden Anrufs diese Anforderung sofort an einen UM-Arbeitsprozess weiter, der alle nachfolgenden Interaktionen mit dem Anrufer übernimmt.

#### UM-Arbeitsprozess-Manager

Eine Komponente, die die Erstellung und Überwachung aller erstellten UM-Arbeitsprozesse übernimmt.

## Unified Messaging

Eine Anwendung, die Voicemail und E-Mail eines Benutzers in einem Postfach konsolidiert, sodass dieser unabhängig vom Nachrichtentyp nur einen einzigen Ort auf Nachrichten überprüfen muss. Der E-Mail-Server wird dabei als Plattform für alle Typen von Nachrichten verwendet, wodurch es überflüssig wird, verschiedene Voicemail- und E-Mail-Infrastrukturen aufrechtzuerhalten.

## Voicemail

Ein System, das Telefonnachrichten in einem Benutzerpostfach aufzeichnet und speichert.

## Voicemailvorschau

Eine Funktion, die von der Audioaufzeichnung transkribierten Text zu einer Sprachnachricht bereitstellt, wenn diese zugestellt wird.

## Sprachnachricht

Eine elektronische Nachricht, deren primärer Inhalt aus digitalisierten Audiodaten besteht.

## VoIP (Voice over IP)

Die Verwendung eines IP-Datennetzwerks, um Sprachanrufe zu übertragen.

## Benutzerschnittstelle für Spracheingabe (Voice User Interface, VUI)

Eine Schnittstelle, die zum Navigieren der Menüs eines Voicemailsystems mithilfe von Spracheingaben verwendet wird.

## VoIP-Gateway

1. Ein Hardwaregerät oder Produkt von Drittanbietern, das eine Verbindung zwischen einer Legacy-PBX-Anlage und einem LAN herstellt. Ein VoIP-Gateway übersetzt oder konvertiert TDM- oder leitungsvermittelte Telefonieprotokolle in paketvermittelte Protokolle, die in einem VoIP-basierten Netzwerk verwendet werden können.
2. Die Exchange Unified Messaging-Darstellung eines beliebigen SIP-Peers, mit dem sie mithilfe von VoIP-Protokollen kommunizieren kann. Es kann ein Gerät dargestellt werden, das mit einer Legacy-PBX- oder IP-PBX-Anlage oder mit Microsoft Lync Server kommuniziert.

## Begrüßung

Eine Begrüßung, die wiedergegeben wird, wenn ein externer Anrufer bei der automatischen UM-Telefonzentrale anruft oder wenn ein Outlook Voice Access-Benutzer oder anderer Anrufer eine Teilnehmerzugriffsnummer anruft, die in einem Satz UM-Wähleinstellungen konfiguriert ist. Die Standardbegrüßungen können von einem Kunden geändert werden, um sie für ein Unternehmen oder einen Standort anzupassen.

# Clients und Mobilgeräte in Exchange Online

18.12.2018 • 2 minutes to read

Es können viele unterschiedliche Clients für den Zugriff auf Informationen in einem Office 365-Postfach verwendet werden. Zu diesen Clients zählen Desktopprogramme wie Microsoft Outlook, Outlook Web App und mobile Clients wie Mobiltelefone, Tablets und andere mobile Geräte. Jeder dieser Clients bietet eine Vielzahl von Features.

## Dokumentation zu Clients und Mobilgeräten

Die folgende Tabelle enthält Links zu Themen, in denen Sie Informationen zu den Clients und Clientzugriffsmethoden finden, die Sie für den Zugriff auf ein Office 365-Postfach verwenden können, sowie zum Verwalten dieser Clients und Clientzugriffsmethoden.

THEMA	BESCHREIBUNG
<a href="#">Exchange ActiveSync</a>	Informieren Sie sich über Exchange ActiveSync, dem Protokoll, das Konnektivität mit den verschiedensten Mobiltelefonen und Tablets bereitstellt. Mit Exchange ActiveSync können Benutzer auf E-Mails, Kalender-, Kontakt- und Aufgabeninformationen zugreifen.
<a href="#">POP3 und IMAP4</a>	Erfahren Sie, wie Sie über das POP3- und das IMAP4-Protokoll Zugriff für Benutzer auf eine Reihe von Funktionen in ihrem Office 365-Postfach bereitstellen können. Diese Clientprotokolle können für E-Mail-Desktopanwendungen und für viele Mobiltelefone und mobile Geräte verwendet werden.
<a href="#">Outlook Web App</a>	Informieren Sie sich über Outlook Web App - die Anwendung, über die Benutzer über einen Webbrower auf ihr Office 365-Postfach zugreifen können.
<a href="#">E-Mail-Info</a>	Informieren Sie sich über E-Mail-Infos, den informativen Meldungen, die Benutzern beim Erstellen einer Nachricht angezeigt werden.

# Exchange ActiveSync in Exchange Online

18.12.2018 • 8 minutes to read

Exchange ActiveSync ist ein Clientprotokoll, über das Sie ein mobiles Gerät mit Ihrem Postfach synchronisieren können.

## Exchange ActiveSync - Übersicht

Exchange ActiveSync ist ein Microsoft Exchange-Synchronisierungsprotokoll, das für die Zusammenarbeit mit Netzwerken mit langer Wartezeit und niedriger Bandbreite optimiert ist. Mithilfe des Protokolls, das auf HTTP und XML basiert, können Mobiltelefone auf die Informationen einer Organisation auf einem Server zugreifen, auf dem Microsoft Exchange ausgeführt wird. Exchange ActiveSync ermöglicht Benutzern von Mobiltelefonen den Zugriff auf ihre E-Mails, ihren Kalender, ihre Kontakte und Aufgaben sowie den Zugriff auf diese Informationen während des Offlinearbeits.

## Features in Exchange ActiveSync

Exchange ActiveSync stellt die folgenden Funktionen bereit:

- Unterstützung für HTML-Nachrichten
- Unterstützung für Nachverfolgungsflag
- Gruppierung von E-Mails nach Unterhaltung
- Möglichkeit zum Synchronisieren einer gesamten Unterhaltung
- Unterstützung für das Anzeigen des Antwortstatus von Nachrichten
- Unterstützung für schnellen Nachrichtenabruf
- Informationen zu Besprechungsteilnehmern
- Erweiterte Exchange-Suche
- PIN-Zurücksetzung
- Optimierte Gerätesicherheit durch Kennwortrichtlinien
- AutoErmittlung für drahtlose Bereitstellung
- Unterstützung für die Einstellung der automatischen Antwortfunktion, wenn Benutzer nicht verfügbar (abwesend, auf Reisen oder nicht im Büro) sind
- Unterstützung für Aufgabensynchronisierung
- Direct Push
- Unterstützung für Verfügbarkeitsinformationen für Kontakte

## Verwalten von Exchange ActiveSync

Standardmäßig ist Exchange ActiveSync aktiviert. Alle Benutzer, die über ein Exchange-Postfach verfügen, können ihre mobilen Geräte mit dem Microsoft Exchange-Server synchronisieren.

Sie können die folgenden Exchange ActiveSync Aufgaben ausführen:

- Aktivieren und Deaktivieren von Exchange ActiveSync für Benutzer
- Festlegen von Richtlinien, wie minimale Kennwortlänge, Gerätesperre und maximale Fehleingaben des Kennworts
- Einleiten eines Remotezurücksetzungsvorgangs zum Löschen aller Daten von einem verlorenen oder gestohlenen Mobiltelefon
- Ausführen einer Vielzahl von Berichten zur Anzeige oder zum Export in verschiedenen Formaten
- Steuerung der mobilen Gerätetypen, die über Gerätezugriffsregeln eine Synchronisierung mit Ihrer Organisation durchführen können

### **Verwalten des Zugriffs über mobile Geräte in Exchange ActiveSync**

Sie können steuern, welche mobilen Geräte eine Synchronisierung durchführen können. Hierzu überwachen Sie neue mobile Geräte bei der Verbindungsherstellung mit Ihrer Organisation, oder Sie richten Regeln ein, mit denen die mobilen Gerätetypen festgelegt werden, die eine Verbindung herstellen dürfen. Unabhängig von der gewählten Methode zur Festlegung der mobilen Geräte, für die eine Synchronisierung zulässig ist, können Sie den Zugriff durch ein spezifisches mobiles Gerät für einen bestimmten Benutzer jederzeit gewähren oder verweigern.

### **Funktionen zur Gerätesicherheit in Exchange ActiveSync**

Über die Möglichkeit hinaus, Sicherheitsoptionen für die Kommunikation zwischen dem Exchange-Server und Ihren mobilen Geräten zu konfigurieren, bietet Exchange ActiveSync die folgenden Features zum Steigern der Sicherheit mobiler Geräte:

- **Remotezurücksetzung:** Wenn ein mobiles Gerät verloren gehen, Diebstahl oder anderweitig gefährdet ausstellen ein Befehls Remotezurücksetzung aus dem Exchange Server-Computer oder von einem beliebigen Webbrowser mithilfe von Outlook Web App. Dieser Befehl löscht alle Daten vom mobilen Gerät.
- **Gerät Kennwortrichtlinien:** Exchange ActiveSync können Sie mehrere Optionen für Gerätekennwörter konfigurieren. Zu diesen Optionen gehören die folgenden:
  - **Minimale Kennwortlänge (Zeichen):** Diese Option gibt die Länge des Kennworts für das mobile Gerät an. Die standardmäßige Länge beträgt 4 Zeichen jedoch bis 18 enthalten sein können.
  - **Minimale Anzahl von Zeichen festgelegt:** Verwenden Sie dieses Textfeld, um die Komplexität der Alphanumerisches Kennwort angeben und erzwingen, dass Benutzer eine Reihe von unterschiedliche Zeichen ein Gerät Folgendes verwenden: Kleinbuchstaben, Großbuchstaben, Symbole und Zahlen .
  - **Alphanumerisches Kennwort:** Diese Option bestimmt, kennwortsicherheit. Sie können die Verwendung eines Zeichens oder Sonderzeichen im Kennwort zusätzlich Zahlen zu erzwingen.
  - **Leerlaufzeit (Sekunden):** Diese Option bestimmt, wie lange das mobile Gerät inaktiv sein muss, bevor der Benutzer, für ein Kennwort aufgefordert wird für das mobile Gerät aufzuheben.
  - **Kennwortchronik erzwingen:** Aktivieren Sie dieses Kontrollkästchen, um das Mobiltelefon, um zu verhindern, dass den Benutzer ihre Kennwörter vorherigen wiederverwenden zu erzwingen. Die Nummer, die Sie festlegen, bestimmt die Anzahl der vergangenen Kennwörter, die der Benutzer wird nicht wiederverwenden.
  - **Kennwortwiederherstellung aktivieren:** Aktivieren Sie dieses Kontrollkästchen, um kennwortwiederherstellung für das mobile Gerät zu aktivieren. Benutzer können Outlook Web App zum Nachschlagen von ihr Wiederherstellungskennwort und Entsperren von ihrem mobilen Gerät verwenden. Administratoren können die Exchange-Verwaltungskonsole zum Nachschlagen des Kennworts eines Benutzers Wiederherstellung verwenden.
  - **Gerät nach (Versuche):** mit dieser Option können Sie angeben, ob der Speicher des Mobiltelefons nach mehreren fehlgeschlagenen Kennworteingaben Kennworteingaben gelöscht werden soll.

- **Verschlüsselung Geräterichtlinien:** Es gibt eine Reihe von Verschlüsselungsrichtlinien für mobile Geräte, die Sie für eine Gruppe von Benutzern erzwingen können. Diese Richtlinien umfassen Folgendes:

- **Verschlüsselung auf dem Gerät erforderlich:** Aktivieren Sie dieses Kontrollkästchen, um die Verschlüsselung auf dem mobilen Gerät. Dies erhöht die Sicherheit durch Verschlüsseln aller Informationen auf dem mobilen Gerät.
- **Verschlüsselung auf Speicherplatten:** Wählen Sie dieses Kontrollkästchen, um die Verschlüsselung auf dem mobilen Gerät austauschbaren Speicherplatte. Dies erhöht die Sicherheit durch Verschlüsseln aller Informationen auf den Speicher des mobilen Geräts.

#### **IMPORTANT**

Obwohl das Exchange ActiveSync-Protokoll für die verschiedenen Features oben aufgeführten unterstützt, liegt es das Mobilgerät-Betriebssystem und Hersteller (OEMs) zum Erstellen von Unterstützung für diese Features in ihre mobile-Betriebssystem und e-Mail-apps (Standard oder Drittanbieter). Nicht alle oben aufgeführten EAS-Funktionen werden von 3. Partei mobile Geräte wie iOS, Android, usw. unterstützt. Microsoft hat keine Kontrolle über die EAS-Features von diesen 3. Mobilgerät Hersteller unterstützt werden. Wenden Sie sich an den Hersteller direkt für die Hilfe in EAS-Features auf mobilen Geräten mit 3. Partei.

# Postfachrichtlinien für mobile Geräte in Exchange Online

18.12.2018 • 14 minutes to read

In Office 365 können Sie Postfachrichtlinien für mobile Geräte erstellen, um eine allgemeine Zusammenstellung von Richtlinien oder Sicherheitseinstellungen auf eine Gruppe von Benutzern anzuwenden. Eine standardmäßige Postfachrichtlinie für mobile Geräte wird in jeder Office 365-Organisation erstellt.

## Übersicht über Postfachrichtlinien für mobile Geräte

Mit Postfachrichtlinien für mobile Geräte können Sie zahlreiche verschiedene Einstellungen verwalten. Hierzu gehören Folgende:

- Kennwort anfordern
- Minimale Kennwortlänge festlegen
- Numerische PIN zulassen oder Sonderzeichen im Kennwort erfordern
- Festlegen, nach welcher Inaktivitätsdauer der Benutzer das Kennwort für das Gerät erneut eingeben muss
- Gerät nach einer bestimmten Anzahl von Fehleingaben des Kennworts vollständig zurücksetzen

## Verwalten von Exchange ActiveSync-Postfachrichtlinien

Postfachrichtlinien für Mobile Geräte können in der Exchange-Verwaltungskonsole (EAC) oder Exchange Online PowerShell erstellt werden. Wenn Sie eine Richtlinie in der Exchange-Verwaltungskonsole erstellen, können Sie nur eine Teilmenge der verfügbaren Einstellungen konfigurieren. Sie können den Rest der Einstellungen von Exchange Online PowerShell konfigurieren.

## Einstellungen für Postfachrichtlinien für mobile Geräte

Die folgende Tabelle enthält eine Zusammenfassung der Einstellungen, die mithilfe von Postfachrichtlinien für mobile Geräte festgelegt werden können.

### Einstellungen für Postfachrichtlinien für mobile Geräte

EINSTELLUNG	BESCHREIBUNG
Bluetooth zulassen	Diese Einstellung gibt an, ob ein mobiles Gerät Bluetooth-Verbindungen zulässt. Die verfügbaren Optionen lauten "Deaktivieren", "Nur Freisprechen" und "Zulassen". Der Standardwert ist "Allow".
Browser zulassen	Diese Einstellung gibt an, ob Pocket Internet Explorer auf dem mobilen Gerät zulässig ist. Diese Einstellung wirkt sich nicht auf dem mobilen Gerät installiert drittanbieterbrowsern aus. Der Standardwert lautet <code>\$true</code> .
Kamera zulassen	Diese Einstellung gibt an, ob die Kamera mobilen Gerät verwendet werden kann. Der Standardwert lautet <code>\$true</code> .

EINSTELLUNG	BESCHREIBUNG
Consumer-E-Mail zulassen	Diese Einstellung bestimmt, ob Benutzer des mobilen Geräts eine persönliche e-Mail-Konto (POP3 oder IMAP4) konfigurieren kann, auf dem mobilen Gerät. Der Standardwert lautet <code>\$true</code> . Diese Einstellung festzulegen nicht Zugriff auf e-Mail-Konten, die mobilen Gerät Drittanbieter-e-Mail-Programme verwenden.
Desktop-Synchronisierung zulassen	Diese Einstellung gibt an, ob das mobile Gerät mit einem Computer über ein Kabel, Bluetooth, synchronisieren kann oder IrDA-Verbindung. Der Standardwert lautet <code>\$true</code> .
Externe Geräteverwaltung zulassen	Diese Einstellung gibt an, ob ein externes Geräteverwaltungsprogramm das mobile Gerät verwalten darf.
E-Mails im HTML-Format zulassen	Diese Einstellung gibt an, ob das mobile Gerät synchronisiert e-Mail im HTML-Format werden kann. Wenn diese Einstellung aktiviert, <code>\$false</code> , alle e-Mails wird in normalen Text konvertiert.
Gemeinsame Nutzung der Internetverbindung zulassen	Diese Einstellung gibt an, ob das mobile Gerät als Modem für eines Desktops oder eines portablen Computers verwendet werden kann. Der Standardwert lautet <code>\$true</code> .
AllowIrDA	Diese Einstellung gibt an, ob Infrarotverbindungen zu und von dem mobilen Gerät zulässig sind.
OTA-Update für mobile Geräte zulassen	Diese Einstellung gibt an, ob die postfachrichtlinieneinstellungen für mobile Geräte über eine mobilfunknetzverbindung an das mobile Gerät gesendet werden können. Der Standardwert lautet <code>true</code> .
Nicht bereitstellbare Geräte zulassen	Diese Einstellung gibt an, ob mobile Geräte, die möglicherweise nicht die Anwendung aller Richtlinieneinstellungen unterstützen, mithilfe von Office 365 eine Verbindung mit Exchange ActiveSync herstellen dürfen. Das Zulassen nicht bereitstellbarer mobiler Geräte hat Auswirkungen auf die Sicherheit. Beispielsweise können auf einigen nicht bereitstellbaren Geräten möglicherweise die Kennwortanforderungen einer Organisation nicht implementiert werden.
POPIMAPEmail zulassen	Diese Einstellung gibt an, ob der Benutzer einen POP3- oder ein IMAP4-e-Mail-Konto auf dem mobilen Gerät konfigurieren kann. Der Standardwert lautet <code>\$true</code> . Diese Einstellung nicht den Zugriff von Drittanbieter-e-Mail-Programmen steuern.
Remotedesktop zulassen	Diese Einstellung gibt an, ob das mobile Gerät eine Remotedesktopverbindung initiieren kann. Der Standardwert lautet <code>\$true</code> .
Einfaches Kennwort zulassen	Diese Einstellung aktiviert oder deaktiviert die Möglichkeit, ein einfaches Kennwort wie 1111 oder 1234 verwenden. Der Standardwert lautet <code>\$true</code> .

EINSTELLUNG	BESCHREIBUNG
Aushandlung des S/MIME-Verschlüsselungsalgorithmus zulassen	Diese Einstellung gibt an, ob die Messaginganwendung auf dem mobilen Gerät den Verschlüsselungsalgorithmus aushandeln kann, wenn das Zertifikat eines Empfängers den angegebenen Verschlüsselungsalgorithmus nicht unterstützt.
S/MIME-Softwarezertifikate zulassen	Diese Einstellung gibt an, ob S/MIME-Softwarezertifikate auf dem mobilen Gerät zulässig sind.
Speicherkarte zulassen	Diese Einstellung gibt an, ob das mobile Gerät auf Informationen zugreifen darf, die auf einer Speicherkarte abgelegt sind.
Textnachrichten zulassen	Diese Einstellung gibt an, ob Text messaging auf dem mobilen Gerät zulässig ist. Der Standardwert lautet <code>\$true</code> .
Nicht signierte Anwendungen zulassen	Diese Einstellung gibt an, ob nicht signierte Anwendungen auf dem mobilen Gerät installiert werden können. Der Standardwert lautet <code>\$true</code> .
Nicht signierte Installationspakete zulassen	Diese Einstellung gibt an, ob eine nicht signierte Installationspaket auf dem mobilen Gerät ausgeführt werden kann. Der Standardwert lautet <code>\$true</code> .
WiFi zulassen	Diese Einstellung gibt an, ob drahtlosen Internetzugriff auf dem mobilen Gerät zulässig ist. Der Standardwert lautet <code>\$true</code> .
Alphanumerisches Kennwort erforderlich	Diese Einstellung erfordert, dass ein Kennwort numerische und nicht-numerische Zeichen enthält. Der Standardwert lautet <code>\$true</code> .
Liste genehmigter Anwendungen	Mit dieser Einstellung wird eine Liste genehmigter Anwendungen gespeichert, die auf dem mobilen Gerät ausgeführt werden dürfen.
Anlagen aktiviert	Diese Einstellung aktiviert, Anlagen auf dem mobilen Gerät heruntergeladen werden. Der Standardwert lautet <code>\$true</code> .
Geräteverschlüsselung aktiviert	Diese Einstellung aktiviert die Verschlüsselung auf dem mobilen Gerät. Nicht alle mobilen Geräte können eine Verschlüsselung erzwingen. Weitere Informationen hierzu finden Sie in der Dokumentation zum Gerät sowie zum mobilen Betriebssystem.
Geräterichtlinien-Aktualisierungsintervall	Diese Einstellung gibt an, wie oft die Postfachrichtlinie für das mobile Gerät vom Server an das mobile Gerät gesendet wird.
IRM aktiviert	Diese Einstellung gibt an, ob auf dem mobilen Gerät die Verwaltung von Informationsrechten (Information Rights Management, IRM) aktiviert ist.
Max. Anlagengröße	Diese Einstellung steuert die maximale Größe von Anlagen, die auf das mobile Gerät heruntergeladen werden können. Der Standardwert ist "Unbegrenzt".

EINSTELLUNG	BESCHREIBUNG
Filter für max. Kalenderalter	<p>Diese Einstellung gibt den maximalen Bereich der Kalendertage an, die auf das mobile Gerät synchronisiert werden können. Die folgenden Werte werden akzeptiert:</p> <ul style="list-style-type: none"> <li>All</li> <li>OneDay</li> <li>ThreeDays</li> <li>OneWeek</li> <li>TwoWeeks</li> <li>OneMonth</li> </ul>
Filter für max. E-Mail-Alter	<p>Mit dieser Einstellung wird die maximale Anzahl von Tagen angegeben, für die E-Mail-Elemente auf das mobile Gerät synchronisiert werden. Die folgenden Werte werden akzeptiert:</p> <ul style="list-style-type: none"> <li>All</li> <li>OneDay</li> <li>ThreeDays</li> <li>OneWeek</li> <li>TwoWeeks</li> <li>OneMonth</li> </ul>
Max. Größe für E-Mail-Textkörperkürzung	<p>Mit dieser Einstellung wird die maximale Größe angegeben, bei der E-Mail-Nachrichten bei der Synchronisierung auf das mobile Gerät abgeschnitten werden. Der Wert wird in Kilobytes (KB) angegeben.</p>
Max. Größe für E-Mail-Textkörperkürzung, HTML	<p>Mit dieser Einstellung wird die maximale Größe angegeben, bei der E-Mail-Nachrichten im HTML-Format bei der Synchronisierung auf das mobile Gerät abgeschnitten werden. Der Wert wird in Kilobytes (KB) angegeben.</p>
Zeitsperre für max. Inaktivität	<p>Dieser Wert gibt an, wie lange das mobile Gerät inaktiv sein kann, bevor es mithilfe eines Kennworts erneut aktiviert werden muss. Sie können ein Intervall zwischen 30 Sekunden und einer Stunde eingeben. Der Standardwert beträgt 15 Minuten.</p>
Max. fehlgeschlagene Kennwortversuche	<p>Diese Einstellung gibt die Anzahl von Versuchen an, die einem Benutzer zur Verfügung stehen, um das korrekte Kennwort für das Gerät einzugeben. Sie können einen Wert von 4 bis 16 eingeben. Der Standardwert ist 8.</p>
Min. komplexe Zeichen im Kennwort	<p>Diese Einstellung gibt die Mindestanzahl von komplexen Zeichen an, die für das Kennwort des Mobiltelefons erforderlich sind. Komplexe Zeichen sind Zeichen, die keine Buchstaben sind.</p>
Min. Kennwortlänge	<p>Diese Einstellung gibt die Mindestanzahl der Zeichen für das Kennwort des mobilen Geräts an. Sie können einen Wert von 1 bis 16 eingeben. Der Standardwert ist 4.</p>
Kennwort aktiviert	<p>Diese Einstellung aktiviert das Kennwort für das mobile Gerät.</p>
Kennwortablauf	<p>Diese Einstellung ermöglicht dem Administrator das Konfigurieren eines Zeitraums, nach dem das Kennwort für das mobile Gerät geändert werden muss.</p>

EINSTELLUNG	BESCHREIBUNG
Kennwortverlauf	Diese Einstellung gibt die Anzahl der letzten Kennwörter an, die im Postfach eines Benutzers gespeichert werden dürfen. Ein gespeicherte Kennwort kann vom Benutzer nicht erneut verwendet werden.
Kennwortwiederherstellung aktiviert	Wenn diese Einstellung aktiviert ist, generiert das mobile Gerät ein Wiederherstellungskennwort, das an den Server gesendet wird. Wenn ein Benutzer das Kennwort für das mobile Gerät vergisst, kann die Sperrung des mobilen Geräts mithilfe des Wiederherstellungskennworts aufgehoben werden. Der Benutzer kann dann ein neues Kennwort für das mobile Gerät erstellen.
Geräteverschlüsselung anfordern	Diese Einstellung gibt an, ob das Geräteverschlüsselung erforderlich ist. Wenn auf festgelegt <code>\$true</code> , muss das mobile Gerät unterstützen und implementieren Sie die Verschlüsselung mit dem Server synchronisieren können.
Verschlüsselte S/MIME-Nachrichten anfordern	Diese Einstellung gibt an, ob S/MIME-Nachrichten verschlüsselt werden müssen. Der Standardwert lautet <code>\$false</code> .
S/MIME-Verschlüsselungsalgorithmus anfordern	Mit dieser Einstellung wird angegeben, welcher erforderliche Algorithmus beim Verschlüsseln von S/MIME-Nachrichten verwendet werden muss.
Manuelle Synchronisierung beim Roaming anfordern	Diese Einstellung gibt an, ob das mobile Gerät beim Roaming manuell synchronisiert werden muss. Das Zulassen der automatischen Synchronisierung beim Roaming führt häufig zu höheren Datenkosten für den Datentarif des mobilen Geräts als erwartet.
Algorithmus für signiertes S/MIME anfordern	Mit dieser Einstellung wird angegeben, welcher erforderliche Algorithmus beim Signieren einer Nachricht verwendet werden muss.
Signierte S/MIME-Nachrichten anfordern	Mit dieser Einstellung wird angegeben, ob das mobile Gerät nur signierte S/MIME-Nachrichten versenden darf.
Verschlüsselung der Speicherkarte anfordern	Diese Einstellung gibt an, ob die Speicherkarte verschlüsselt werden muss. Nicht alle Betriebssysteme für mobile Geräte unterstützen die Verschlüsselung von Speicherkarten. Weitere Informationen hierzu finden Sie in der Dokumentation zum mobilen Gerät sowie zum mobilen Betriebssystem.
Liste nicht genehmigter InROM-Anwendungen	Diese Einstellung gibt eine Liste von Anwendungen an, die nicht im ROM ausgeführt werden dürfen.

# POP3 und IMAP4

18.12.2018 • 10 minutes to read

**Zusammenfassung:** Eine Übersicht über POP3 und IMAP4 und die Unterschiede zwischen beiden.

Standardmäßig sind POP3 und IMAP4 für alle Benutzer in Exchange Online aktiviert.

- Zum Aktivieren oder Deaktivieren von POP3 und IMAP4 für einzelne Benutzer, finden Sie unter [Aktivieren oder Deaktivieren von POP3 oder IMAP4-Zugriffs für einen Benutzer](#).
- Unter [Festlegen von POP3- oder IMAP4-Einstellungen für einen Benutzer](#) erfahren Sie, wie Sie die Einstellungen für POP3 und IMAP4 für einzelne Benutzer personalisieren können.

Benutzer können jedes beliebige E-Mail-Programm verwenden, das POP3 und IMAP4 unterstützt, um sich mit Exchange Online zu verbinden. Zu diesen Programmen gehören Outlook, Microsoft Outlook Express, Entourage und E-Mail-Programme von Drittanbietern wie Mozilla Thunderbird und Eudora. Die von den einzelnen E-Mail-Clientanwendungen unterstützten Funktionen variieren. Informationen zu den jeweiligen Funktionen, die von bestimmten POP3- und IMAP4-Clientanwendungen zur Verfügung gestellt werden, finden Sie in der jeweiligen Dokumentation zur betreffenden Anwendung.

POP3 und IMAP4 bieten Zugriff auf die grundlegenden E-Mail-Funktionen von Exchange Online und ermöglichen Offline-Zugriff auf E-Mails. Umfassende Funktionen wie Kalendereinträge, Kontaktverwaltung und sonstige Funktionen, die verfügbar sind, wenn Benutzer sich über Outlook, Exchange ActiveSync, Outlook Web App oder Outlook Voice Access anmelden, stehen jedoch nicht zur Verfügung.

## NOTE

Immer wenn ein Benutzer ein POP- oder IMAP-basiertes E-Mail-Programm zum Öffnen seiner Office 365-E-Mail nutzt, kommt es zu einer mehrsekündigen Verzögerung. Deren Ursache ist die Verwendung eines Proxyservers, der einen weiteren Hop für die Authentifizierung hinzufügt. Der Proxyserver untersucht zunächst den zugewiesenen PoD-Server (Clientzugriffsserver), bei dem eine Authentifizierung erfolgt.

## Benutzereinstellungen zur Einrichtung von POP3- oder IMAP4-Zugriff auf Exchange-Online-Postfächern

Nachdem Sie den POP3- und IMAP4-Clientzugriff aktiviert haben, müssen Sie den Benutzern die Informationen aus der folgenden Tabelle an die Hand geben, damit sie ihre E-Mail-Programme mit ihrem Exchange Online-Postfach verbinden können.

POP3- und IMAP4-E-Mail-Programme verwenden zum Versenden von Nachrichten an den E-Mail-Server weder POP3 noch IMAP4. E-Mail-Programme, die POP3 und IMAP4 verwenden, versenden Nachrichten mit dem SMTP-Protokoll.

	SERVERNAME	PORT	VERSCHLÜSSELUNGSMETHODEN
POP3	Outlook.Office365.com	995	TLS
IMAP4	Outlook.Office365.com	993	TLS
SMTP	SMTP.Office365.com	587	TLS

# Grundlegendes zu den Unterschieden zwischen POP3 und IMAP4

Wenn POP3-E-Mail-Programme E-Mails auf einen Clientcomputer herunterladen, werden die heruntergeladenen Nachrichten standardmäßig vom Server entfernt. Wenn keine Kopien der E-Mails des Benutzers auf dem E-Mail-Server gespeichert werden, kann der Benutzer nicht von mehreren Computern aus auf diese E-Mails zugreifen. Einige POP3-E-Mail-Programme können jedoch so konfiguriert werden, dass Kopien der Nachrichten auf dem Server gespeichert werden, damit von anderen Computern aus der Zugriff auf die E-Mails möglich ist. POP3-Clientprogramme können nur zum Herunterladen von Nachrichten vom E-Mail-Server in einen einzigen Ordner (in der Regel in den Ordner "Posteingang") auf dem Clientcomputer verwendet werden. Das POP3-Protokoll kann mehrere Ordner auf dem E-Mail-Server nicht mit mehreren Ordner auf dem Clientcomputer synchronisieren. POP3 unterstützt außerdem keinen Zugriff auf öffentliche Ordner.

E-Mail-Clientprogramme, die IMAP4 verwenden, sind flexibler und bieten im Allgemeinen eine größere Anzahl an Funktionen als E-Mail-Clientprogramme, die POP3 verwenden. Wenn IMAP4-E-Mail-Programme E-Mails auf einen Clientcomputer herunterladen, verbleibt standardmäßig eine Kopie der heruntergeladenen Nachrichten auf dem E-Mail-Server. Da eine Kopie der E-Mails des Benutzers auf dem E-Mail-Server gespeichert wird, kann der Benutzer von mehreren Computern aus auf diese E-Mails zugreifen. Bei Verwendung von IMAP4 kann der Benutzer auf mehrere E-Mail-Ordner auf dem E-Mail-Server zugreifen bzw. mehrere dieser Ordner erstellen. Die Benutzer können dann auf alle Nachrichten auf dem Server von Computern an mehreren Standorten aus zugreifen. Die meisten IMAP4-Anwendungen können z. B. so konfiguriert werden, dass eine Kopie der gesendeten Elemente des Benutzers auf dem Server verbleibt, damit die gesendeten Elemente auf einem beliebigen anderen Computer angezeigt werden können. IMAP4 unterstützt zusätzliche Funktionen, die von den meisten IMAP4-Anwendungen unterstützt werden. Einige IMAP4-Programme enthalten z. B. eine Funktion, mithilfe derer Benutzer nur die Kopfzeilen ihrer E-Mails (Absender und Betreff der Nachricht) auf dem Server anzeigen und anschließend nur die Nachrichten herunterladen können, die sie lesen möchten.

## Sende- und Empfangsoptionen für POP3- und IMAP4-E-Mail-Programme

Mit POP3- und IMAP4-E-Mail-Programmen können Benutzer auswählen, wann eine Verbindung mit dem Server zum Senden und Empfangen von E-Mails hergestellt werden soll. In diesem Abschnitt werden einige der gängigsten Konnektivitätsoptionen behandelt. Außerdem werden einige Aspekte erläutert, die Ihre Benutzer beim Auswählen der Verbindungsoptionen in ihren POP3- und IMAP4-E-Mail-Programmen berücksichtigen sollten.

### Allgemeine Konfigurationseinstellungen

Drei der am häufigsten verwendeten Verbindungseinstellungen können wie folgt für eine POP3- oder IMAP4-Clientanwendung festgelegt werden:

- Senden und Empfangen von Nachrichten bei jedem Start der E-Mail-Anwendung. Bei Verwendung dieser Option werden E-Mails nur beim Start der E-Mail-Anwendung gesendet und empfangen.
- Manuelles Senden und Empfangen von Nachrichten. Bei Verwendung dieser Option werden Nachrichten nur dann gesendet und empfangen, wenn der Benutzer auf den Befehl Senden und Empfangen in der Clientbenutzeroberfläche klickt.
- Senden und Empfangen von Nachrichten immer nach einer festgelegten Anzahl von Minuten. Bei Verwendung dieser Option stellt die Clientanwendung immer nach Ablauf eines in Minuten festgelegten Zeitraums eine Verbindung mit dem Server her, um Nachrichten zu senden und neue Nachrichten herunterzuladen.

Informationen zum Konfigurieren dieser Einstellungen für die von Ihnen verwendete E-Mail-Anwendung finden Sie in der Hilfedokumentation zur jeweiligen E-Mail-Anwendung.

### Überlegungen bei der Auswahl von Sende- und Empfangsoptionen

Einige E-Mail-Programme sind standardmäßig so eingestellt, dass sie nach dem Abrufen von Nachrichten keine Kopien der Nachrichten auf dem Server beibehalten. Wenn Benutzer über mehrere E-Mail-Programme oder Geräte auf ihre Nachrichten zugreifen möchten, sollten sie darauf achten, dass eine Kopie auf dem Server gespeichert wird.

Wenn das Gerät oder der Computer, auf dem eine POP3- oder IMAP4-E-Mail-Anwendung ausgeführt wird, immer mit dem Internet verbunden ist, möchten Benutzer ihre E-Mail-Anwendung ggf. so konfigurieren, dass Nachrichten in einem festgelegten Minutenintervall gesendet und empfangen werden. Durch regelmäßige Verbindungen mit dem Server wird sichergestellt, dass die E-Mail-Anwendung des Benutzers mit den neuen Informationen auf dem Server aktualisiert wird. Wenn das Gerät oder der Computer, auf dem eine POP3- oder IMAP4-E-Mail-Anwendung ausgeführt wird, nicht immer mit dem Internet verbunden ist, möchten Benutzer ihre E-Mail-Anwendung ggf. so konfigurieren, dass Nachrichten manuell gesendet und abgerufen werden.

**NOTE**

Wenn der Benutzer eine mit IMAP4 kompatible E-Mail-Anwendung verwendet, die den Befehl "IMAP4 IDLE" unterstützt, ist er ggf. in der Lage, E-Mails nahezu in Echtzeit an das Exchange-Postfach zu senden und von diesem zu empfangen. Damit diese Verbindungsmethode funktioniert, müssen sowohl die E-Mail-Server- als auch die Clientanwendung den Befehl "IMAP4 IDLE" unterstützen. In den meisten Fällen müssen Benutzer keine Einstellungen in ihrem IMAP4-Programm konfigurieren, um diese Verbindungsmethode verwenden zu können.

# Aktivieren oder Deaktivieren des POP3- oder IMAP4-Zugriffs für einen Benutzer

18.12.2018 • 4 minutes to read

Standardmäßig sind POP3 und IMAP4 für alle Benutzer in Exchange Online aktiviert. Sie können sie für einzelne Benutzer deaktivieren. Weitere Informationen im Zusammenhang mit POP3 und IMAP4 finden Sie unter [POP3 und IMAP4](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Ende: zwei Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter Abschnitt "POP3- und IMAP4-Einstellungen" im Thema [Featureberechtigungen in Exchange Online](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aktivieren oder Deaktivieren von POP3 oder IMAP4 für einen Benutzer mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Klicken Sie im Ergebnisbereich wählen Sie den Benutzer, für den Sie POP3 aktivieren oder deaktivieren möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Dialogfeld **Benutzerpostfach** in die Konsolenstruktur und dann auf **Postfachfeatures**.
4. Gehen Sie im Ergebnisbereich unter **E-Mail-Konnektivität** wie folgt vor:
  - Klicken Sie zum Aktivieren von POP3 für den Benutzer unterhalb von **POP3: Deaktiviert** auf **Aktivieren**.
  - Klicken Sie zum Aktivieren von IMAP4 für den Benutzer unterhalb von **IMAP4: Deaktiviert** auf **Aktivieren**.
  - Klicken Sie zum Deaktivieren von POP3 für den Benutzer, unterhalb von **POP3: Aktiviert** auf **Deaktivieren**.
  - Klicken Sie zum Deaktivieren von IMAP4 für den Benutzer unterhalb von **IMAP4: Aktiviert** auf **Deaktivieren**.
5. Klicken Sie auf **Speichern**.

## Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren von POP3 oder IMAP4 für einen Benutzer

In diesem Beispiel wird POP3 für den Benutzer "Christa Knapp" aktiviert.

```
Set-CASMailbox -Identity "Christa Knapp" -POPEnabled $true
```

Im folgenden Beispiel wird IMAP4 für den Benutzer John Smith aktiviert.

```
Set-CASMailbox -Identity "Christa Knapp" -IMAPEnabled $true
```

Im folgenden Beispiel wird POP3 für den Benutzer John Smith deaktiviert.

```
Set-CASMailbox -Identity "Christa Knapp" -POPEnabled $false
```

In diesem Beispiel wird IMAP4 für den Benutzer John Smith deaktiviert.

```
Set-CASMailbox -Identity "Christa Knapp" -IMAPEnabled $false
```

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Wählen Sie im Ergebnisbereich den Benutzer aus, für den Sie POP3 oder IMAP4 aktivieren oder deaktivieren möchten, und klicken Sie dann auf **Bearbeiten**.
3. Klicken Sie im Dialogfeld **Benutzerpostfach** in die Konsolenstruktur und dann auf **Postfachfeatures**.
4. Sehen Sie im Ergebnisbereich unter **E-Mail-Konnektivität** nach.
  - Wenn POP3 für den Benutzer deaktiviert ist, sehen Sie die Anzeige **POP3: Deaktiviert**.
  - Wenn IMAP4 für den Benutzer deaktiviert ist, sehen Sie die Einstellung **IMAP4: Deaktiviert**.
  - Wenn POP3 für den Benutzer aktiviert ist, sehen Sie die Einstellung **POP3: Aktiviert**.
  - Wenn IMAP4 für den Benutzer aktiviert ist, sehen Sie die Einstellung **IMAP4: Aktiviert**.
5. Klicken Sie auf **Speichern**.

# Festlegen von POP3- oder IMAP4-Einstellungen für einen Benutzer

18.12.2018 • 9 minutes to read

Das Cmdlet **Set-CASMailbox** wird verwendet, um die PO3- und IMAP4-Optionen für jeden Benutzer zu konfigurieren. Die Konfigurationsoptionen werden in der folgenden Tabelle beschrieben.

PARAMETER	BESCHREIBUNG	WERTE
<i>PopForceICalForCalendarRetrievalOption</i> <i>ImapForceICalForCalendarRetrievalOption</i>	Legt das bevorzugte Format für Besprechungsanfragen fest. Standardmäßig erscheinen Besprechungsanfragen als Outlook Web App-Links. Sie können sie in das iCal-Format ändern.	<code>\$true</code> : Besprechungsanfragen werden alle Outlook Web App-links <code>\$false</code> : Besprechungsanfragen werden alle iCal-format
<i>PopSuppressReadReceipt</i> <i>ImapSuppressReadReceipt</i>	Legt fest, ob Lesebestätigungen gesendet werden sollen, wenn eine Nachricht heruntergeladen wird und wenn sie geöffnet wird, oder nur, wenn die Nachricht geöffnet wird. Standardmäßig werden, wenn Lesebestätigungen gefordert sind, zwei Lesebestätigungen gesendet: eine, wenn ein Benutzer eine Nachricht herunterlädt, und eine weitere, wenn er die Nachricht öffnet. Sie können dies so ändern, dass nur eine Lesebestätigung gesendet wird: dann, wenn der Empfänger die Nachricht öffnet.	<code>\$false</code> : POP3- oder IMAP4-Benutzer werden eine lesebestätigung jedes Mal gesendet eine Nachricht ein Empfänger heruntergeladen wird. Benutzer werden auch eine lesebestätigung gesendet, wenn der Benutzer die Nachricht öffnet. Dies ist die Standardeinstellung. <code>\$true</code> : POP3- oder IMAP4-Benutzer, die verwenden die Option <b>Senden lesebestätigung für meiner gesendeten Nachrichten</b> in ihrem e-Mail-Client, empfangen eine lesebestätigung nur, wenn der Empfänger die Nachricht öffnet.
<i>PopMessagesRetrievalMimeType</i> <i>ImapMessagesRetrievalMimeType</i>	Legt das bevorzugte Format für empfangene Nachrichten fest. Die Standardeinstellung ist die Verwendung des für die jeweilige Nachricht besten Formats.	Verwenden einer Zahl oder eines Textwerts. 0 oder <code>TextOnly</code> : nur-Text 1 oder <code>HtmlOnly</code> : HTML 2 oder <code>HtmlAndTextAlternative</code> : HTML und alternativen Text 3 oder <code>TextEnriched</code> : Enriched Text 4 oder <code>TextEnrichedAndTextAlternative</code> : Enriched Text und alternativen Text 5 oder <code>BestBodyFormat</code> : beste Textformat. Dies ist der Standardwert. 6 oder <code>Tnef</code> : Transport-Neutral Encapsulation Format (TNEF). Auch bekannt als RTF-Format, Outlook-rich-Text-Format oder MAPI-RTF-Format.

PARAMETER	BESCHREIBUNG	WERTE
<code>PopEnableExactRFC822Size</code> <code>ImapEnableExactRFC822Size</code>	Legt fest, ob die genaue Größe der Nachrichten berechnet wird. Es wird nicht empfohlen, diesen Wert zu ändern, außer wenn der Standardwert Probleme für Ihren E-Mail-Client verursacht. Standardmäßig wird statt der exakten Nachrichtengröße die geschätzte Nachrichtengröße an den E-Mail-Client gesendet.	<code>\$true</code> : Verwenden Sie tatsächlichen Nachrichtengröße. <code>\$false</code> : Verwendung geschätzte Nachrichtengröße. Dies ist die Standardeinstellung.

Weitere Informationen zu POP3 und IMAP4 finden Sie unter [POP3 und IMAP4](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Sie können nur Exchange Online PowerShell verwenden, um dieses Verfahren ausführen. So verwenden Sie Windows PowerShell für die Verbindung zu Exchange Online finden Sie unter [Connect to Exchange Online PowerShell](#).
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter Eintrag "POP3- und IMAP4-Einstellungen" im Thema [Featureberechtigungen in Exchange Online](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden Sie Exchange Online PowerShell, um die Besprechung festzulegen Anforderungsformular für einen POP3- oder IMAP4-Benutzer

Im folgenden Beispiel werden alle Besprechungsanfragen in eingehenden Mails für USER01 in das iCal-Format für POP3-Benutzer umgewandelt.

```
Set-CASMailbox USER01 -PopUseProtocolDefaults $false -PopForceICalForCalendarRetrievalOption $true
```

Im folgenden Beispiel werden alle Besprechungsanfragen in eingehenden Mails für USER01 in das iCal-Format für IMAP4-Benutzer umgewandelt.

```
Set-CASMailbox USER01 -ImapUseProtocolDefaults $false -ImapForceICalForCalendarRetrievalOption $true
```

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie erfolgreich die Besprechungsfrage festlegen Format für einen POP3- oder IMAP4-Benutzer, führen den folgenden Befehl in Exchange Online PowerShell, und stellen Sie sicher, dass die Werte angezeigt werden die Werte, die Sie konfiguriert haben:

```
Get-CASMailbox USER01 | format-list *ForceIcal*, *UseProtocolDefaults
```

## Verwenden Sie Exchange Online PowerShell, um das Lesen des Empfangs-Option für einen POP3- oder IMAP4-Benutzer unterdrücken festzulegen

Im folgenden Beispiel wird diese Option so eingestellt, dass der POP3-Absender nur dann eine Lesebestätigung erhält, wenn die Nachricht geöffnet wird.

```
Set-CASMailbox USER01 -PopUseProtocolDefaults $false -PopSuppressReadReceipt $true
```

Im folgenden Beispiel wird diese Option so eingestellt, dass der IMAP4-Absender nur dann eine Lesebestätigung erhält, wenn die Nachricht geöffnet wird.

```
Set-CASMailbox USER01 -ImapUseProtocolDefaults $false -ImapSuppressReadReceipt $true
```

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie die Option lesebestätigung für einen POP3- oder IMAP4-Benutzer ordnungsgemäß festgelegt, führen Sie den folgenden Befehl in Exchange Online PowerShell, und stellen Sie sicher, dass die angezeigten Werte den Werten sind, die Sie konfiguriert haben:

```
Get-CASMailbox USER01 | format-list *SuppressReadReceipt,*UseProtocolDefaults
```

## Verwenden von Exchange Online PowerShell Festlegen des Nachrichtenformats Retrieval für ein POP3- oder IMAP4-Benutzer

Im folgenden Beispiel wird das Nachrichtenformat Retrieval Text nur für POP3-Zugriffs für `USER01`.

```
Set-CASMailbox USER01 -PopUseProtocolDefaults $false -PopMessagesRetrievalMimeTypeFormat TextOnly
```

Im folgenden Beispiel wird das Nachrichtenformat Retrieval Text nur für IMAP4-Zugriff für `USER01`.

```
Set-CASMailbox USER01 -ImapUseProtocolDefaults $false -ImapMessagesRetrievalMimeTypeFormat TextOnly
```

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sicherzustellen, dass Sie das Nachrichtenformat Abruf erfolgreich für einen POP3- oder IMAP4-Benutzer festlegen, führen Sie den folgenden Befehl in Exchange Online PowerShell, und stellen Sie sicher, dass die angezeigten Werte den Werten sind, die Sie konfiguriert haben:

```
Get-CASMailbox USER01 | format-list *MessagesRetrievalMimeTypeFormat,*UseProtocolDefaults
```

## Verwenden von Exchange Online PowerShell legen Sie die Berechnung der Nachricht Größe für einen POP3- oder IMAP4-Benutzer fest

In diesem Beispiel wird die exakte Größe von POP-Nachrichten für `USER01` berechnet.

**IMPORTANT**

Legen Sie den Parameter *PopEnableExactRFC822Size* auf `$true` nur, wenn der Client POP für diesen Benutzer nicht funktioniert.

```
Set-CASMailbox USER01 -PopUseProtocolDefaults $false -PopEnableExactRFC822Size $true
```

In diesem Beispiel wird die exakte Größe von IMAP-Nachrichten für USER01 berechnet.

**IMPORTANT**

Legen Sie den Parameter *ImapEnableExactRFC822Size* auf `$true` nur, wenn Sie der IMAP-Client für diesen Benutzer nicht funktioniert.

```
Set-CASMailbox USER01 -ImapUseProtocolDefaults $false -ImapEnableExactRFC822Size $true
```

**Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Um sicherzustellen, dass Sie erfolgreich die Nachricht Größe Berechnung für einen POP3- oder IMAP4-Benutzer festlegen, führen Sie den folgenden Befehl in Exchange Online PowerShell, und stellen Sie sicher, dass die angezeigten Werte den Werten sind, die Sie konfiguriert haben:

```
Get-CASMailbox USER01 | format-list *EnableExact*,*UseProtocolDefaults
```

## Weitere Informationen

[Herstellen einer Verbindung mit Exchange Online mithilfe der Remote-PowerShell](#)

[POP3 und IMAP4](#)

[Aktivieren oder Deaktivieren von POP3 oder IMAP4-Zugriffs für einen Benutzer](#)

[Set-CASMailbox](#)

# Outlook for iOS and Android in Exchange Online

18.12.2018 • 7 minutes to read

Die Outlook-app für iOS und Android ist darauf ausgelegt, e-Mail, Kalender, Kontakte und andere Dateien, Aktivieren von Benutzern in Ihrer Organisation zu bewältigen zusammengefügt von ihren mobilen Geräten. Dieser Artikel enthält eine Übersicht über die Architektur, damit Office 365-Administratoren bereitstellen und Verwalten von Outlook für iOS und Android in ihren Organisationen können.

## NOTE

Benutzern steht das [Outlook für iOS und Android-Hilfe-Center](#) zur Verfügung. Hier finden sie unter anderem gerätespezifische Hilfestellung bei der Verwendung der App sowie Informationen zur Problembehandlung.

## Architektur von Outlook für iOS und Android

Outlook für iOS und Android-app wird von der Microsoft-Cloud vollständig bereitgestellt. Alle Office 365 Enterprise, Geschäfts- und Bildungseinrichtungen Konten werden systemintern unterstützt, unterstützt die bedeutet, dass keine Postfachdaten außerhalb von Office 365 zwischengespeichert ist. Daten einfach in seiner aktuellen Exchange Online-Postfachs bleibt und durch eine sichere TLS-Verbindungen End-to-End, zwischen Office 365 und die App für iOS Outlook geschützt und Android wird vollständig über Microsoft-Dienste, die Verpflichtung an bereitstellen zugestellt Sicherheit, Datenschutz und Compliance.

Die Office 365-basierte Architektur bietet die folgenden Vorteile:

1. **Daten Equal:** Benutzer von Postfachdaten direkten bleibt, und daher weiterhin Daten Equal und Regionality Versprechen der Office 365 für Daten im Ruhezustand berücksichtigen. Anders ausgedrückt, werden Daten im Postfach des Benutzers innerhalb der Region gespeichert, in der sich der Mandant befindet.
2. **Geräte-ID:** jede Outlook für iOS und Android-Verbindung in der Verwaltungskonsole von Office 365 registriert und ist berechtigt, die als eine eindeutige Verbindung verwaltet werden.
3. **Moderne Authentifizierung (OAuth):** Outlook für iOS und Android nutzt modernen Authentifizierung (OAuth) zum Schutz der Anmeldeinformationen des Benutzers. Moderne Authentifizierung bietet Outlook für iOS und Android einen sicheren Mechanismus für den Zugriff auf Office 365-Daten ohne je Anmeldeinformationen des Benutzers. Beim Anmelden, den Benutzer authentifiziert direkt mit einer Identitätsplattform (entweder Azure AD oder lokalen Identitätsanbieter wie AD FS) und erhält ein Zugriffstoken in zurück, welche gewährt Outlook für iOS und Android den Zugriff auf Postfach oder Dateien des Benutzers. Zu keiner Zeit ist der Dienst im keinerlei Zugriff auf das Kennwort des Benutzers vorhanden.
4. **Unterstützung von Enterprise Mobility + Security:** Kunden können die Vorteile von Microsoft Enterprise Mobility + Security (EMS) einschließlich Microsoft Intune und Azure Active Directory Premium nutzen, um bedingten Zugriff und Intune-App-Schutzrichtlinien zu aktivieren, die Nachrichtendaten von Unternehmen auf dem mobilen Gerät kontrollieren und sichern.

## Daten Synchronisierungsprotokoll

In der Office 365-basierte Architektur ist Outlook für iOS und Android eine der zwei unterschiedliche Daten Synchronisierung Protokolle nutzen:

- eine proprietäre Gerät API + REST-API
- eine systemeigene Microsoft Sync-Technologie

Heute, die Mehrheit der Konten, die mit Outlook für iOS und Android verbinden über eine statusfreie Protokoll Translator-Komponente, die erstellt und in Azure ausgeführt wird. Diese Komponente leitet Daten und Befehle übersetzt, aber es keine Benutzerdaten zwischengespeichert. Die app wird mit dem Outlook-Gerät API, eine proprietäre codiert, die API, die Befehle und Daten zu und von der App Exchange Online-Daten synchronisiert wird über den öffentlich zugänglichen REST-APIs zugegriffen werden kann. Das Konvertierungsprogramm Protokoll ermöglicht die Kommunikation zwischen Outlook und Exchange Online.



Dezember 2018 ab, wird Microsoft Kunden auf eine systemeigene Microsoft Sync-Technologie migrieren, die die statusfreie Protokoll Translator-Komponente aus die Office 365-basierte Architektur entfernt. Mit der systemeigenen Microsoft Sync-Technologie verbindet Outlook für iOS und Android direkt mit Office 365 für datenverbindungen stellt sicher, dass die Daten durch eine HTTP-TLS-gesicherte Verbindung verwenden End-to-End geschützt ist.



Die systemeigene Microsoft Sync-Technologie bietet mehrere Vorteile:

1. **Eliminiert mittlere Ebene Services:** Daten mit der systemeigenen Microsoft Sync-Technologie Synchronisierung zwischen der app und Office 365, den Wegfall von middle-Tier-Dienste.
2. **Verringerung der Wartezeit:** durch die Proprietary Outlook Gerät API und statusfreie Protokoll Translator ersetzen, eine Verringerung der End-to-End-Wartezeit zwischen der app und Office 365 vorhanden ist.
3. **Zusätzliche Office 365-Instanz unterstützt:** Entfernen von zwischengeschaltete statusfreie Protokoll Konverter für datenverbindungen mit der Microsoft Unterstützung für andere eindeutigen Office 365-Instanzen, wie Office 365 Government Community Cloud hohe und Office 365 Verteidigungsministeriums, die zuvor aus mit Outlook für iOS und Android blockiert wurden.
4. **Protokoll Konsolidierung:** heute, jede Outlook-Client-Plattform eine andere Daten Sync-Protokoll, das behindert Innovationen und schnelle Bereitstellung von neuen Features für alle Outlook-Clients verwendet. Das systemeigene Microsoft Sync-Technologie, die Outlook für iOS und Android Übernahme ist von der systemeigenen Windows 10 e-Mail-Client für eine Anzahl von Jahren und in der Zukunft verwendet wurde wird von Outlook für Mac verwendet werden
5. **Neue Features entsperren:** die systemeigene Microsoft Sync-Technologie wird Outlook für iOS und Android systemeigene Office 365-Features nutzen wird nicht unterstützt heute wie S/MIME, Microsoft Information Protection beschriften und shared aktivieren Postfächer. Diese und weitere Features von Office 365 werden bald nach der Aktualisierung Architektur einführen.

# Outlook für iOS und Android in Exchange Online: FAQ

18.12.2018 • 37 minutes to read

**Zusammenfassung:** In diesem Artikel werden die am häufigsten gestellten Fragen von Kunden und Administratoren zur Nutzung von Outlook für iOS und Android mit Exchange Online und Office 365 behandelt.

Die Outlook für iOS und Android-App ermöglicht Kunden in Ihrer Organisation, mehr Aufgaben über ihre Mobilgeräte zu erledigen, indem Zugriff auf E-Mails, Kalender, Kontakte und andere Dateien ermöglicht wird. In den folgenden Abschnitten werden die am häufigsten gestellten Fragen behandelt, die wir zu drei Hauptbereichen erhalten:

- Architektur von Outlook für iOS und Android und Sicherheit
- Verwaltung und Pflege von Outlook für iOS und Android in Ihrer Exchange-Organisation, nachdem diese bereitgestellt wurde
- Häufig gestellte Fragen von Endbenutzern, die mit der Outlook für iOS und Android-App auf ihren mobilen Geräten auf Informationen in Ihrer Exchange-Organisation zugreifen

## Architektur und Sicherheit

Bei den folgenden Fragen geht es um die allgemeine Architektur von Outlook für iOS und Android in Exchange Online, sowie über die Benutzerauthentifizierung und andere Sicherheitsaspekte.

### F.: Welche Cloud-Architektur wird von Outlook für iOS und Android für Office 365-Konten verwendet?

Weitere Informationen über die Architektur finden Sie unter [Outlook für iOS und Android in Exchange Online](#).

### F.: Kann ich zwei unterschiedliche Office 365-Konten aus unterschiedlichen Office 365-Regionen zu Outlook für iOS und Android hinzufügen?

Ja. Kunden mit einem Office 365 Government-Plan können jedoch möglicherweise nur Konten mit Outlook für iOS und Android aus einer einzelnen Office 365-Region verbinden. Dies bedeutet, dass Office 365 Government-Kunden nicht über ein Postfach verfügen können, das sich in den europäischen Office 365-Rechenzentren befindet, und gleichzeitig über ein Office 365 Government-Plan-Postfach innerhalb der gleichen Outlook für iOS und Android-App auf dem gleichen Gerät.

### F.: Welche Authentifizierungsmethode wird Outlook für iOS und Android verwendet? Werden Anmeldeinformationen in Office 365 gespeichert?

Outlook für iOS und Android nutzt die ADAL (Active Directory Authentication Library)-basierte Authentifizierung für den Zugriff auf Exchange Online-Postfächer in Office 365. Bei der ADAL-Authentifizierung, die von Office-Apps sowohl auf Desktopgeräten als auch auf mobilen Geräten verwendet wird, meldet sich der Benutzer direkt beim Office 365-Identitätsanbieter (Azure Active Directory) an, statt seine Anmeldeinformationen in Outlook einzugeben.

Die ADAL-basierte Anmeldung ermöglicht die Nutzung von OAuth in Office 365-Konten und stellt gleichzeitig einen sicheren Mechanismus bereit, über den Outlook für iOS und Android Zugriff auf E-Mails erhält, ohne selbst auf Benutzeranmeldeinformationen zugreifen zu müssen. Der Benutzer authentifiziert sich bei der Anmeldung unmittelbar bei Office 365 und erhält ein Zugriffstoken. Dieses Token gewährt Outlook für iOS und Android Zugriff auf das entsprechende Postfach. OAuth stellt einen sicheren Mechanismus bereit, über den Outlook ohne Benutzeranmeldeinformationen auf Office 365 und den Outlook-Clouddienst zugreifen kann.

Weitere Informationen finden Sie im Office-Blog im Beitrag [New access and security controls for Outlook for iOS](#)

and Android.

#### **F.: Unterstützen Outlook für iOS und Android und andere mobile Microsoft Office-Apps einmaliges Anmelden?**

Alle Microsoft-Apps, die die Active Directory-Authentifizierungsbibliothek (ADAL) nutzen, unterstützen einmaliges Anmelden. Darüber hinaus wird einmaliges Anmelden auch unterstützt, wenn die Apps in Verbindung mit dem Microsoft Authenticator oder mit Apps des Microsoft-Unternehmensportals verwendet werden.

Token können freigegeben und von anderen Microsoft-Apps (z. B. Word Mobile) in den folgenden Szenarien wiederverwendet werden:

1. Wenn die Apps von demselben Signaturzertifikat signiert werden und denselben Dienstendpunkt oder dieselbe Zielgruppen-URL (z.B. die Office 365-URL) verwenden. In diesem Fall wird das Token im freigegebenen App-Speicher gespeichert.
2. Wenn die Apps einmaliges Anmelden mit einer Broker-App nutzen oder unterstützen. Die Token werden innerhalb der Broker-App gespeichert. Microsoft Authenticator ist ein Beispiel für eine Broker-App. Im Broker-App-Szenario startet ADAL, nachdem Sie versucht haben, sich bei Outlook für iOS und Android anzumelden, die Microsoft Authenticator-App, die eine Verbindung zu Azure Active Directory zum Abrufen des Tokens herstellt. Dann wird das Token gespeichert und erneut für Authentifizierungsanforderungen von anderen Apps verwendet, solange die konfigurierte Token-Gültigkeitsdauer dies zulässt.

Weitere Informationen finden Sie unter [Gewusst wie: Aktivieren von App-übergreifendem SSO unter iOS mit ADAL](#).

#### **F.: Was ist die Gültigkeitsdauer der Token, die von der Active Directory-Authentifizierungsbibliothek (ADAL) in Outlook für iOS und Android generiert und verwendet werden?**

Es werden zwei Token generiert, wenn sich ein Benutzer über ADAL-aktivierte Apps wie Outlook für iOS und Android, die Authenticator-App oder die Unternehmensportal-App authentifiziert: ein Zugriffstoken und ein Aktualisierungstoken. Das Zugriffstoken wird zum Zugreifen auf die Ressource (Exchange-Nachrichtendaten) verwendet, wohingegen ein Aktualisierungstoken zum Abrufen eines neuen Zugriffs- oder Aktualisierungstokenpaars verwendet wird, wenn das aktuelle Zugriffstoken abläuft.

Standardmäßig beträgt die Gültigkeitsdauer des Zugriffstoken eine Stunde und die des Aktualisierungstokens 14 Tage. Diese Werte können angepasst werden. Weitere Informationen finden Sie unter [Konfigurierbare Tokengültigkeitsdauern in Azure Active Directory](#). Wenn diese Gültigkeitsdauern reduziert werden sollen, beachten Sie, dass möglicherweise auch die Leistung von Outlook für iOS und Android reduziert wird, da durch eine kürzere Gültigkeitsdauer die Anzahl von Versuchen erhöht wird, die die Anwendung zum Abrufen eines frischen Tokens benötigt.

#### **F.: Was geschieht mit dem Zugriffstoken, wenn das Kennwort eines Benutzers geändert wird?**

Ein zuvor gewährtes Zugriffstoken ist gültig, bis es abläuft. Nach Ablauf versucht der Client, das Aktualisierungstoken zu verwenden, um ein neues Zugriffstoken abzurufen, aber da sich das Kennwort des Benutzers geändert hat, wird das Aktualisierungstoken ungültig gemacht (unter der Voraussetzung, dass die Verzeichnissynchronisierung zwischen lokal und Azure Active Directory stattgefunden hat). Das ungültige Aktualisierungstoken erzwingt, dass der Benutzer sich erneut authentifiziert, um ein neues Zugriffstoken- und Aktualisierungstokenpaar abzurufen.

#### **F.: Unterstützt Outlook für iOS und Android die zertifikatbasierte Authentifizierung?**

Ja, Outlook für iOS und Android zertifikatbasierte Authentifizierung für moderne-Authentifizierung aktiviert Konten (Office 365-Konten oder [lokalen Konten Hybrid modernen Authentifizierung nutzen](#)) unterstützt. Weitere Informationen finden Sie unter:

- [Konfigurieren der Active Directory Federation Services \(ADFS\) in Office 365](#)
- [Zertifikatbasierte Authentifizierung in iOS](#)

- [Zertifikatbasierte Authentifizierung in Android](#)

**F.: Was ermöglicht die Synchronisierung im Hintergrund? Ich Beachten Sie, dass wenn ich mit aktiviert die app starten, ich warten Nachrichten noch herunterladen, auch wenn ich eine neue e-Mail-Benachrichtigungen für diese erhalten haben, und manchmal erhalte Erinnerungen für Termine, die abgebrochen wurde.**

Synchronisierung im Hintergrund aktiviert neue Benachrichtigung, kalendererinnerungen, Logo Count Updates und Synchronisierung im Hintergrund von Postfach- und Kalenderinformationen Informationen für Outlook für iOS und Android.

Wenn der Benutzer in der mobilen Betriebssystem Einstellungen Synchronisierung im Hintergrund deaktiviert ist, muss der Benutzer starten Sie die Anwendung und es im Vordergrund, um Nachrichten synchronisieren und haben einen Kalender auf dem neuesten Stand halten.

Hintergrund-Synchronisierung in Outlook für iOS und Android kann auch durch die folgenden Aktionen vorübergehend deaktiviert werden:

- Beenden von Outlook für iOS zu erzwingen.
- Neustarten der iOS-Geräte.
- Outlook für iOS stürzt ab, und vom Benutzer nicht neu gestartet wird.
- Öffnen die app nicht für einen bestimmten Zeitraum. iOS wird [automatisch Fixieren von Drittanbieter - apps](#), wie Outlook, basierend auf Verwendungsmuster. Android [doze-Modus und app standby](#) Funktionen können auch verhindern, dass Hintergrund Updates für die app während diese Features aktiv sind.
- Auf einige Android-Geräte können Sie auch Hintergrund Verarbeitung oder Network Access pro-app einschränken. In diesen Fällen werden Outlook für Android kann nicht im Hintergrund verarbeitet.

Wenn das mobile Betriebssystem Synchronisierung im Hintergrund verhindert, werden Benutzer Folgendes fest:

- Neue Mail-Benachrichtigungen weiterhin, jedoch übermittelt werden beim Starten der app müssen die neuen Nachrichten heruntergeladen werden.
- Kalendererinnerungen werden für Termine ausgelöst werden, die abgebrochen haben, da die app konnte keine Verbindung herunterladen und die Besprechungsabsage verarbeiten können.

#### **NOTE**

Apple ermöglicht seine systemeigene E-Mail und Kalender-apps in aktualisiert ohne Einschränkungen Hintergrund. Aus diesem Grund werden Benutzer Unterschied bei der Hintergrund-Synchronisierung zwischen der apps auftreten feststellen. Dies führt jedoch auch verbesserte Akkulaufzeit und weniger Daten Verbrauch mit Outlook für iOS.

**F.: Verfügt jede Benutzerinstanz von Outlook für iOS und Android über eine eindeutige Geräte-ID in der Office 365-basierten Architektur? Wie wird die Geräte-ID generiert und ist dies dieselbe Geräte-ID, die in Intune verwendet wird?**

Nach der anfänglichen Konto-Anmeldung wird Outlook für iOS und Android eine Verbindung mit der Office 365-basierte Architektur. Eine eindeutige Geräte-ID wird generiert, und dieser Geräte-ID wird in Active Directory-Gerätedatensätze angezeigt (die kann abgerufen werden mit Cmdlets wie [Get-MobileDevice](#) in Exchange Online Powershell) und die in der HTTP-Anforderungsheader angezeigt wird.

Intune verwendet eine anderes Gerät-ID. Der grundlegende Workflow für zum Zuweisen von Intune Geräte-ID wird in der [App-basierte bedingten Zugriff mit Intune](#) beschrieben. In Intune wird die Geräte-ID zugewiesen, wenn das Gerät Jahrestag für alle Gerät bedingte Access-Szenarien Beitritt. Dies ist eine AAD generierte eindeutige ID für das Gerät. Intune verwendet diese eindeutige ID beim Senden von Informationen zur Einhaltung und ADAL diese eindeutige ID bei der Authentifizierung auf Dienste.

**F.: Unterstützt Outlook für iOS und Android RMS?**

Ja. Outlook für iOS und Android unterstützt das Lesen geschützter Nachrichten. Im Zusammenhang mit RSM funktioniert Outlook für iOS und Android anders als Desktopversionen von Outlook. Nachdem eine geschützte Nachricht empfangen und der Zugriff versucht wurde und Outlook sichergestellt hat, dass der Benutzer RM-Nachrichten lesen kann, stellt Outlook bei Desktopversionen eine Verbindung zu Exchange her, um einen Verschlüsselungsschlüssel anzufordern. Der Outlook-Desktopclient verwendet diesen Verschlüsselungsschlüssel zum Entschlüsseln der Nachricht vor dem Benutzer (clientseitig). Mobile Clients arbeiten anders. Wenn Outlook für iOS und Android seine anfängliche Beziehung zu Exchange einrichtet, wird Exchange benachrichtigt, dass RMS unterstützt wird. Exchange entschlüsselt alle geschützten Nachrichten vor der Übergabe an den Client. Die Entschlüsselung wird also serverseitig durchgeführt. Outlook für iOS und Android führt selbst keine Entschlüsselung durch.

In Fällen, in denen Outlook für iOS und Android geschützte Nachrichten empfängt und Endbenutzer auffordert, einen RM-Client zum Öffnen der Datei zu verwenden, bedeutet dies, dass Exchange die Nachricht nicht entschlüsselt hat, was an einem Problem auf der Exchange-Seite liegt.

#### **NOTE**

Outlook für iOS nutzt iOS des systemeigenen Preview-Technologie, um schnell Anlagen für Endbenutzer verfügbar zu machen. iOS des Preview-Technologie bietet keine Unterstützung für die Verwaltung von Informationsrechten und meldet Fehler "der Vorgang konnte nicht abgeschlossen werden. (OfficeImportErrorDomain Fehler 912) "Wenn ein Benutzer versucht, eine Anlage durch Rechte geschützten zu öffnen. Benutzer müssen Tippen auf die jeweiligen Word, Excel oder PowerPoint app-Symbol, um die Anlage durch Rechte geschützten in der systemeigenen app zu öffnen.

#### **F.: Welche Ports und Endpunkte verwendet Outlook für iOS und Android?**

Outlook für iOS und Android kommuniziert über TCP-Port 443. Die App greift je nach den Aktivitäten des Benutzers auf verschiedene Endpunkte zu. Vollständige Informationen sind unter [Netzwerkanforderungen in Office 365 ProPlus](#) verfügbar.

#### **F.: Unterstützt Outlook für iOS und Android Proxykonfigurationen?**

Outlook für iOS und Android unterstützt Proxykonfigurationen Ja, wenn die Proxy-Infrastruktur die folgenden Anforderungen erfüllt:

- **Unterstützt die HTTP-Protokoll ohne Entschlüsselung von TLS und Prüfung.** Die Office 365-basierte Architektur für Outlook für iOS und Android nutzt Zertifikat verankern, um je Man-in-the-Middle-Angriffe gemindert werden können.
- **Unterstützt und SOCKS-Proxy-Funktion aktiviert hat.** Outlook für iOS und Android-Client verwendet TCP-Verbindungen für unsere Office 365-basierte Architektur. Die IP-Adressbereiche für die Verbindungen SOCKS werden nicht auf eine Teilmenge von Azure IP-Adressbereiche, beschränkt, was bedeutet, dass Kunden einen weißen Bereich definieren können nicht.
- **Keine Authentifizierung ausgeführt wird.**

Outlook für iOS und Android wird die Proxykonfiguration nutzen, wie vom Betriebssystem Plattform definiert. Normalerweise wird diese Konfigurationsinformationen über eine PAC-Datei bereitgestellt. Die PAC-Datei muss konfiguriert sein, um mit Hostnamen anstelle von Protokoll und die SOCKS-Proxy-Informationen mit der Host-URL. keine zusätzlichen benutzerdefinierten Einstellungen werden unterstützt.

## **Systemeigene Microsoft Sync-Technologie-migration**

Die folgenden Fragen werden über die Migration von der REST-API Daten Sync-Protokoll der systemeigenen Microsoft Sync-Technologie wird von Outlook für iOS und Android für den Zugriff auf Postfachdaten verwendet.

#### **F: Gibt es mindestens Version von Outlook für iOS und erforderlich Android, um die systemeigene Microsoft Sync-Technologie verwenden?**

Wir sind noch Details, um die unterstützte Mindestversion abschließen; Versuchen Sie es später wieder.

**F: Was werden meine Benutzer bemerken, wenn die systemeigene Microsoft Sync-Technologie unsere Mandanten migriert wird?**

Vorausgesetzt, dass der Benutzer eine unterstützte Version von Outlook für iOS und Android, nach der Migration Ihrer Mandanten ausgeführt wird, können Ihre Benutzer finden Sie eine kurze Bekanntmachung zurück, der angibt, dass es ihre e-Mail und Kalender-Daten aktualisieren. Andernfalls wird die Benutzeroberfläche zum Migrieren zu den aktualisierten Architektur nahtlos sein.

**F: als mandantenadministrator an kann ich steuern, welcher der Benutzer die systemeigene Microsoft Sync-Technologie migriert werden?**

Nein, werden die Migration zu den systemeigenen Microsoft Sync-Technologie am pro Mandant-durch-Mandanten und nicht auf eine einzelne Benutzer. Während die Mandanten Auswahlreihenfolge für die Migration zufällig ist, sind wir absichtlich zum Migrieren von Office 365-Postfächer zuerst als. Wenn Sie Kunde Betrieb in einer hybridkonfiguration sind, in dem ein Teil Ihrer Postfächer: lokal bleiben, werden der lokalen Benutzer [Hybrid modernen Authentifizierung](#) nutzen die systemeigenen Microsoft Sync-Technologie zu einem späteren Zeitpunkt migriert. Dies bedeutet, dass die Office 365-Benutzer während der lokalen Benutzer weiterhin die REST-API für die Verbindung zu Exchange Online verwenden, die systemeigene Microsoft Sync-Technologie migrieren.

Nach der Migration Ihres Mandanten wechselt ein Benutzer nicht die systemeigene Microsoft Sync-Technologie bis zu Nachdem sie starten/Outlook für iOS und Android fortsetzen.

**F: Wenn meine Benutzer nicht auf einen unterstützten Build von Outlook für iOS und Android vor der Migration eines Mandanten aktualisiert haben, bedeutet dies, dass der Benutzer Zugriff auf e-Mails und Kalender-Daten beim Mobile verlieren?**

Nein, wird der Benutzer weiterhin eine Verbindung über das vorhandene Daten REST-basierte Sync-Protokoll.

**F: betroffen meine App-Richtlinien Intune oder Azure AD bedingten Zugriff Richtlinien diese Migration sein?**

Nein, weiterhin Richtlinien Intune App-Richtlinien und Azure AD bedingten Zugriff auf die gezielte Identität, unabhängig von der Nutzung von Outlook für iOS und Android Daten Sync-Protokoll angewendet werden soll.

**F: müssen ich meine Exchange-Richtlinien für mobile Geräte Access aktualisieren (zulassen blockieren Quarantäne (ABQ) Regeln)?**

Nein, wird die Benutzer-Agent-Zeichenfolge, die Outlook für iOS und Android verwendet wird, nicht geändert.

Weitere Informationen zu, Benutzer-Agent Neuigkeiten finden Sie unter [Sichern von Outlook für iOS und Android in Exchange Online](#).

**F: als Exchange-Administrator gibt es eine Möglichkeit, zu bestimmen, welche Daten Sync-Protokoll Outlook für iOS und Android-Clients werden in die Office 365-basierte Architektur mit?**

Ja, führen Sie den folgenden Befehl in Exchange Online PowerShell aus:

```
Get-MobileDevice | where {$_.DeviceModel -eq "Outlook for iOS and Android"} | Format-List  
FriendlyName,DeviceID,DeviceOS,ClientType
```

Die `ClientType` -Eigenschaft gibt an, welche Daten Sync-Protokoll verwendet wird. Wenn der Wert REST ist, wird der Client der REST-API verwenden. Wenn der Wert Outlook ist, wird der Client die systemeigene Microsoft Sync-Technologie verwenden.

Alternativ kann ein Benutzer Anmeldung bei Outlook im Web und aus in **Optionen**, wählen Sie **Mobile Geräte**, die Details eines mobilen Geräts an. Der Benutzer sehen wie das Cmdlet den Wert für die `ClientType` Eigenschaft.

## Verwalten und Überwachen von Outlook für iOS und Android in Ihrer Organisation

Die folgenden Fragen werden Informationen zum Verwalten und überwachen das Outlook für iOS und Android-

app in Ihrer Organisation nach der Bereitstellung der app.

#### **F.: Muss ein Supportticket in der App eingereicht werden, wenn ein Problem mit Outlook für iOS und Android auftritt?**

Ja, wenn Sie das Problem beheben möchten oder wenn Sie uns über einen Produktfehler oder eine Beschränkung informieren möchten, müssen Sie ein Supportticket in der App einreichen. Nur über das Einreichen eines Supporttickets in der App können die Protokolle Outlook-App gesammelt und von unseren Produkttechnikern analysiert werden.

Kunden mit einer Vereinbarung zum Microsoft Premier können Support-Anfragen mit Kundendienst und Support (CSS) öffnen. Anstatt des Benutzers ein in app-Support-Ticket zu initiieren, kann der Benutzer sammeln Diagnose zum Hochladen der Protokolle und die Freigabe des Vorfalls ID mit CSS/Premier nutzen. Sammeln von Diagnose Erfassen von Daten aus Outlook für iOS und Android, Authentifizierung und das Unternehmensportal und Laden Sie alle relevanten Protokolle in Microsoft wird. Microsoft-Supportmitarbeiter Ausweitung können des Vorfalls ID an, die Zugriff auf die Diagnoseprotokolle und beheben das Problem des Benutzers.

Um die Protokolle zu erfassen:

1. Tippen Sie in Outlook für iOS und Android Einstellungen auf Hilfe und Feedback.
2. Tippen Sie auf Diagnose erfassen.
3. Tippen Sie zweimal auf Erste Schritte.
4. Tippen Sie auf Hochladen von Outlook-Protokolle (iOS) oder Protokoll speichern (Android).
5. Freigeben des Vorfalls ID mit CSS.

#### **F.: Als Exchange-Administrator möchte ich Outlook für iOS und Android bereitstellen, aber ich kann mich nicht zum Testen anmelden. Was könnte das Problem sein?**

Vorausgesetzt, dass die Authentifizierung nicht behoben ist, sind zwei Bereiche, die Sie prüfen können:

1. Überprüfen Sie, ob es eine EWS-Anwendungsrichtlinie gibt, die einschränkt, welche Clientanwendungen eine Verbindung herstellen können.
2. Überprüfen Sie, ob Sie EWS für das Konto aktiviert haben.

Weitere Informationen finden Sie unter [Sichern von Outlook für iOS und Android in Exchange Online](#). Wenn durch eine der oben genannten Überprüfungen das Problem nicht gelöst wird, reichen Sie ein Supportticket in der App ein.

#### **F.: Unterstützt Outlook für iOS und Android EMM- oder MDM-Lösungen von Drittanbietern?**

Outlook für iOS und Android unterstützt Intune für Geräte- und Management. MDM Drittanbieter können bereitstellen die Outlook-app die gleiche Weise, wie sie eine beliebige IOS- oder Android-app bereitstellen würde mit ihren vorhandenen Tools. Sie können auch Gerät Verwaltungssteuerelemente Gerät-ID, geräteverschlüsselung, zu löschen und mehr, alle für eine sichere e-Mail-Erfahrung wichtig sind, aber alle sind auch völlig unabhängig von Outlook für iOS und Android angewendet. Um die Verwaltung und den Schutz von Unternehmensdaten innerhalb der app (wie durch die Beschränkung auf Aktionen mit Unternehmensdaten wie Ausschneiden, kopieren, einfügen und "Speichern unter"), müssen Kunden Microsoft Intune verwenden. Ausführliche technische Informationen finden Sie unter Dokumentation zu [Azure Active Directory bedingten Zugriff](#) und [Intunes App-Schutz](#).

#### **F.: Ist eine Lizenz für die Verwendung von Outlook für iOS und Android erforderlich?**

Outlook für iOS und Android ist kostenlos Consumer Verwendung von iOS-App-Store und von Google wiedergeben. Kommerzielle Benutzer erfordern jedoch ein Office 365-Abonnement, die Office-deskstopanwendungen: Business, Business Premium, Enterprise E3, E5, und ProPlus oder die entsprechenden Versionen dieser Pläne für Behörden oder Education. Kommerzielle Benutzer mit den folgenden Abonnements werden diagonal mit Outlook mobile app auf Geräten mit integrierten Bildschirmen 10.1" zulässige oder weniger:

Office 365 Enterprise E1, Office 365 F1, Office 365 Business Essentials, Office 365 A1, und wenn Sie nur ein Exchange Online-Lizenz (ohne Office). Wenn Sie nur eine Exchange-lokale (Exchange Server)-Lizenz verfügen, sind Sie nicht berechtigt, um die app verwenden.

## Häufig gestellte Fragen von Endbenutzern

Die folgenden Fragen betreffen die Endbenutzer in Ihrer Organisation, die Outlook für iOS und Android auf ihren Geräten zum Zugreifen auf ihre Exchange-Postfächer verwenden.

### **F: Meine Benutzer aktiviert die "Speichern Kontakte" Erweiterte Einstellungsoption. Sie beschweren, dass nicht alle Kontakte auf ihren iOS-Geräten synchronisiert wurden. Gibt es Einschränkungen mit Synchronisierung?**

Der anfängliche Export von Kontakten kann nur beginnen, wenn Outlook im Vordergrund ist. Benutzer kann zwischen apps wechseln und der Export wird fortgesetzt, während Outlook im Arbeitsspeicher aktiv ist. Sind iOS Einschränkungen beim Synchronisieren mit iCloud, die in Dateninkonsistenzen auftreten können, aber die Outlook wird automatisch eine Abstimmung, um sicherzustellen, dass die Kontakte immer konsistent exportiert werden (z. B. Abstimmung entfernt Duplikate in der Ereignis, das Outlook erkennt exportiert Kontakte aus einer vorherigen Export-Aktivität). In der Ereignisprozedur Sie eine Inkonsistenz sehen, und es nicht behoben nach kurzer Zeit wurde noch, 24 Stunden zu warten, und starten Sie die app zum Auslösen des Abstimmungsprozess neu.

### **F.: Warum müssen die Office Mobile-Apps auf Android-Geräten installiert werden, damit Anlagen in Outlook gerendert werden können, wohingegen iOS-Geräte eine Vorschau der Anlagen innerhalb von Outlook bieten?**

Die liegt an den Unterschieden in den grundlegenden Betriebssystemen. iOS stellt eine systemeigene Inhaltswiedergabe für bekannte Anlagentypen bereit, die Outlook für iOS verwendet, um ein einfaches Anlagenrendering bereitzustellen. Android bietet keine ähnliche Funktion. Android-Benutzer müssen die Office-Apps und/oder Drittanbieter-Apps installieren, um den Anlageninhalt zu rendern.

### **F.: Eine neue Nachricht enthielt eine Anlage, aber ich konnte die Anlage nicht öffnen, während ich offline war. Woran liegt das?**

In Outlook (wie auch in anderen mobilen Clients) werden Anlagen nicht automatisch heruntergeladen. Dies ist beabsichtigt, um auf dem Gerät Platz zu sparen. Anlagen werden nur auf Anforderung des Benutzers heruntergeladen.

### **F.: Vor einer Woche habe ich auf eine Anlage in einer Nachricht zugegriffen, aber da ich nun offline bin, kann ich nicht mehr auf diese Anlage auf meinem iOS-Gerät zugreifen. Ich kann aber auf meinem Android-Gerät darauf zugreifen. Woran liegt das?**

Outlook für iOS speichert Anlagen in seiner eigenen Datenbank. Dementsprechend nimmt jede Anlage, die wir auf den Client herunterladen, sehr viel Platz in unserer Datenbank in Anspruch. Um sicherzustellen, dass der Client schnelle Leistung bereitstellen und nur eine kleine Menge Speicherplatz in Anspruch nehmen kann, werden Daten verhältnismäßig aggressiv basierend auf ihrer Nutzung (Anlagen werden bis zu sieben Tage zwischengespeichert) gelöscht.

Im Gegensatz zu iOS verwendet Android ein zugängliches Dateisystem, wenn Outlook für Android also eine Anlage herunterlädt, gelangt diese nicht in die Datenbank, sondern wird als temporäre Datei gespeichert.

### **F: Warum Daten in Outlook für iOS verschwinden, und klicken Sie dann erneut angezeigt, nachdem ich den Posteingang Experten oder das Organisieren von Threadeinstellungen für den umschalten?**

Sobald diese Optionen geändert werden, führt Outlook für iOS Zurücksetzen des Geräts an. Dies löscht die vorhandenen Daten, die an die app heruntergeladen wurde und erfordert eine erneute Synchronisierung.

### **Frage: anzeigen kann ich in Outlook für iOS Organisationsinformationen Diagramm?**

Ja. Outlook für iOS bietet Organisationsinformationen als Teil einer Person Visitenkarte Details Ihres Unternehmens. Ihr Unternehmen des reporting-Struktur und eine Liste der Kollegen auch angegeben ist, bei der Kontaktaufnahme mit Personen und Teams entwickelt benötigten Mitarbeiter unterstützen.

Die Liste der Personen, die als Teil der Liste der anderen Kollegen unter **Organisation anzeigen** angezeigt basiert auf allgemeine e-Mail-Verteilerlisten, Gruppenmitgliedschaften und Grad Trennung in der Organisationsstruktur in

Azure Active Directory definiert.

Wenn Sie keine Organigramm-Daten in der app verfügbar gemacht haben, wenden Sie sich an Ihrer Directory-Administrator. Es gibt zwei Hauptzenarien zu berücksichtigen sind:

1. Ihr Unternehmen verfügt über eine hybridtopologie, in einem lokalen Verzeichnis mit Azure Active Directory synchronisiert wird. Sie müssen Active Directory mit Diagramm Organisationsinformationen, entweder direkt in das Verzeichnis oder über Ihr System Personalabteilung aktualisieren. Daten werden automatisch in AAD synchronisiert werden und werden auf den über die globale Adressliste in Exchange Online.
2. Ihr Unternehmen nutzt Azure Active Directory nur für Directory Management. Sie müssen Azure Active Directory mit Diagramm Organisationsinformationen, entweder direkt in das Verzeichnis oder über Ihr System Personalabteilung zu aktualisieren. Diese Daten werden auf den über die globale Adressliste in Exchange sein Online.

**F: wie viele Daten Postfach mit Outlook für iOS und Android synchronisiert wird?**

Outlook für iOS und Android synchronisiert 500 Elementen pro Ordner, mit bis zu 1000 Elementen pro Ordner, wenn der Benutzer **Weitere Unterhaltungen laden** tippt. Die app schneidet der Elemente pro Ordner nach unten zu 500, in regelmäßigen Abständen, um die app eine optimale Leistung zu gewährleisten.

**F: Warum sind Aufgaben und Notizen nicht mit Outlook für iOS und Android verfügbar?**

Microsofts strategische Ausrichtung für die Verwaltung von Aufgaben und Notizen auf mobilen Geräten ist die Aufgabenleiste und OneNote-apps. Aufgabenleiste bietet Integration in die Aufgaben in Exchange Online-Postfächern gespeichert.

# Einrichten des Kontos mit der modernen Authentifizierung in Exchange Online

18.12.2018 • 9 minutes to read

**Zusammenfassung:** Hier erfahren Sie, wie Benutzer mit Konten mit aktiverter moderner Authentifizierung schnell ihre Outlook für iOS und Android-Konten in Exchange Online einrichten können.

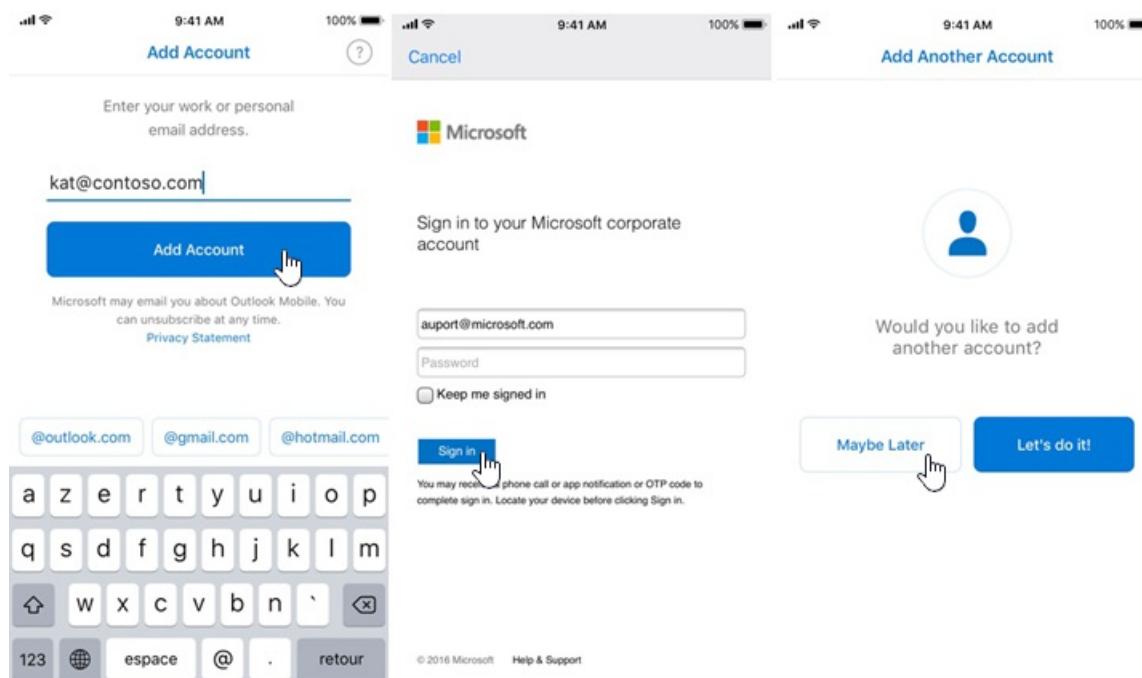
Es gibt zwei Methoden, die Benutzer in Ihrer Exchange Online-Organisation eigene Outlook für iOS und Android Konten einrichten: automatische Erkennung und einmaliges Anmelden. Beide Methoden nutzen modernen Authentifizierung. Darüber hinaus bietet Outlook für iOS und Android IT-Administratoren die Möglichkeit, Konto Konfigurationen auf ihre Office 365-Benutzer als auch; Steuerelement "push", ob Outlook für iOS und Android Persönliche Konten unterstützt.

## Automatische Erkennung

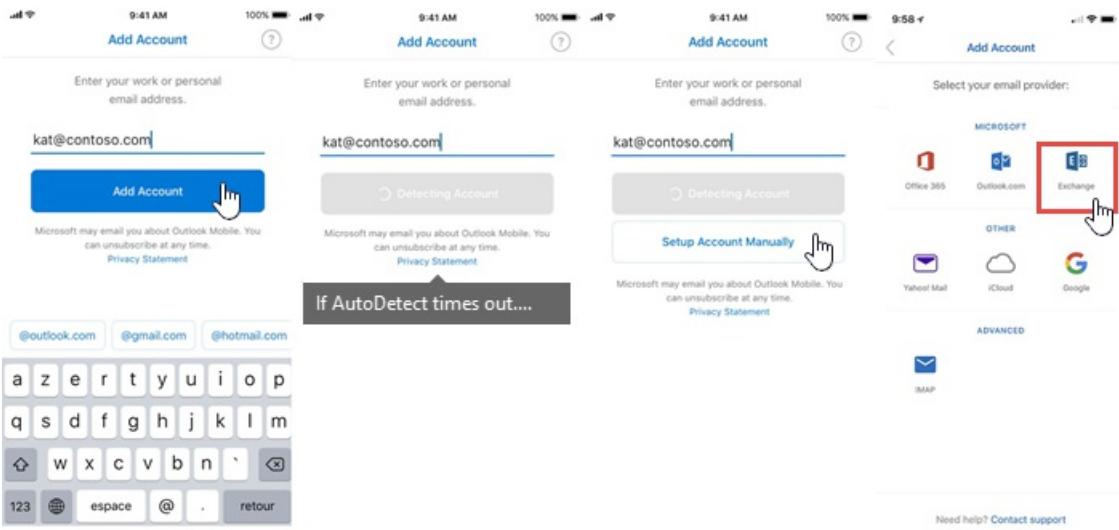
Outlook für iOS und Android bietet eine Lösung namens Automatische Erkennung, mit der Endbenutzer ihre Konten schnell einrichten können. Automatische Erkennung bestimmt anhand der SMTP-Domäne zunächst den Kontotyp des Benutzers. Kontotypen, die von diesem Dienst abgedeckt sind, umfassen Office 365, Outlook.com, Google, Yahoo und iCloud. Als Nächstes nimmt die automatische Erkennung auf Grundlage dieses Kontotyps entsprechende Konfigurationen an der App auf dem Gerät des Benutzers vor. Dies spart Zeit, und Benutzer müssen keine Konfigurationseinstellungen wie Hostname und Portnummer manuell eingeben.

Für moderne-Authentifizierung, die von allen Office 365-Konten und [lokalen Konten Hybrid modernen Authentifizierung nutzen](#), automatische Erkennung Abfragen Exchange Online-Kontoinformationen des Benutzers verwendet wird, und konfiguriert dann Outlook für iOS und Android (engl.) Klicken Sie auf dem Gerät des Benutzers, damit die app eine Verbindung zu Exchange Online herstellen kann. Während dieses Vorgangs ist die einzige vom Benutzer erforderliche Informationen ihre SMTP-Adresse und Anmeldeinformationen.

Die folgenden Abbildungen enthalten ein Beispiel für eine Konfiguration mithilfe der automatischen Erkennung:



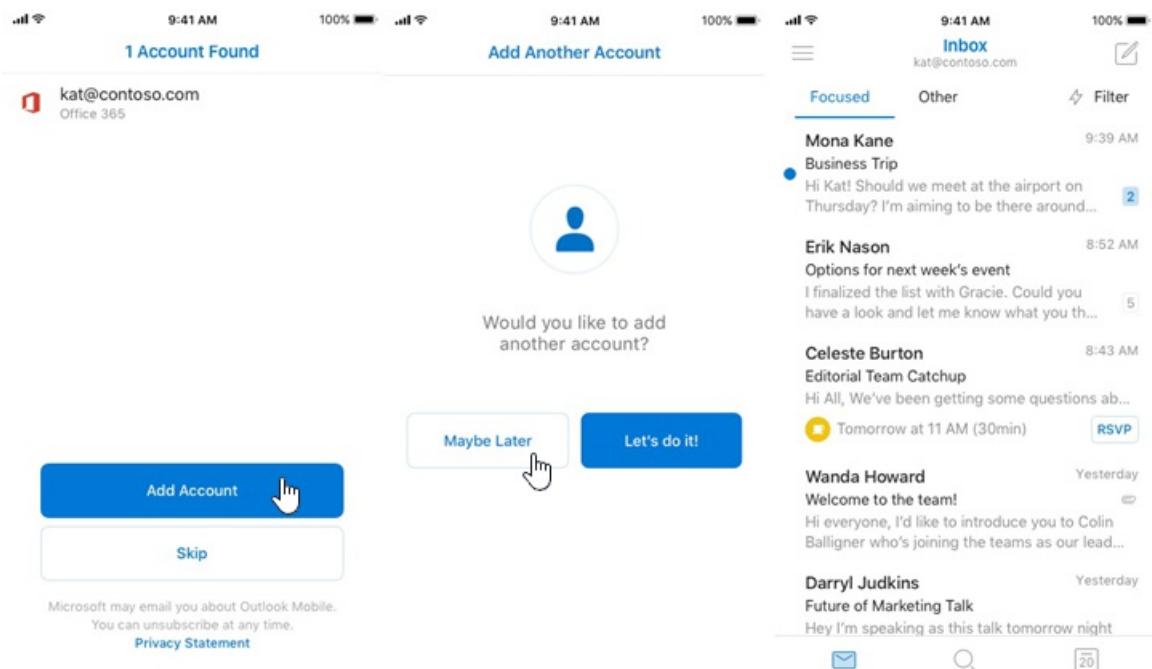
Wenn bei der automatischen Erkennung für einen Benutzer Fehler auftreten, enthalten die folgenden Abbildungen einen alternativen Kontokonfigurationspfad unter Verwendung der manuellen Konfiguration:



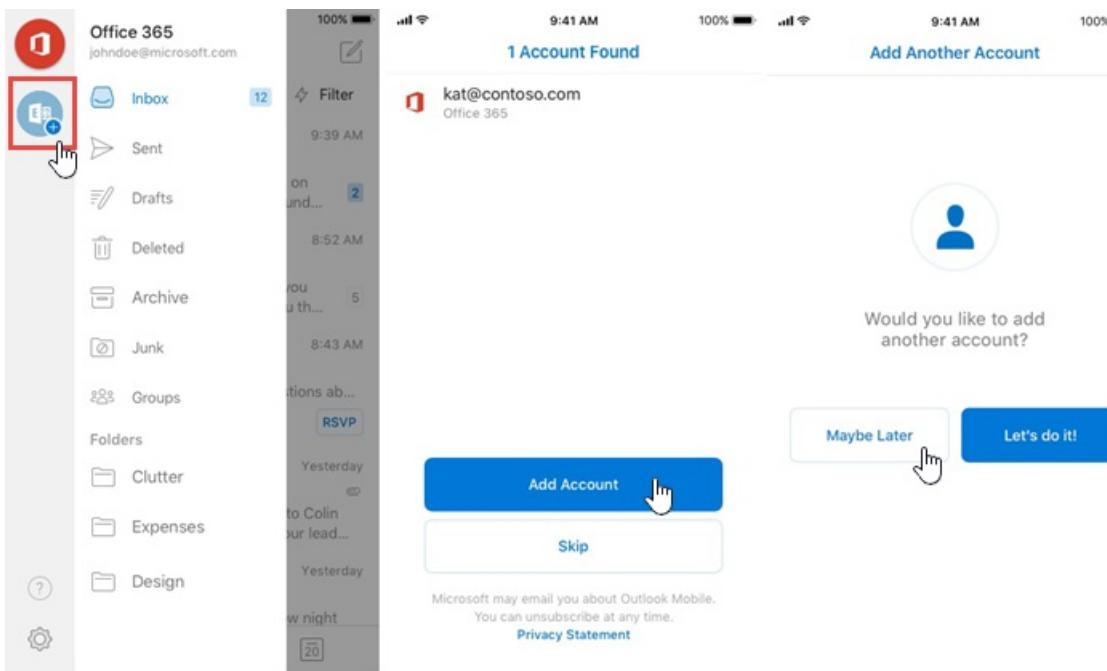
## Einmaliges Anmelden

Outlook für iOS und Android unterstützt einmaliges Anmelden über Authentifizierung erneut token verwenden. Wenn ein Benutzer zu einer anderen Microsoft-app auf ihrem Gerät, wie Word oder Unternehmensportal, bereits, in angemeldet ist Outlook für iOS für Android erkennt das Token und für eine eigene Authentifizierung verwenden. Wenn eine solche ein Token erkannt wird, Benutzer bereits registriert in Outlook für iOS und Android ihre verfügbares Konto angezeigt wird als "Found" unter **Konten** im Menü **Einstellungen**. Neue Benutzer werden ihr Konto auf dem ersten Konto angezeigt.

Die folgenden Abbildungen enthalten ein Beispiel für eine Kontofiguration mithilfe des einmaligen Anmeldens für einen neuen Benutzer:



Wenn ein Benutzer Outlook für iOS und Android bereits verwendet, z. B. für ein persönliches Konto, ein Office 365-Konto jedoch erkannt wird, weil er sich kürzlich registriert hat, sieht der Pfad für das einmalige Anmelden wie folgt aus:



## Setup Kontokonfiguration über Enterprise Mobilität management

Outlook für iOS und Android bietet IT-Administratoren die Möglichkeit, "Office 365-Konten oder lokalen Konten Hybrid modernen Authentifizierung nutzen push Konto Konfigurationen". Diese Funktion kann mit jedem Mobile Device Management (MDM)-Anbieter, der den [App-Konfiguration verwaltet](#) DDE-Kanal für Android für IOS- oder [Android im Unternehmen](#) Kanals verwendet werden.

Für Benutzer in Microsoft Intune registriert können Sie die kontokonfigurationseinstellungen mit Intune in Azure-Verwaltungsportal bereitstellen.

Sobald Setup Kontokonfiguration wurde Setup im MDM Anbieter und der Benutzer registriert wird ihr Gerät, Outlook für iOS und Android erkennt, die ein Konto "gefunden wird" und dann fordert den Benutzer auf das Konto hinzufügen. Die einzige Information, die der Benutzer die EINGABETASTE, um das Setup abschließen muss ist ihr Kennwort. Klicken Sie dann Inhalt von Postfächern der Benutzer geladen, und der Benutzer kann mithilfe der app beginnen.

Weitere Informationen über die Konto Setup Konfigurationsschlüssel der Konfiguration erforderlich, um diese Funktion zu aktivieren finden Sie unter der Konto-Setup-Konfigurationsabschnitt in [Bereitstellen von Outlook für iOS und Android-App Configuration Settings](#).

## Organisation Konten Modus zulässig

Unter Einhaltung der Richtlinien zur Verhinderung Sicherheit und Richtlinientreue unserer Kunden größten und hochgradig regulierten ist eine wichtige Konstante in der Office 365-Wert. Einige Unternehmen haben eine Anforderung zum Erfassen aller Communications Informationen in ihrer Umgebung im Unternehmen sowie, stellen Sie sicher, dass die Geräte nur für die geschäftliche Kommunikation verwendet werden. Um diesen Anforderungen zu unterstützen, können Outlook für iOS und Android auf corporate verwalteten Geräten konfiguriert werden nur einer einzigen, unternehmensweiten Konto in Outlook für iOS und Android bereitgestellt werden. Wie funktioniert mit Setup Kontokonfiguration, diese Funktion mit jedem beliebigen Mobile Device Management (MDM)-Anbieter, der den [App-Konfiguration verwaltet](#) DDE-Kanal für Android für IOS- oder [Android im Unternehmen](#) Kanals verwendet. Dies wird mit Office 365 Benutzerkonten unterstützt oder lokalen Konten Hybrid modernen Authentifizierung nutzen, jedoch nur ein einzelnes corporate-Konto hinzugefügt werden Outlook für iOS und Android.

Weitere Informationen zu den Einstellungen, die zum Bereitstellen der Organisation zulässig Konten-Modus konfiguriert werden müssen, finden Sie in der Organisation Konten Modus Abschnitt in der [Bereitstellung von](#)

Outlook für iOS und Android-App-Konfigurationseinstellungen zulässig.

**NOTE**

Setup Kontokonfiguration und Organisation zulässigen Konten Modus können zusammen konfiguriert werden, um kontoeinrichtung zu vereinfachen.

Um sicherzustellen, diese Benutzer können nur im Unternehmen e-Mail auf registrierten Geräte (gibt an, ob IOS- oder Android Enterprise sein) mit Intune zugreifen, Sie müssen eine bedingte Zugriffsrichtlinie Azure Active Directory mit dem Grant-Steuerelementen [nutzen](#) **Geräte erfordern als kompatibel markiert** am Arbeitsplatz und **erfordern Client app genehmigt**. Informationen zum Erstellen von diesem Typ der Richtlinie können in [Azure Active Directory-basierte app bedingten Zugriff](#) gefunden werden.

**IMPORTANT**

Grant-Steuerelement [erfordern Gerät als kompatible gekennzeichnet werden](#) muss das Gerät vom Intune verwaltet werden.

1. Die erste Richtlinie ermöglicht Outlook für iOS und Android und OAuth kann Exchange ActiveSync-Clients eine Verbindung zu Exchange Online blockiert. Finden Sie unter "Schritt 1: Konfigurieren einer Richtlinie des Azure AD-bedingte Zugriff für Exchange Online", aber für die fünfte Schritt wählen Sie "Erfordern Gerät als kompatibel markiert werden", "Erfordern genehmigte Client-app" und "Erfordern alle ausgewählten Steuerelemente".
2. Durch die zweite Richtlinie wird verhindert, dass Exchange ActiveSync-Clients über die Standardauthentifizierung eine Verbindung zu Exchange Online herstellen. Weitere Informationen finden Sie unter „Schritt 2 - Konfigurieren einer Azure AD-Richtlinie für bedingten Zugriff für Exchange Online mit ActiveSync (EAS)“.

# Verwalten von Outlook für iOS und Android in Exchange Online

18.12.2018 • 12 minutes to read

**Zusammenfassung:** In diesem Artikel werden bewährte Methoden zum Verwalten von mobilen Geräten mit Outlook für iOS und Android in Exchange Online beschrieben.

Outlook für iOS und Android bietet Benutzern ein schnelles und intuitives E-Mail- und Kalender-Erlebnis, wie man es von einer modernen mobilen App erwartet, und ist dabei die einzige App, die die besten Features von Office 365 unterstützt. Microsoft bietet außerdem eine Reihe von Dienstprogrammen für die Verwaltung und den Schutz von Unternehmensdaten auf mobilen Geräten in Ihrer Exchange Online-Organisation.

## Optionen für die Verwaltung von Geräten und Anwendungen in Office 365

Kunden, die Outlook für iOS und Android verwalten möchten, haben die folgenden Optionen:

1. **Empfohlen:** Die Enterprise Mobility + Security-Suite, einschließlich Microsoft Intune und bedingter Azure Active Directory-Zugriff.
2. Verwaltung mobiler Geräte (Mobile Device Management, MDM) für Office 365.
3. Zugriffs- und Postfachrichtlinien für mobile Geräte.

### NOTE

Implementierungsdetails zu diesen drei Optionen finden Sie unter [Sichern von Outlook für iOS und Android in Exchange Online](#).

Microsoft empfiehlt Office 365-Kunden aufgrund der erweiterten Funktionen dieser Dienste, entweder die Enterprise Mobility + Security-Suite für den Schutz Unternehmensdaten auf mobilen Geräten zu verwenden. Die wichtigsten Funktionen der integrierten MDM für Office 365 sind im Office 365-Abonnement enthalten, während die umfassenderen Funktionen von Enterprise Mobility + Security den Kauf eines zusätzlichen Abonnements erfordern.

### IMPORTANT

Zugriffsregeln für mobile Geräte (Zulassen, Blockieren oder Quarantäne) in Exchange Online werden übersprungen, wenn der Zugriff durch eine Richtlinie für bedingten Zugriff verwaltet wird, die entweder [Konfigurieren von Richtlinien für den gerätebasierten bedingten Zugriff für Azure Active Directory](#) oder [Referenz zu den Einstellungen für den bedingten Azure Active Directory-Zugriff](#) umfasst.

Ein vollständiger Vergleich zwischen MDM und Intune steht in [Auswählen zwischen MDM für Office 365 und Microsoft Intune](#) zur Verfügung.

#### **NOTE**

Wenn Sie Cmdlets für mobile Geräte wie `Get-MobileDevice` zum Überprüfen des Status eines Geräts, der Zeitstempel für Outlook für iOS und Android Synchronisierung angegeben, durch die `LastSyncTime`-Eigenschaft ist möglicherweise bis zu 15 Minuten nach dem tatsächlich Zeitpunkt der Synchronisierung. Während der Synchronisierung von Geräten in Echtzeit auftritt, kann der zurückgegebene Zeitstempel hinter lag.

## **Verwenden von Enterprise Mobility + Security**

Die umfassendsten Schutzfunktionen für Office 365-Daten sind verfügbar, wenn Sie ein Abonnement für die Enterprise Mobility + Security-Suite abschließen, das Microsoft Intune, Azure Information Protection sowie Azure Active Directory Premium-Features, z. B. bedingten Zugriff, umfasst.

#### **NOTE**

Das Abonnement der Enterprise Mobility + Security-Suite umfasst zwar sowohl Lizenzen für Microsoft Intune als auch für Enterprise Mobility + Security, Kunden können aber Lizenzen für Microsoft Intune und Azure Active Directory Premium auch separat erwerben. Alle Benutzer müssen für die Verwendung der Richtlinien für bedingten Zugriff und Intune-Schutz für Apps, die in diesem Artikel besprochen werden, lizenziert sein.

Intune bietet Funktionen zur Verwaltung mobiler Anwendungen (Mobile Application Management, MAM) sowie andere Funktionen für bedingten Zugriff und Geräteverwaltung. Mit Richtlinien für Intune-Schutz für Apps können Sie Aktionen wie z. B. Ausschneiden, Kopieren, Einfügen und „Speichern unter“ von Unternehmensdaten zwischen von Intune verwalteten Apps und nicht von Intune verwalteten Apps einschränken. Weitere Informationen finden Sie unter [Erstellen und Zuweisen von App-Schutzrichtlinien](#). Darüber hinaus enthalten die von Intune verwalteten Apps für Outlook ein neues Feature zur Verwaltung von mehreren Identitäten, mit dem Benutzer in derselben Outlook-App auf ihre privaten und geschäftlichen E-Mail-Konten zugreifen können, während die Intune MAM-Richtlinien nur auf das Geschäftskonto des Benutzers angewendet werden. Dadurch wird ein wesentlich nahtloseres Benutzererlebnis ermöglicht.

Der bedingte Zugriff ist eine Funktion von Azure AD, die es Ihnen ermöglicht, eine Steuerung des Zugriffs auf Apps in Ihrer Umgebung basierend auf spezifischen Bedingungen von einem zentralen Ort aus zu erzwingen. Mithilfe von Richtlinien für bedingten Zugriff können Sie die korrekten Zugriffssteuerungen unter den erforderlichen Bedingungen anwenden. Bedingter Azure Active Directory-Zugriff bietet eine höhere Sicherheit, wenn diese erforderlich ist, und gibt Benutzern Freiraum, wenn keine erhöhte Sicherheit erforderlich ist.

Wichtige Funktionen der Enterprise Mobility + Security-Suite mit Outlook für iOS und Android:

- **Bedingter Zugriff.** Durch Azure Active Directory wird sichergestellt, dass auf Exchange Online-E-Mails nur zugegriffen werden kann, wenn die Anforderungen für bedingten Zugriff erfüllt sind. Weitere Informationen zur Geräteregistrierung finden Sie unter [Bedingter Zugriff in Azure Active Directory](#).
- **Intune-Schutz für Apps.** Mit Outlook für iOS und Android können Sie Ihre Unternehmensdaten mit Richtlinien für Intune-Schutz für Apps schützen. Dies ist eine hervorragende Option für BYOD-Szenarien („Bring your own device“), in denen Sie Unternehmensdaten schützen möchten, ohne die Geräte eines Benutzers zu verwalten. Weitere Informationen zu Richtlinien für den Intune-Schutz von Apps finden Sie unter [Schützen von App-Daten mithilfe der App-Schutzrichtlinien mit Microsoft Intune](#).
- **Geräteregistrierung.** Mit Intune können Sie die Geräte und Apps Ihrer Mitarbeiter sowie deren Zugriff auf Ihre Unternehmensdaten verwalten. In diesem Modell wird von Outlook für iOS und Android sichergestellt, dass auf Exchange Online-E-Mails nur auf Telefonen und Tablets zugegriffen werden kann, die von Ihrem Unternehmen verwaltet werden und den Richtlinien Ihrer Organisation entsprechen. Wenn sich Benutzer auf einem nicht verwalteten mobilen Gerät bei der Outlook-App anmelden, fordert Outlook die Benutzer auf, das Gerät in Intune mithilfe der Azure-Richtlinie für bedingten Zugriff zu registrieren, und überprüft dann, ob das Gerät die Standards der Organisation bezüglich Gerätekompatibilität erfüllt.

- **Geräteverwaltung und Berichte.** Mit dem Registrierungsvorgang können Organisationen Sicherheitsrichtlinien festlegen und verwalten, die z. B. PIN-Sperren auf Geräteebene erzwingen, Datenverschlüsselung erfordern und gefährdete Geräte blockieren, um den Zugriff nicht vertrauenswürdiger Geräte auf E-Mails und Daten des Unternehmens zu verhindern. Jedes registrierte Gerät wird im Office 365 Admin Center angezeigt, und es können Berichte über Details der Geräte erstellt werden, die auf Ihre Unternehmensdaten zugreifen.
- **Selektives Zurücksetzen.** Microsoft Intune kann Office 365-E-Mail-Daten von Outlook für IOS und Android entfernen und gleichzeitig private E-Mail-Konten intakt lassen (unabhängig davon, ob das Gerät registriert ist oder nicht). Dies ist eine zunehmend wichtige Anforderung, da immer mehr Unternehmen einen „Bring your own device“-Ansatz für Telefone und Tablets verfolgen.

Weitere Informationen zu Microsoft Intune finden Sie unter [Microsoft Intune-Dokumentation](#).

### **Verwenden der integrierten mobilen Geräteverwaltung (MDM) für Office 365**

MDM für Office 365 bietet Geräteverwaltungsfunktionen ohne zusätzliche Kosten. Microsoft Intune unterstützt diese grundlegenden Funktionen durch Bereitstellung einer Kerngruppe von Steuerelementen im Office 365 Admin Center für Organisationen, die die Grundlagen benötigen.

Da dies eine Lösung zur Geräteverwaltung ist, gibt es keine systemeigene Funktion, um zu steuern, welche Apps verwendet werden können, auch nachdem das Gerät registriert wurde. Wenn Sie den Zugriff auf Outlook for iOS und Android beschränken möchten, müssen Sie Azure Active Directory Premium-Lizenzen erwerben und Richtlinien für bedingten Zugriff verwenden.

Outlook für iOS und Android unterstützt die von MDM bereitgestellten Funktionen für Office 365 vollständig.

Ausführliche Informationen zu MDM finden Sie in den folgenden Ressourcen:

- [Übersicht über die Verwaltung mobiler Geräte \(MDM\) für Office 365](#)
- [Verwalten von Einstellungen und Features auf Ihren Geräten mit Microsoft Intune-Richtlinien](#)
- Anweisungen für die Endbenutzer zur Registrierung eines Geräts in Office 365 MDM: [Registrieren eines mobilen Geräts in Office 365](#)

### **Verwenden von Zugriffs- und Postfachrichtlinien für mobile Geräte**

Microsoft empfiehlt, mit denen Office 365-Kunden die Enterprise-Mobilität + Security Suite oder den integrierten MDM für Office 365 Unternehmensdaten auf mobilen Geräten, aufgrund der erweiterten Funktionen von dieser Dienste verwalten. Outlook für iOS und Android unterstützt den Zugriff durch mobile Geräte und Postfachrichtlinien für mobile Geräte (früher als Exchange Active Sync-Richtlinien bezeichnet), die über das Exchange Administrationscenter verfügbar sind.

Outlook für iOS und Android unterstützt die folgenden Einstellungen für Postfachrichtlinien für mobile Geräte:

- Geräteverschlüsselung aktiviert
- Min. Kennwortlänge
- Kennwort aktiviert

Weitere Informationen finden Sie unter [Postfachrichtlinien für mobile Geräte in Exchange Online](#).

Exchange-Administratoren können eine Remote-Gerät-zurücksetzung für Outlook für iOS und Android initiieren. Bei Anforderung der Remote-Gerät-zurücksetzung entfernt die App das Profil und alle damit verbundenen Daten.

# Sichern von Outlook für iOS und Android in Exchange Online

18.12.2018 • 31 minutes to read

Outlook für iOS und Android bietet Benutzern ein schnelles und intuitives E-Mail- und Kalender-Erlebnis, wie man es von einer modernen mobilen App erwartet, und ist dabei die einzige App, die die besten Features von Office 365 unterstützt.

Es ist äußerst wichtig, Unternehmens- und Organisationsdaten zu schützen, die auf den Mobilgeräten Ihrer Benutzer gespeichert sind. Überprüfen Sie zunächst [Einrichten von Outlook für iOS und Android](#), um sicherzustellen, dass die Benutzer alle erforderlichen Apps installiert haben. Wählen Sie anschließend eine der folgenden Optionen aus, um Ihre Geräte und die Daten Ihrer Organisation zu schützen:

1. **Empfohlen:** Wenn Ihre Organisation über ein Abonnement von Enterprise Mobility + Security verfügt oder Lizenzen für Microsoft Intune und Azure Active Directory Premium separat erworben hat, führen Sie die Schritte unter [Verwenden der Enterprise Mobility + Security-Suite zum Schutz von Unternehmensdaten mit Outlook für iOS und Android](#) aus, um Unternehmensdaten mit Outlook für iOS und Android zu schützen.
2. Wenn Ihre Organisation nicht über Abonnement von Enterprise Mobility + Security oder Lizenzen für Microsoft Intune und Azure Active Directory Premium verfügt, führen Sie die Schritte unter [Verwenden der mobilen Geräteverwaltung für Office 365](#) aus, und verwenden Sie die Verwaltung mobiler Geräte (MDM) für Office 365-Funktionen, die in Ihrem Office 365-Abonnement enthalten sind.
3. Führen Sie die Schritte in [Verwenden von Exchange Online-Richtlinien für mobile Geräte](#) aus, um grundlegende Postfachrichtlinien für mobile Exchange-Geräte und Gerätezugriffsrichtlinien zu implementieren.

Wenn Sie jedoch Outlook für iOS und Android nicht in Ihrer Organisation verwenden möchten, finden Sie unter [Blockieren von Outlook für iOS und Android](#) weitere Informationen.

## NOTE

Lesen Sie den Abschnitt [Anwendungsrichtlinien in den Exchange-Webdiensten \(EWS\)](#) weiter unten in diesem Artikel, wenn Sie stattdessen eine EWS-Anwendungsrichtlinie implementieren möchten, um in Ihrer Organisation den Zugriff über Mobilgeräte zu steuern.

## Einrichten von Outlook für iOS und Android

Für Geräte, die in einer MDM-Lösung registriert sind, verwenden Benutzer die MDM-Lösung, z. B. das Intune-Unternehmensportal, um die erforderlichen Apps zu installieren: Outlook für iOS und Android und Microsoft Authenticator.

Für Geräte, die nicht in einer MDM-Lösung registriert sind, müssen Benutzer Folgendes installieren:

- Outlook für iOS und Android über den Apple App Store oder den Google Play Store
- Die Microsoft Authenticator-App über den Apple App Store oder den Google Play Store
- App des Intune-Unternehmensportals über den Apple App Store oder den Google Play Store

Nach der Installation der App können Benutzer die folgenden Schritte ausführen, um ihr Unternehmens-E-Mail-

Konto hinzuzufügen und grundlegende App-Einstellungen zu konfigurieren:

- Einrichten von E-Mail in der mobilen Outlook-App für iOS
- Einrichten von E-Mail in der Outlook für Android-App
- Optimieren der mobilen Outlook-App für Ihr iOS- oder Android-Smartphone

#### **IMPORTANT**

Um die App-basierten Richtlinien für bedingten Zugriff zu verwenden, muss die Microsoft Authenticator-App auf iOS-Geräten installiert werden. Für Android-Geräte wird die App für das Intune-Unternehmensportal verwendet. Weitere Informationen finden Sie unter [App-basierter bedingter Zugriff mit Intune](#).

## Verwenden der Enterprise Mobility + Security-Suite zum Schutz von Unternehmensdaten mit Outlook für iOS und Android

#### **IMPORTANT**

Die Liste zulassen/blockieren/Quarantä (ABQ) bietet keine Garantie für Sicherheit (wenn ein Client die Kopfzeile DeviceType Spoofing, Umständen ist es möglich umgehen für einen bestimmten Gerätetyp blockieren). Um sichere Einschränken des Zugriffs auf bestimmte Gerätetypen, wird empfohlen, Sie bedingte Zugriffsrichtlinien konfigurieren. Weitere Informationen finden Sie unter [App-basierte bedingten Zugriff mit Intune](#).

Die umfassendsten Schutzfunktionen für Office 365-Daten sind verfügbar, wenn Sie ein Abonnement für die Enterprise Mobility + Security-Suite abschließen, das Microsoft Intune und Azure Active Directory Premium-Features, z. B. bedingten Zugriff, umfasst. Sie sollten mindestens eine Richtlinie für bedingten Zugriff, die nur Konnektivität mit Outlook für iOS und Android von mobilen Geräten aus zulässt, sowie eine Richtlinie für Intune-Schutz für Apps bereitstellen, durch die der Schutz der Unternehmensdaten sichergestellt wird.

#### **NOTE**

Das Abonnement der Enterprise Mobility + Security-Suite umfasst zwar sowohl Microsoft Intune als auch Azure Active Directory Premium, Kunden können aber Lizenzen für Microsoft Intune und Azure Active Directory Premium auch separat erwerben. Alle Benutzer müssen für die Verwendung der Richtlinien für bedingten Zugriff und Intune-Schutz für Apps, die in diesem Artikel besprochen werden, lizenziert sein.

## Blockieren aller E-Mail-Apps mit Ausnahme von Outlook für iOS und Android mithilfe des bedingten Zugriffs

Sobald sich Ihre Organisation entschlossen hat, den Benutzerzugriff auf Exchange-Daten zu standardisieren und Outlook für iOS und Android als die einzige E-Mail-App für Endbenutzer einzusetzen, kann eine Richtlinie für bedingten Zugriff konfiguriert werden, die andere mobile Zugriffsmethoden blockiert. Zu diesem Zweck benötigen Sie zwei Richtlinien für bedingten Zugriff, wobei jede Richtlinie auf alle potenziellen Benutzer abzielt. Informationen zum Erstellen dieser Richtlinien finden Sie unter [App-basierter bedingter Zugriff mit Azure Active Directory](#).

1. Die erste Richtlinie lässt Outlook für iOS und Android zu und verhindert, dass OAuth-fähige Exchange ActiveSync-Clients eine Verbindung zu Exchange Online herstellen. Weitere Informationen finden Sie unter „Schritt 1 - Konfigurieren einer Azure AD-Richtlinie für bedingten Zugriff für Exchange Online“.
2. Durch die zweite Richtlinie wird verhindert, dass Exchange ActiveSync-Clients über die Standardauthentifizierung eine Verbindung zu Exchange Online herstellen. Weitere Informationen finden Sie unter „Schritt 2 - Konfigurieren einer Azure AD-Richtlinie für bedingten Zugriff für Exchange Online mit ActiveSync (EAS)“.

Die Richtlinien nutzen das Gewährungssteuerelement [Genehmigte Client-App erfordern](#), durch das sichergestellt wird, dass nur Microsoft-Apps, in die das Intune SDK integriert ist, Zugriff gewährt wird.

#### NOTE

Nachdem die bedingte Zugriffsrichtlinien aktiviert sind, kann es bis zu 6 Stunden für alle zuvor verbundenen mobilen Gerät blockiert werden. Mobiles Gerätezugriffsregeln (zulassen, blockieren oder Quarantäne) in Exchange Online werden übersprungen, wenn der Zugriff durch eine bedingte Zugriffsrichtlinie verwaltet wird, die entweder [erfordern ein Gerät, um als kompatibel markiert werden](#) oder [erfordern Client app genehmigt](#) enthält. Um app-basierte bedingte Zugriffsrichtlinien nutzen zu können, muss die Microsoft Authenticator app auf iOS-Geräten installiert werden. Für Android-Geräte wird die app Unternehmensportal Intune genutzt. Weitere Informationen finden Sie unter [App-basierte bedingten Zugriff mit Intune](#).

### Schützen von Unternehmensdaten in Outlook für iOS und Android mit Richtlinien für Intune-Schutz für Apps

Unabhängig davon, ob das Gerät in einer MDM-Lösung registriert ist, muss eine Richtlinie für Intune-Schutz für Apps sowohl für iOS- als auch für Android-Apps erstellt werden, und zwar über die Schritte in [Erstellen und Zuweisen von App-Schutzrichtlinien](#). Diese Richtlinien müssen mindestens die folgenden Bedingungen erfüllen:

1. Sie umfassen alle mobilen Microsoft-Anwendungen, z. B. Word, Excel oder PowerPoint, da dadurch sichergestellt wird, dass Benutzer auf Unternehmensdaten zugreifen und diese auf sichere Weise in einer Microsoft-App bearbeiten können.
2. Sie simulieren die Sicherheitsfunktionen, die Exchange für mobile Geräte bereitstellt, z. B.:
  - Für den Zugriff ist eine PIN erforderlich (die „Typ auswählen“, „PIN-Länge“, „Einfache PIN zulassen“ und „Fingerabdruck zulassen“ umfasst)
  - Verschlüsseln von App-Daten
  - Blockieren der Ausführung von verwalteten Apps auf per Jailbreak oder Rooting manipulierten Geräten
3. Sie sind für alle Benutzer zugewiesen. Dadurch wird sichergestellt, dass alle Benutzer geschützt sind, unabhängig davon, ob sie Outlook für iOS und Android verwenden.

Zusätzlich zu den oben genannten minimalen Richtlinienanforderungen, sollten Sie in Erwägung ziehen, Richtlinieneinstellungen für erweiterten Schutz bereitzustellen, z. B. **Ausschneiden, Kopieren und Einfügen mit anderen Apps einschränken**, um Datenlecks weiter zu verhindern. Weitere Informationen zu den verfügbaren Einstellungen finden Sie unter [Einstellungen für Android-App-Schutzrichtlinien in Microsoft Intune](#) und [Einstellungen für App-Schutzrichtlinien für iOS](#).

#### IMPORTANT

Um Intune-App-Schutzrichtlinien für Apps auf Android-Geräten anzuwenden, die nicht in Intune registriert sind, muss der Benutzer auch das Intune-Unternehmensportal installieren. Weitere Informationen finden Sie unter [Das passiert, wenn Ihre Android-App von App-Schutzrichtlinien verwaltet wird](#).

## Verwenden der mobilen Geräteverwaltung für Office 365

Wenn Sie nicht die Enterprise Mobility + Security-Suite nutzen möchten, können Sie die Verwaltung mobiler Geräte (MDM) für Office 365 verwenden. Für diese Lösung müssen mobile Geräte registriert werden. Wenn ein Benutzer versucht, auf Exchange Online mit einem Gerät zuzugreifen, das nicht registriert ist, wird verhindert, dass der Benutzer auf die Ressource zugreift, bis das Gerät registriert ist.

Da dies eine Lösung zur Geräteverwaltung ist, gibt es keine systemeigene Funktion, um zu steuern, welche Apps verwendet werden können, auch nachdem das Gerät registriert wurde. Wenn Sie den Zugriff auf Outlook für iOS

und Android beschränken möchten, müssen Sie Azure Active Directory Premium-Lizenzen erwerben und die Richtlinien für bedingten Zugriff verwenden, wie unter [Blockieren aller E-Mail-Apps mit Ausnahme von Outlook für iOS und Android mithilfe des bedingten Zugriffs](#) beschrieben.

Ein globaler Office 365-Administrator muss folgende Schritte ausführen, um MDM für Office 365 zu aktivieren und einzurichten. Vollständige Schritte finden Sie unter [Einrichten der Verwaltung mobiler Geräte \(MDM\) in Office 365](#). Zusammenfassend umfassen diese Schritte Folgendes:

1. Aktivieren von MDM für Office 365, indem Sie die folgenden Schritte im Security & Compliance Center ausführen.
2. Einrichten von MDM für Office 365 durch Erstellen eines APN-Zertifikats zum Verwalten von iOS-Geräten und durch Hinzufügen eines DNS-Eintrags für Ihre Domäne zur Unterstützung von Windows-Telefonen.
3. Erstellen von Geräterichtlinien und Anwenden der Richtlinie auf Benutzergruppen. In diesem Fall erhalten Ihre Benutzer eine Registrierungsnachricht auf ihrem Gerät. Wenn sie die Registrierung abgeschlossen haben, werden ihre Geräte von den Richtlinien eingeschränkt, die Sie eingerichtet haben.

#### **NOTE**

In MDM für Office 365 erstellte Richtlinien und Zugriffsregeln überschreiben Exchange-Postfachrichtlinien für mobile Geräte und Zugriffsregeln für Geräte, die in der Exchange-Verwaltungskonsole erstellt wurden. Nachdem ein Gerät in MDM für Office 365 registriert wurde, wird die Exchange-Postfachrichtlinie für mobile Geräte oder eine auf das Gerät angewandte Gerätezugriffsregel ignoriert.

## Verwenden von Exchange Online-Richtlinien für mobile Geräte

Wenn Sie nicht die Enterprise Mobility + Security-Suite oder die MDM für Office 365-Funktionen nutzen möchten, können Sie eine Exchange-Postfachrichtlinie für mobile Geräte zum Schutz des Geräts sowie Gerätezugriffsregeln zur Einschränkung der Gerätekonnektivität implementieren.

### **Postfachrichtlinie für mobile Geräte**

Outlook für iOS und Android unterstützt die folgenden Einstellungen für Postfachrichtlinien für mobile Geräte in Exchange Online:

- Gerätverschlüsselung aktiviert
- Min. Kennwortlänge
- Kennwort aktiviert

Informationen zum Erstellen oder Ändern einer vorhandenen Postfachrichtlinie für mobile Geräte finden Sie unter [Postfachrichtlinien für mobile Geräte in Exchange Online](#).

Darüber hinaus unterstützt Outlook für iOS und Android die Geräturücksetzungsfunktion von Exchange Online. Wenn diese ausgeführt wird, wird nur die App zurückgesetzt, da Exchange Online die Outlook für iOS und Android-App als das mobile Gerät betrachtet. Weitere Informationen zum Ausführen einer Remotezurücksetzung finden Sie unter [Zurücksetzen eines mobilen Geräts in Office 365](#).

#### **NOTE**

Outlook für iOS und Android unterstützt nur den Befehl für die Remotezurücksetzung „Daten löschen“; die Option der Remotezurücksetzung nur für das Konto wird nicht unterstützt.

### **Richtlinie für Gerätezugriff**

Outlook für iOS und Android sollte standardmäßig aktiviert sein. In einigen vorhandenen Exchange Online-

Umgebungen ist die App jedoch möglicherweise blockiert. Das kann verschiedene Gründe haben. Sobald sich Ihre Organisation entschlossen hat, den Benutzerzugriff auf Exchange-Daten zu standardisieren und Outlook für iOS und Android als die einzige E-Mail-App für Endbenutzer einzusetzen, können Sie andere E-Mail-Apps blockieren, die auf den iOS- oder Android-Geräten der Benutzer ausgeführt werden. Es gibt zwei Optionen zur Implementierung dieser Blockierungen innerhalb von Exchange Online: Die erste Option blockiert alle Geräte und erlaubt ausschließlich die Verwendung von Outlook für iOS und Android. Die zweite Option blockiert die Verwendung der nativen Exchange ActiveSync-Apps auf spezifischen Geräten.

### Option 1: Blockieren aller E-Mail-Apps mit Ausnahme von Outlook für iOS und Android

Sie können eine Block Standardregel definieren und konfigurieren Sie anschließend eine Regel zum gewähren für Outlook für iOS und Android und Windows-Geräten, über die folgenden Exchange Online PowerShell-Befehle. Diese Konfiguration wird verhindert, dass jede systemeigene Anwendung Exchange ActiveSync eine Verbindung herstellen, und lässt nur Outlook für iOS und Android.

1. Erstellen Sie die Standardblockierungsregel:

```
Set-ActiveSyncOrganizationSettings -DefaultAccessLevel Block
```

2. Erstellen Sie eine Zulassungsregel für Outlook für iOS und Android:

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceModel -QueryString "Outlook for iOS and Android" -AccessLevel Allow
```

3. **Optional:** Erstellen Sie Regeln, die Outlook auf Windows-Geräten den Aufbau von Exchange ActiveSync-Verbindungen erlauben („WP“ bedeutet Windows Phone, „WP8“ bedeutet Windows Phone 8 und höher und „WindowsMail“ steht für die in Windows 10 integrierte Mail-App):

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString "WP" -AccessLevel Allow  
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString "WP8" -AccessLevel Allow  
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString "WindowsMail" -AccessLevel Allow
```

### Option 2: Blockieren von nativen Exchange ActiveSync-Apps auf Android- und iOS-Geräten

Alternativ können Sie native Exchange ActiveSync-Apps auf bestimmten Android- und iOS-Geräten oder Geräten anderen Typs blockieren.

1. Vergewissern Sie sich, dass keine Regeln für den Exchange ActiveSync-basierten Gerätezugriff implementiert sind, die Outlook für iOS und Android blockieren:

```
Get-ActiveSyncDeviceAccessRule | where {$_.AccessLevel -eq "Block" -and $_.QueryString -like "Outlook*"} | ft Name,AccessLevel,QueryString -auto
```

<span data-ttu-id="ccd84-209">Entfernen Sie mit dem folgenden Befehl alle eventuell vorhandenen Gerätezugriffsregeln, die Outlook für iOS und Android blockieren:</span><span class="sxs-lookup"><span data-stu-id="ccd84-209">If any device access rules that block Outlook for iOS and Android are found, type the following to remove them:</span></span>

```
Get-ActiveSyncDeviceAccessRule | where {$_.AccessLevel -eq "Block" -and $_.QueryString -like "Outlook*"} | Remove-ActiveSyncDeviceAccessRule
```

2. Mithilfe der folgenden Befehle können Sie die meisten Android- und iOS-Geräte blockieren:

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString "Android" -AccessLevel Block  
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString "iPad" -AccessLevel Block  
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString "iPhone" -AccessLevel Block  
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString "iPod" -AccessLevel Block
```

3. Nicht alle Hersteller von Android-Geräten geben für das Merkmal „DeviceType“ den Wert „Android“ an. Möglicherweise legen Hersteller für jede veröffentlichte Version einen eigenen eindeutigen Wert fest. Generieren Sie mithilfe des folgenden Befehls einen Bericht über alle Geräte mit einer aktiven Exchange ActiveSync-Partnerschaft, um andere Android-Geräte zu finden, die auf Ihre Umgebung zugreifen:

```
Get-MobileDevice | Select-Object DeviceOS,DeviceModel,DeviceType | Export-Csv c:\temp\neasdevices.csv
```

4. Erstellen Sie je nach den Ergebnissen von Schritt 3 zusätzliche Blockierungsregeln. Wenn Sie beispielsweise feststellen, dass in Ihrer Umgebung sehr viele Android-Geräte des Typs „HTCOne“ genutzt werden, können Sie eine Exchange ActiveSync-Gerätezugriffsregel erstellen, die diesen spezifischen Gerätetyp blockiert, und so erzwingen, dass die Benutzer dieser Geräte Outlook für iOS und Android verwenden. In diesem Szenario würden Sie Folgendes eingeben:

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString "HTCOne" -AccessLevel Block
```

```
> [ !NOTE ]  
> <span data-ttu-id="ccd84-217">Der Parameter „QueryString“ akzeptiert keine Platzhalterzeichen oder Teilübereinstimmungen.</span><span class="sxs-lookup"><span data-stu-id="ccd84-217">The QueryString parameter does not accept wildcards or partial matches.</span></span>  
  
<span data-ttu-id="ccd84-218">**Weitere Ressourcen**:</span><span class="sxs-lookup"><span data-stu-id="ccd84-218">**Additional resources**:</span></span>
```

- [Neue ActiveSyncDeviceAccessRule](#)
- [Get-MobileDevice](#)
- [Set-ActiveSyncOrganizationSettings](#)

## Blockieren von Outlook für iOS und Android

Wenn Sie nicht möchten, dass Benutzer in Ihrer Organisation auf Exchange-Daten in Outlook für iOS und Android zugreifen, ist der von Ihnen gewählte Ansatz davon abhängig, ob Sie bedingte Azure Active Directory-Zugriffsrichtlinien oder Gerätezugriffsrichtlinien von Exchange Online verwenden.

### **Option 1: Blockieren des Zugriffs auf mobile Geräte mithilfe einer Richtlinie für bedingten Zugriff**

Bedingter Azure Active Directory-Zugriff bietet keinen Mechanismus, bei dem Sie Outlook für iOS und Android blockieren können und dabei gleichzeitig andere Exchange ActiveSync-Clients zulassen. Richtlinien für bedingten Zugriff können dennoch verwendet werden, um einen Zugriff mobiler Geräte auf zweierlei Arten zu blockieren:

- Option A: Blockieren des Zugriffs durch mobile Geräte auf iOS- und Android-Plattformen
- Option B: Blockieren des Zugriffs auf einer bestimmten Mobilgeräteplattform

### **Option A: Blockieren des Zugriffs durch mobile Geräte auf iOS- und Android-Plattformen**

Wenn Sie den Zugriff mobiler Geräte für alle Benutzer oder eine Untergruppe von Benutzern mithilfe des bedingten Zugriffs verhindern möchten, führen Sie die folgenden Schritte aus.

Erstellen Sie Richtlinien für bedingten Zugriff, wobei jede Richtlinie entweder auf alle Benutzer oder eine

Untermenge von Benutzern über eine Sicherheitsgruppe abzielt. Weitere Informationen finden Sie unter [App-basierter bedingter Zugriff mit Azure Active Directory](#).

1. Die erste Richtlinie blockiert Outlook für iOS und Android und verhindert, dass andere OAuth-fähige Exchange ActiveSync-Clients eine Verbindung zu Exchange Online herstellen. Weitere Informationen finden Sie unter „Schritt 1 - Konfigurieren einer Azure AD-Richtlinie für bedingten Zugriff für Exchange Online“. Für den fünften Schritt wählen Sie jedoch **Zugriff blockieren** aus.
2. Durch die zweite Richtlinie wird verhindert, dass Exchange ActiveSync-Clients über die Standardauthentifizierung eine Verbindung zu Exchange Online herstellen. Weitere Informationen finden Sie unter „Schritt 2 - Konfigurieren einer Azure AD-Richtlinie für bedingten Zugriff für Exchange Online mit ActiveSync (EAS)“.

### **Option B: Blockieren des Zugriffs auf einer bestimmten Mobilgeräteplattform**

Wenn Sie verhindern möchten, dass eine bestimmte Mobilgeräteplattform eine Verbindung zu Exchange Online herstellt, aber gleichzeitig zulassen möchten, dass Outlook für iOS und Android eine Verbindung mithilfe dieser Plattform herstellen kann, erstellen Sie die folgenden Richtlinien für bedingten Zugriff, wobei jede Richtlinie auf alle Benutzer abzielt. Weitere Informationen finden Sie unter [App-basierter bedingter Zugriff mit Azure Active Directory](#).

1. Die erste Richtlinie lässt Outlook für iOS und Android auf der bestimmten Mobilgeräteplattform zu und verhindert, dass andere OAuth-fähige Exchange ActiveSync-Clients eine Verbindung zu Exchange Online herstellen. Weitere Informationen finden Sie unter „Schritt 1 - Konfigurieren einer Azure AD-Richtlinie für bedingten Zugriff für Exchange Online“. Für Schritt 4a wählen Sie jedoch die gewünschte Mobilgeräteplattform aus (z. B. iOS), für die Sie Zugriff gewähren möchten.
2. Die zweite Richtlinie blockiert die App auf der bestimmten Mobilgeräteplattform und verhindert, dass andere OAuth-fähige Exchange ActiveSync-Clients eine Verbindung zu Exchange Online herstellen. Weitere Informationen finden Sie unter „Schritt 1 - Konfigurieren einer Azure AD-Richtlinie für bedingten Zugriff für Exchange Online“. Für Schritt 4a wählen Sie jedoch die gewünschte Mobilgeräteplattform aus (z. B. Android), für die Sie Zugriff blockieren möchten. Für Schritt 5 wählen Sie **Zugriff blockieren** aus.
3. Durch die dritte Richtlinie wird verhindert, dass Exchange ActiveSync-Clients über die Standardauthentifizierung eine Verbindung zu Exchange Online herstellen. Weitere Informationen finden Sie unter „Schritt 2 - Konfigurieren einer Azure AD-Richtlinie für bedingten Zugriff für Exchange Online mit ActiveSync (EAS)“.

### **Option 2: Blockieren von Outlook für iOS und Android mithilfe von Exchange-Zugriffsregeln für mobile Geräte**

Wenn Sie den Zugriff mobiler Geräte über die Gerätezugriffsregeln von Exchange Online verwalten, haben Sie zwei Möglichkeiten:

- Option A: Blockieren von Outlook für iOS und Android auf den Plattformen iOS und Android
- Option B: Blockieren von Outlook für iOS und Android auf einer bestimmten Mobilgeräteplattform

Jede Exchange-Organisation definiert eigene Richtlinien für Sicherheit und Geräteverwaltung. Kommt eine Organisation zu dem Schluss, dass Outlook für iOS und Android ihren Anforderungen nicht entspricht oder nicht die beste Lösung für ihren Anwendungsfall ist, können Administratoren die App blockieren. Ist die App blockiert, haben mobile Exchange-Benutzer in Ihrer Organisation über die integrierten Mail-Apps von iOS und Android weiterhin Zugriff auf ihr Postfach.

Die `New-ActiveSyncDeviceAccessRule` Cmdlet besitzt eine `Characteristic`-Parameter und drei `Characteristic` Optionen, mit denen Administratoren können das Outlook für iOS und Android-app zu blockieren. Die Optionen sind `UserAgent`, `DeviceModel` und `DeviceType`. In den beiden blockierenden Optionen in den folgenden Abschnitten beschrieben Sie verwenden eine oder mehrere der folgenden charakteristische Werte, um den Zugriff zu beschränken, die Outlook für iOS und Android auf die Postfächer in Ihrer Organisation hat.

In der folgenden Tabelle sind die Werte für jedes Merkmal aufgeführt:

MERKMAL	ZEICHENFOLGE FÜR IOS	ZEICHENFOLGE FÜR ANDROID
DeviceModel	Outlook für iOS und Android	Outlook für iOS und Android
DeviceType	Outlook	Outlook
UserAgent	Outlook-iOS/2.0	Outlook-Android/2.0

### Option A: Blockieren von Outlook für iOS und Android auf den Plattformen iOS und Android

Mit der `New-ActiveSyncDeviceAccessRule` -Cmdlet können eine Gerätezugriffsregel an, mit einer der `DeviceModel` oder `DeviceType` Merkmale. In beiden Fällen wird die Regel blockiert Outlook für iOS und Android für alle Plattformen und wird verhindert, dass jedes Gerät, auf dem Plattform iOS und Android-Plattform, den Zugriff auf ein Exchange-Postfach über die App.

Es folgen zwei Beispiele für eine Gerätezugriffsregel an. Im ersten Beispiel wird die `DeviceModel` Merkmal; im zweiten Beispiel wird die `DeviceType` Merkmale.

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceType -QueryString "Outlook" -AccessLevel Block
```

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceModel -QueryString "Outlook for iOS and Android" -AccessLevel Block
```

### Option B: Blockieren von Outlook für iOS und Android auf einer bestimmten Mobilgeräteplattform

Mit der `UserAgent` charakteristische, Sie können definieren eine Gerätezugriffsregel an, die über eine bestimmte Plattform Outlook für iOS und Android blockiert. Diese Regel wird verhindert, dass ein Gerät mit Outlook für iOS und Android Verbindung über die Plattform, die Sie angeben. Die folgenden Beispiele zeigen, wie Sie mit der gerätespezifischen Wert für die `UserAgent` Merkmale.

So blockieren Sie Android und lassen iOS zu:

```
New-ActiveSyncDeviceAccessRule -Characteristic UserAgent -QueryString "Outlook-Android/2.0" -AccessLevel Block  
New-ActiveSyncDeviceAccessRule -Characteristic UserAgent -QueryString "Outlook-iOS/2.0" -AccessLevel Allow
```

So blockieren Sie iOS und lassen Android zu:

```
New-ActiveSyncDeviceAccessRule -Characteristic UserAgent -QueryString "Outlook-Android/2.0" -AccessLevel Allow  
New-ActiveSyncDeviceAccessRule -Characteristic UserAgent -QueryString "Outlook-iOS/2.0" -AccessLevel Block
```

## Anwendungsrichtlinien in den Exchange-Webdiensten (EWS)

Neben Microsoft Intune, MDM für Office 365 und Exchange-Richtlinien für mobile Geräte kann der Zugriff, den mobile Geräte auf Informationen in Ihrer Organisation haben, auch über EWS-Anwendungsrichtlinien verwaltet werden. EWS-Anwendungsrichtlinien können steuern, ob Anwendungen die REST-API nutzen dürfen. Beachten Sie: Wenn Sie eine EWS-Anwendungsrichtlinie konfigurieren, die nur spezifischen Anwendungen Zugriff auf Ihre Messagingumgebung gewährt, müssen Sie die Benutzer-Agent-Zeichenfolge für Outlook für iOS und Android in die EWS-Zulassungsliste eintragen.

Das folgende Beispiel zeigt, wie Sie die Benutzer-Agent-Zeichenfolgen in die EWS-Zulassungsliste eintragen können:

```
Set-OrganizationConfig -EwsAllowList @{Add="Outlook-iOS/*","Outlook-Android/*"}
```

# Bereitstellen von Outlook für iOS und Android-app-Konfigurationseinstellungen

18.12.2018 • 20 minutes to read

**Zusammenfassung:** Gewusst wie: Anpassen des Verhaltens von Outlook für iOS und Android in Ihrer Exchange-Organisation.

Outlook für iOS und Android unterstützt app-Einstellungen, mit denen Office 365 und Verwaltung von mobilen Geräten (MDM), wie Intune, Administratoren zum Anpassen des Verhaltens der app.

Outlook für iOS und Android unterstützt die folgenden Konfigurationsszenarien:

- Setup-Kontokonfiguration
- Organisation Konten Modus zulässig
- Data Protection settings

Jedes Configuration-Szenario wird die spezifischen Anforderungen markieren. Beispielsweise gibt an, ob das Konfigurationsszenario erfordert Gerät-Registrierung und somit arbeiten mit jedem Provider MDM oder Intune App Protection Richtlinien erfordert.

## IMPORTANT

Für Konfigurationseinstellungen, die mit Android-Geräte über eine Android Enterprise Arbeit Profil und Outlook für Android registriert werden müssen muss über die verwalteten Google wiedergeben bereitgestellt werden, erforderlich Gerät Registrierung gespeichert werden. Weitere Informationen finden Sie unter [Einrichten von Registrierung von Android Arbeit Profil Geräte](#) und [Richtlinien für die Konfiguration von hinzufügen app für verwaltete Android-Geräte](#).

## Setup kontokonfigurationseinstellungen

Outlook für iOS und Android bietet Administratoren die Möglichkeit, Konto Konfigurationen für ihre Office 365-Benutzer "push". Diese Funktion funktioniert nur mit registrierten Geräten, wird jedoch mit jedem Provider MDM unterstützt. Wenn Sie nicht Intune verwenden, müssen Sie mit der MDM Dokumentation zur Bereitstellung dieser Einstellungen finden Sie in.

Weitere Informationen zu Setup Kontokonfiguration finden Sie unter [setup-Konto mit modernen Authentifizierung in Exchange Online](#).

SCHLÜSSEL	WERT	REGISTRIERUNG GERÄTETYP
com.microsoft.outlook.EmailProfile.EmailAddress	Dieser Wert gibt die E-Mail-Adresse an, die zum Senden und Empfangen von E-Mail verwendet werden soll. <b>Weretty:</b> Zeichenfolge <b>Akzeptierte Werte:</b> E-Mail-Adresse <b>Standard, wenn nicht angegeben:</b> <leer> <b>Erforderlich:</b> Ja <b>Beispiel:</b> user@companyname.com <b>Intune Token*</b> : {{Mail}}	Verwalteten Geräten

Schlüssel	Wert	Registrierung Gerätetyp
com.microsoft.outlook.EmailProfile.EmailUPN	<p>Dieser Wert gibt den Benutzerprinzipalnamen oder den Benutzernamen für das E-Mail-Profil an, das verwendet wird, um das Konto zu authentifizieren.</p> <p><b>Werttyp:</b> Zeichenfolge  <b>Akzeptierte Werte:</b> UPN-Adresse oder Benutzername  <b>Standard, wenn nicht angegeben:</b> &lt;leer&gt;  <b>Erforderlich:</b> Ja  <b>Beispiel:</b> userupn@companyname.com  <b>Intune Token*</b>: {{Userprincipalname}}</p>	Verwalteten Geräten
com.microsoft.outlook.EmailProfile.AccountType	<p>Dieser Wert gibt den Kontotyp an, der basierend auf dem Authentifizierungsmodell konfiguriert wird.</p> <p><b>Werttyp:</b> Zeichenfolge  <b>Akzeptierte Werte:</b> ModernAuth  <b>Erforderlich:</b> Ja  <b>Beispiel:</b> ModernAuth</p>	Verwalteten Geräten

## Organisation zulässig Konten-Einstellungen für den Modus

Outlook für iOS und Android bietet Administratoren die Möglichkeit zum Einschränken von e-Mails und Speicher-Anbieter-Konten auf nur Firmenkonten. Diese Funktion funktioniert nur mit registrierten Geräte. Es wird jedoch mit jedem Provider MDM unterstützt. Wenn Sie nicht Intune verwenden, müssen Sie mit der MDM Dokumentation zur Bereitstellung dieser Einstellungen finden Sie in.

Weitere Informationen über die Organisation zulässigen Konten Modus finden Sie in der [setup-Konto mit modernen Authentifizierung in Exchange Online](#).

Schlüssel	Wert	Plattform	Registrierung Gerätetyp
IntuneMAMAllowedAccountsOnly	<p>Dieser Wert gibt an, ob Organisation zulässig Kontomodus aktiv ist.</p> <p><b>Werttyp:</b> Zeichenfolge  <b>Akzeptierte Werte:</b> aktiviert, deaktiviert  <b>Erforderlich:</b> Ja  <b>Wert:</b> aktiviert</p>	iOS	Verwalteten Geräten
IntuneMAMUPN	<p>Dieser Wert gibt die User Principal Name für das Konto an.</p> <p><b>Werttyp:</b> Zeichenfolge  <b>Akzeptierte Werte:</b> UPN-Adresse  <b>Erforderlich:</b> Ja  <b>Beispiel:</b> userupn@companyname.com  <b>Intune Token*:</b> {{Userprincipalname}}</p>	iOS	Verwalteten Geräten

Schlüssel	Wert	Plattform	Registrierung Gerätetyp
com.microsoft.intune.mam.AllowedAccountUPNs	<p>Dieser durch Trennzeichen getrennte Wert gibt die UPNs erlaubte Organisation Kontomodus zulässig.</p> <p><b>Akzeptierte Werte:</b> UPN-Adresse</p> <p><b>Erforderlich:</b> Ja</p> <p><b>Beispiel:</b> userupn@companyname.com</p> <p><b>Intune Token*:</b> {{Userprincipalname}}</p>	Android	Verwalteten Geräten

## Data Protection settings

Outlook für iOS und Android unterstützt Richtlinien für die app für die folgenden Einstellungen von Data Protection, wenn die app von Intune verwaltet wird:

- Verwalten der Verwendung der wearable-Technologie
- Verwalten von e-Mail und Ihren Kalender Erinnerungen für iOS
- Verwalten von der App systemeigene Kontakte synchronisiert Kontaktfelder

Diese Einstellungen können unabhängig davon Gerätetestatus Registrierung der App bereitgestellt werden.

### Konfigurieren von Wearables für Outlook für iOS und Android (engl.)

Standardmäßig unterstützt Outlook für iOS und Android wearable-Technologie, sodass der Benutzer zum Empfangen von Benachrichtigungen über Textnachrichten und Ereignis Erinnerungen und die Möglichkeit für die Interaktion mit Nachrichten und tägliche Kalender anzeigen. Organisationen, die den Zugriff auf Unternehmensdaten auf Wearables deaktivieren möchten, können den folgenden Schlüssel über Richtlinien für die App bereitstellen.

Schlüssel	Wert	Registrierung Gerätetyp
com.microsoft.intune.mam.areWearablesAllowed	<p>Dieser Wert gibt an, ob Outlook-Daten mit einem Wearable-Gerät synchronisiert werden können. Wird der Wert auf False gesetzt, wird die Wearable-Synchronisierung deaktiviert.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> False</p>	Verwaltete apps

### Konfigurieren von Benachrichtigungen für Outlook für iOS

Die Architektur der Apple-Benachrichtigung wird sichergestellt, dass Benachrichtigungen auf iOS-Geräte und WatchOS gespiegelt werden. Welches Gerät die Benachrichtigung angezeigt, hängt davon ab, der Gerätetestatus: Wenn die Apple Watch nicht gesperrt ist und auf eine Handgelenk, während das Gerät iOS gesperrt ist, klicken Sie dann WatchOS den Benutzer mit der Benachrichtigung benachrichtigt wird. Apple bietet keinen Mechanismus, können Sie durch den Administrator steuern und Benachrichtigungen auf WatchOS verhindern, wobei weiterhin diese auf iOS-Geräte übermittelt werden.

Die folgenden Konfigurationseinstellungen werden Benachrichtigungen auf IOS- und WatchOS vollständig deaktiviert. Der Nachteil ist, dass der Endbenutzer nie neue e-Mail-Benachrichtigungen oder kalendererinnerungen auf iOS-Geräten angezeigt wird. Der Benutzer muss zum Starten des Outlook für iOS, um entdecken der neuen e-

Mail-Nachrichten oder finden Sie unter Termine im Kalender.

Schlüssel	Wert	Registrierung Gerätetyp
com.microsoft.outlook.Mail.NotificationsEnabled	<p>Dieser Wert gibt an, ob Outlook e-Mail-Benachrichtigungen werden kann. Festlegen des Werts auf False deaktiviert die e-Mail-Benachrichtigungen.</p> <p><b>Zulässige Werte:</b> True, False  <b>Standard, wenn nicht angegeben:</b> True  <b>Beispiel:</b> False</p>	Verwaltete apps
com.microsoft.outlook.Mail.NotificationsEnabled.UserChangeAllowed	<p>Dieser Wert gibt an, wenn der Benutzer anpassen kann die e-Mail-Benachrichtigung Einstellung innerhalb der App, die den Wert auf False festlegen den Benutzer verhindert, dass die Einstellung e-Mail-Benachrichtigung anpassen.</p> <p><b>Zulässige Werte:</b> True, False  <b>Standard, wenn nicht angegeben:</b> True  <b>Beispiel:</b> False</p>	Verwaltete apps
com.microsoft.outlook.Calendar.NotificationsEnabled	<p>Dieser Wert gibt an, ob Outlook Erinnerungen Kalender zulassen. Festlegen des Werts auf False deaktiviert Kalender Erinnerung Benachrichtigungen.</p> <p><b>Zulässige Werte:</b> True, False  <b>Standard, wenn nicht angegeben:</b> True  <b>Beispiel:</b> False</p>	Verwaltete apps
com.microsoft.outlook.Calendar.NotificationsEnabled.UserChangeAllowed	<p>Dieser Wert gibt an, wenn der Benutzer angepasst werden kann die Einstellung der Erinnerung Calendar Benachrichtigung innerhalb der App, die den Wert auf False festlegen den Benutzer verhindert, dass die Kalender Erinnerung Benachrichtigung Einstellung anpassen.</p> <p><b>Zulässige Werte:</b> True, False  <b>Standard, wenn nicht angegeben:</b> True  <b>Beispiel:</b> False</p>	Verwaltete apps

#### Konfigurieren von Kontakt Feld Synchronisierung mit systemeigenen Kontakte für Outlook für iOS und Android (engl.)

Die Einstellungen in der folgenden Tabelle können Sie die Kontaktfelder steuern, die zwischen Outlook auf iOS und Android und die systemeigene Kontakte Applications synchronisiert werden.

##### NOTE

Outlook für Android unterstützt bidirektionale Synchronisierung Netzwerkkontakte. Jedoch, wenn ein Benutzer ein Feld in der systemeigenen Kontakte app, die bearbeitet (wie das Feld **Notizen**) beschränkt ist, werden anschließend diese Daten nicht wieder in Outlook für Android synchronisieren.

Schlüssel	Wert	Registrierung Gerätetyp
com.microsoft.outlook.ContactSync.AddressAllowed	<p>Dieser Wert gibt an, ob die Adresse des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.BirthDayAllowed	<p>Dieser Wert gibt an, ob das Geburtsdatum des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.CompanyAllowed	<p>Dieser Wert gibt an, ob der Unternehmensname des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.DepartmentAllowed	<p>Dieser Wert gibt an, ob die Abteilung des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.EmailAllowed	<p>Dieser Wert gibt an, ob die E-Mail-Adresse des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.InstantMessageAllowed	<p>Dieser Wert gibt an, ob die Chatadresse des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.JobTitleAllowed	<p>Dieser Wert gibt an, ob die Position des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps

Schlüssel	Wert	Registrierung Gerätetyp
com.microsoft.outlook.ContactSync.NicknameAllowed	<p>Dieser Wert gibt an, ob der Spitzname des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.NotAllowed	<p>Dieser Wert gibt an, ob die Notizen des Kontakts mit systemeigenen Kontakten synchronisiert werden sollen.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.PhoneHomeAllowed	<p>Dieser Wert gibt an, ob die private Telefonnummer des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.PhoneHomeFaxAllowed	<p>Dieser Wert gibt an, ob die private Faxnummer des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.PhoneMobileAllowed	<p>Dieser Wert gibt an, ob die Mobiltelefonnummer des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.PhoneOtherAllowed	<p>Dieser Wert gibt an, ob die sonstige Telefonnummer des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps

Schlüssel	Wert	Registrierung Gerätetyp
com.microsoft.outlook.ContactSync.PhonePagerAllowed	<p>Dieser Wert gibt an, ob die Pager-Telefonnummer des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.PhoneWorkAllowed	<p>Dieser Wert gibt an, ob die dienstliche Telefonnummer des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.PhoneWorkFaxAllowed	<p>Dieser Wert gibt an, ob die dienstliche Faxnummer des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.PrefixAllowed	<p>Dieser Wert gibt an, ob das Anrede des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps
com.microsoft.outlook.ContactSync.SuffixAllowed	<p>Dieser Wert gibt an, ob das Namenssuffix des Kontakts mit systemeigenen Kontakten synchronisiert werden soll.</p> <p><b>Zulässige Werte:</b> True, False</p> <p><b>Standard, wenn nicht angegeben:</b> True</p> <p><b>Beispiel:</b> True</p>	Verwaltete apps

## Bereitstellen der Konfigurationsszenarien mit Microsoft Intune

Wenn Sie Microsoft Intune als Ihrem mobilen Gerät Management Anbieter verwenden, können die folgenden Schritte aus Sie eine app Konfiguration zu erstellen. Nach die Konfiguration erstellt wurde, können Sie ihre Einstellungen für Benutzergruppen zuweisen.

### NOTE

Intune verwalteten apps wird Einchecken mit einem Intervall von 30 Minuten für Konfigurationsrichtlinie für Intune App-Status, wenn in Verbindung mit einer Richtlinie Intune App Schutz bereitgestellt. Wenn eine Richtlinie Intune App Schutz, die dem Benutzer zugewiesen ist nicht, wird das App-Konfigurationsrichtlinie Intune Einchecken Intervall auf 720 Minuten festgelegt.

## IMPORTANT

Bei der Bereitstellung von Richtlinien für die app zu verwalteten Geräten können Probleme auftreten, wenn mehrere Richtlinien andere Werte für die gleiche Configuration-Schlüssel sind und für den gleichen app und die Benutzer vorgesehen sind. Dies ist aufgrund der mangelnden einen Konflikt Lösung Mechanismus für die Beilegung von unterschiedliche Werte. Sie können dies verhindern, indem Sie sicherstellen, dass nur eine einzelne app-Konfigurationsrichtlinie für verwaltete Geräten definiert und für den gleichen app und die Benutzer vorgesehen ist.

## Erstellen einer App-Konfigurationsrichtlinie für Outlook für iOS und Android

1. Melden Sie sich beim Azure-Portal an.
2. Wählen Sie **Weitere Dienste > Überwachung und Verwaltung > Intune**.
3. Wählen Sie auf dem **Client apps** Blade der Liste verwalten **Richtlinien für die App**.
4. Klicken Sie auf dem Blatt **App-Konfigurationsrichtlinien** auf **Hinzufügen**.
5. Geben Sie auf dem Blatt **App-Konfiguration hinzufügen** einen **Namen** und eine optionale **Beschreibung** für die App-Konfigurationseinstellungen ein.
6. Für **Gerät Registrierungs** -Typ Wählen Sie **verwaltete apps** oder **verwaltete Geräte** je nach Konfigurationsszenario Sie bereitstellen werden (siehe die Konfigurationsszenarien für Weitere Informationen).
7. Wenn Sie **verwaltete Geräte** ausgewählt haben, müssen Sie eine weitere Möglichkeit, **Plattform**. Wählen Sie für die **Plattform ios-** oder **Android**.
8. **Zugeordneter app**wählen Sie **die erforderliche app auswählen**und dann auf das Blade **gezielte apps** die Option **Outlook**. Wenn Sie **verwaltete apps**angegeben, wählen Sie die iOS und Android-Plattform Outlook-apps.

### NOTE

Wenn Outlook nicht als eine app verfügbar aufgeführt ist, müssen Sie es hinzufügen durch Befolgen der Anweisungen in [apps für Android Arbeit Profil Geräte mit Intune zuweisen](#) und [Hinzufügen iOS-apps in Microsoft Intune speichern](#).

9. Klicken Sie auf **OK**, um zum Blatt **App-Konfiguration hinzufügen** zurückzukehren.
10. Wählen Sie **Konfigurationseinstellungen** aus. Definieren Sie auf dem Blatt **Konfiguration** die Schlüssel- und Wert-Paare, die Konfigurationen für Outlook für iOS und Android bereitstellen sollen. Die Schlüssel- und Wert-Paare, die Sie definieren können, werden in den folgenden Abschnitten beschrieben.
11. Wenn Sie fertig sind, klicken Sie auf **OK**.
12. Wählen Sie auf der Blade **-app-Konfiguration hinzufügen Hinzufügen**.

Die neu erstellte Konfiguration wird auf dem Blatt **App-Konfiguration** angezeigt.

### NOTE

Wenn Sie **verwaltete Geräte**ausgewählt haben, müssen Sie eine separaten app Konfigurationsrichtlinie für jede Plattform zu erstellen. Darüber hinaus müssen Outlook über das Portal Unternehmen in der Reihenfolge für die Konfigurationseinstellungen wirksam werden installiert werden.

## Zuweisen der von Ihnen erstellten Konfigurationseinstellungen

Sie weisen die Einstellungen Gruppen von Benutzern in Azure Active Directory zu. Wenn ein Benutzer die

Microsoft Outlook-App installiert hat, wird die App von den Einstellungen verwaltet, die Sie angegeben haben.  
Gehen Sie zu diesem Zweck wie folgt vor:

1. Wählen Sie auf dem Blatt **Intune** das Blatt **Mobile Apps** der Liste „Verwalten“ und dann die Option **App-Konfigurationsrichtlinien** aus.
2. Wählen Sie aus der Liste der App-Konfigurationsrichtlinien diejenige aus, die Sie zuweisen möchten.
3. Wählen Sie auf dem nächsten Blatt **Aufgaben** aus.
4. Wählen Sie auf dem Blatt **Aufgaben** die Azure AD-Gruppe aus, der Sie die App-Konfiguration zuweisen möchten, und wählen Sie dann **OK**.

# Verwenden von Outlook für iOS und Android in der Government Community Cloud

18.12.2018 • 11 minutes to read

**Zusammenfassung:** Wie Organisationen in der Office 365 USA Government Community Cloud (GCC) Outlook für iOS und Android für ihre Benutzer aktivieren können.

Outlook für iOS und Android ist vollständig in der Microsoft-Cloud angelegt und umfasst nun eine Lösung, die Daten über Azure Government Community-Rechenzentren (die Azure Government Community-Cloud) weiterleitet. Diese Lösung ist FedRAMP-kompatibel und -genehmigt, was bedeutet, dass die Outlook für iOS und Android-Architektur und der zugrunde liegende Übersetzungsprotokolldienst jetzt die Datenverarbeitungsanforderungen für GCC-Mandanten erfüllen (diese Anforderungen werden von NIST Special Publication 800-145 definiert). Weitere Informationen finden Sie im Plan für Office 365 FedRAMP-Systemssicherheit, der sich im Abschnitt mit den FedRAMP-Überwachungsberichten des [Microsoft Service Trust Portals](#) befindet.

In diesem Artikel wird Folgendes behandelt:

- Aktivieren von Outlook für iOS und Android für neue Office 365 GCC-Kunden
- Aufheben der Blockierung von Outlook für iOS und Android für bestehende Office 365 GCC-Kunden, die in der öffentlichen Microsoft Azure-Cloud blockiert waren.
- Migrieren von mobilen Office 365 GCC-Benutzern aus der öffentlichen Azure-Cloud in die mit Office 365 GCC kompatible Lösung. Dies gilt für Mandanten, deren Blockierung für die öffentliche Azure-Cloud durch Unterzeichnen einer Verzichtserklärung mit Microsoft zuvor aufgehoben wurde.

## NOTE

Outlook für iOS und Android funktioniert zwar mit Office 365 GCC, funktioniert aber derzeit nicht in Office 365 GCC High- oder Office 365 DoD-Mandanten.

## Aktivieren von Outlook für iOS und Android für Office 365 GCC-Kunden

Die Anweisungen zum Aktivieren von Outlook für iOS und Android für Office 365 GCC-Kunden sind von der vorhandenen Bereitstellung abhängig. Es gibt:

1. Organisationen, die Outlook für iOS und Android derzeit überhaupt nicht verwenden.
2. Organisationen, die Outlook für iOS und Android derzeit mit der öffentlichen Azure-Cloud verwenden, nachdem eine Verzichtserklärung mit dem Microsoft-Support unterzeichnet wurde (die Verzichtserklärung zur Umgehung der Government Community Cloud).

### Für Organisationen, die Outlook für iOS und Android derzeit nicht verwenden

Für Office 365 GCC-Kunden, die Outlook für iOS und Android derzeit nicht verwenden, muss für das Aktivieren der App die Blockierung von Outlook für iOS und Android in der Organisation aufgehoben, die App auf die Geräten der Benutzer heruntergeladen und veranlasst werden, dass die Endbenutzer den GCC-Modus auf ihren Geräten aktivieren.

#### 1. Aufheben der Blockierung von Outlook für iOS und Android

Entfernen Sie alle Einschränkungen in Ihrer Exchange-Umgebung, die möglicherweise Outlook für iOS und Android blockieren. Dies bedeutet, dass Sie Ihre Anwendungsrichtlinien für Exchange-Webdienste, Ihre Zugriffsregeln für mobile Geräte in Exchange oder andere relevante Richtlinien für bedingten Zugriff in Azure Active Directory so aktualisieren müssen, dass die App nicht mehr blockiert wird. Informationen zur Aktivierung von Outlook als den einzigen Client für mobiles Messaging in der Organisation finden Sie unter [Sichern von Outlook für iOS und Android in Exchange Online](#).

## 2. Herunterladen und Installieren von Outlook für iOS und Android

Endbenutzer müssen die App auf ihren Geräten installieren. Wie die Installation abläuft, ist davon abhängig, ob die Geräte in einer MDM-Lösung (mobile Geräteverwaltung) registriert sind, z. B. Microsoft Intune. Benutzer mit registrierten Geräten können die App über die MDM-Lösung installieren, z. B. das Intune-Unternehmensportal. Benutzer mit Geräten, die nicht in einer MDM-Lösung registriert sind, können im Apple App Store oder im Google Play Store nach „Microsoft Outlook“ suchen und es von einem dieser Orte herunterladen.

### NOTE

Um die App-basierten Richtlinien für bedingten Zugriff zu verwenden, muss die Microsoft Authenticator-App auf iOS-Geräten installiert werden. Für Android-Geräte wird die App für das Intune-Unternehmensportal verwendet. Weitere Informationen finden Sie unter [App-basierter bedingter Zugriff mit Intune](#).

## 3. Veranlassen, dass Endbenutzer den GCC-Modus auf ihren Geräten aktivieren

Geben Sie Ihren Endbenutzern die folgenden Anweisungen, damit sie den GCC-Modus auf ihren Geräten aktivieren können. Die Anweisungen sind von dem Betriebssystem des jeweiligen Geräts abhängig.

Für iOS-Geräte:

1. Öffnen Sie „Einstellungen“ in iOS, führen Sie einen Bildlauf nach unten durch, um „Outlook“ zu suchen, und tippen Sie dann zum Auswählen darauf.
2. Ziehen Sie in den Outlook-Einstellungen die Umschaltfläche neben **App auf GCC-Konten beschränken** so, dass die Funktion aktiviert wird. Wenn Sie aufgefordert werden, vorhandene Konten zu entfernen, geben Sie „Ja“ an. Beenden Sie dann die Einstellungen.
3. Öffnen Sie Outlook, und fügen Sie dann das Office 365 GCC-Konto hinzu, indem Sie die Anweisungen auf dem Bildschirm befolgen. Verwenden Sie dabei Ihr Office 365 GCC-E-Mail-Konto sowie die entsprechenden Anmeldeinformationen.

Für Android-Geräte, die über eine neue Installation von Outlook für Android verfügen (d. h. ohne vorhandene E-Mail-Konten):

1. Öffnen Sie Outlook auf dem Android-Gerät.
2. Tippen Sie auf dem ersten Bildschirm auf **App auf GCC-Modus beschränken**.
3. Fügen Sie Ihr Office 365 GCC-Konto anhand der Anweisungen auf dem Bildschirm hinzu, und verwenden Sie dabei Ihr Office 365 GCC-E-Mail-Konto sowie die entsprechenden Anmeldeinformationen.

Für Android-Geräte, auf denen Outlook für Android bereits installiert ist:

1. Öffnen Sie Outlook, und wechseln Sie zu „Einstellungen“.
2. Ziehen Sie die Umschaltfläche neben **GCC-Modus** so, dass die Funktion aktiviert wird. Es wird eine Pop-up-Meldung angezeigt, die besagt, dass Ihre Konten und Einstellungen entfernt werden und dass Sie nur GCC-Konten hinzufügen können. Tippen Sie auf **Anwenden**.
3. Die App sollte automatisch neu gestartet werden. Ist dies nicht der Fall, schließen Sie die App manuell, und

starten Sie sie erneut.

4. Führen Sie die Anweisungen auf dem Bildschirm aus, um Ihr Office 365 GCC-Konto hinzuzufügen, und vergewissern Sie sich, dass der GCC-Modus aktiviert ist.

#### Für Organisationen, die nach Unterzeichnung der Verzichtserklärung zur Umgehung der Government Community Cloud derzeit Outlook für iOS und Android verwenden

Bevor Outlook für iOS und Android die Genehmigung und Zertifizierung von FedRAMP abruft, haben sich Office 365 GCC-Kunden möglicherweise entschieden, Outlook für iOS und Android über den Prozess der Verzichtserklärung zur Umgehung der Government Community Cloud zu verwenden, bei dem die Architektur der öffentlichen Azure-Cloud verwendet wird. Für Organisationen, die so vorgegangen sind, müssen Sie die folgenden Schritte ausführen, um das neue End-to-End-Angebot für Office 365 GCC für Outlook für iOS und Android nutzen zu können, das die Azure Government Community Cloud verwendet.

1. Stellen Sie eine Anfrage an den Microsoft-Support, um Ihren Mandanten aus der Whitelist mit Ausnahmen zu entfernen. Ihr Mandant wird dann von den öffentlichen Azure-Rechenzentren blockiert.

##### NOTE

Benutzer können daraufhin keine Verbindung zu ihren E-Mails mithilfe von Outlook für iOS und Android herstellen, benachrichtigen Sie Ihre Benutzer daher auf jeden Fall vorher.

2. Weisen Sie die Endbenutzer an, die entsprechenden Schritte im vorherigen Abschnitt auszuführen, um die Verwendung von Outlook für iOS und Android fortzusetzen.

## Dienste und Features nicht verfügbar

Die folgenden Dienste und Features von Outlook für iOS und Android sind nicht verfügbar für Benutzer von Community-Cloud der US-Regierung:

- **In app-Unterstützung:** Benutzer werden nicht supporttickets aus innerhalb der app zu übermitteln. Sie sollten wenden Sie sich an ihren internen Helpdesk und Protokolle (über die Diagnoseprotokolle freigeben-Option in der Einstellung Hilfe >). Falls erforderlich, der Organisation IT-Abteilung können Sie sich an Microsoft Support direkt.
- **In-app-Feature Anforderungen:** Benutzer werden nicht in der app-Feature Anforderungen übermitteln. Stattdessen werden Benutzer verwenden Sie [Outlook Uservoice](#) geleitet.
- **Mehrere Konten:** nur des Benutzers Office 365 GCC Konto und OneDrive for Business-Konto kann ein einzelnes Gerät hinzugefügt werden. Persönliche Konten können nicht hinzugefügt werden. Kunden können ein anderes Gerät für Persönliche Konten oder eines ActiveSync-Clients von einem anderen Anbieter verwenden.
- **Kalender-Apps:** Kalender-apps (Facebook, Wunderlist, Evernote, Meetup) sind nicht mit GCC Konten verfügbar.
- **Speicheranbieter:** nur der GCC Benutzer OneDrive for Business-Speicher-Konto in Outlook für iOS und Android hinzugefügt werden kann. Drittanbieter-Speicherkonten (z. B. Ablage, Feld) können nicht hinzugefügt werden.
- **Speicherort Services:** Bing Speicherort Dienste sind nicht mit GCC Konten zur Verfügung. Features, die auf Speicherort Dienste wie Cortana Zeit zu lassen, basieren sind ebenfalls nicht verfügbar.

# Mobiler Zugriff auf Exchange Online

18.12.2018 • 2 minutes to read

Benutzer können über zahlreiche unterschiedliche Geräte auf ihr Office 365-Postfach zugreifen. Mobiltelefone, Tablets, Laptops und sogar Geräte wie E-Reader. Diese Geräte können über Exchange ActiveSync, POP3 oder IMAP4 auf Daten in Office 365-Postfächern zugreifen.

## Exchange ActiveSync

Exchange ActiveSync ist ein Synchronisierungsprotokoll, das für die Zusammenarbeit mit Netzwerken mit langer Wartezeit und niedriger Bandbreite optimiert ist. Mithilfe des Protokolls, das auf HTTP und XML basiert, können Mobiltelefone auf die Informationen einer Organisation auf einem Server zugreifen, auf dem Microsoft Exchange ausgeführt wird. Exchange ActiveSync ermöglicht Benutzern von Mobiltelefonen den Zugriff auf ihre E-Mails, ihren Kalender, ihre Kontakte und Aufgaben sowie den Zugriff auf diese Informationen während des Offlinearbeits.

Exchange ActiveSync stellt die folgenden Funktionen bereit:

- Unterstützung für HTML-Nachrichten
- Unterstützung für Nachverfolgungsflag
- Gruppierung von E-Mails nach Unterhaltung
- Möglichkeit zum Synchronisieren einer gesamten Unterhaltung
- Unterstützung für das Anzeigen des Antwortstatus von Nachrichten
- Unterstützung für schnellen Nachrichtenabru
- Informationen zu Besprechungsteilnehmern
- Erweiterte Exchange-Suche
- PIN-Zurücksetzung
- Optimierte Gerätesicherheit durch Kennwortrichtlinien
- AutoErmittlung für drahtlose Bereitstellung
- Unterstützung für die Einstellung der automatischen Antwortfunktion, wenn Benutzer nicht verfügbar (abwesend, auf Reisen oder nicht im Büro) sind
- Unterstützung für Aufgabensynchronisierung
- Direct Push
- Unterstützung für Verfügbarkeitsinformationen für Kontakte

## POP3

POP3 wurde entwickelt, um die Offlineverarbeitung von E-Mails zu unterstützen. Mit POP3 werden E-Mails vom Server entfernt und auf dem lokalen POP3-Client gespeichert, sofern der Client nicht so konfiguriert wurde, dass Nachrichten auf dem Server verbleiben. Dadurch wird die Verantwortung für die Datenverwaltung und Sicherheit auf den Benutzer übertragen. POP3 bietet keine erweiterten Funktionen für die Zusammenarbeit, wie z. B. Kalender, Kontakte und Aufgaben.

## **IMAP4**

IMAP4 bietet sowohl Offline- als auch Onlinezugriff, doch wie POP3 bietet auch IMAP4 keine erweiterten Features für die Zusammenarbeit, wie Kalenderfunktionen, Kontakte und Aufgaben.

# Konfigurieren von Mobiltelefonen für den E-Mail-Zugriff

18.12.2018 • 2 minutes to read

Sie können einem Mobiltelefon, wie eine Windows Phone, verwenden von Microsoft Exchange ActiveSync konfigurieren. Sie sollten dieses Verfahren auf jedem Mobiltelefon in Ihrer Organisation ausführen.

## Voraussetzungen

- Sie haben die Herstellerdokumentation für das Mobiltelefon gelesen, das Sie konfigurieren möchten.
- Exchange ActiveSync ist in Ihrer Organisation aktiviert.

### NOTE

Gerätespezifische Informationen zum Einrichten von Microsoft Exchange-basierte e-Mail auf einem Telefon oder Tablet, finden Sie unter [Einrichten von einem mobilen Gerät mit Office 365 für Unternehmen](#).

## Konfigurieren eines Mobiltelefons für die Verwendung von Exchange ActiveSync

Die meisten Mobiltelefonen und-Geräten werden mithilfe der AutoErmittlung so konfigurieren Sie den mobile e-Mail-Client, damit Exchange ActiveSync verwendet werden können. Um ein e-Mail-Konto in den meisten Mobiltelefonen zu konfigurieren, benötigen Sie zwei Datenelemente Informationen.

- Die E-Mail-Adresse des Benutzers
- Das Kennwort des Benutzers

Wenn das Mobiltelefon wenden Sie sich an den Exchange-Server automatisch über AutoErmittlung kann, müssen Sie manuell das Mobiltelefon einrichten. Manuelles Setup ist erforderlich, e-Mail-Adresse des Benutzers und das Kennwort sowie den Namen des Exchange ActiveSync-Servers. In den meisten Unternehmen ist der Name des Exchange ActiveSync-Server den Servernamen Outlook Web App, ohne die OWA, beispielsweise mail.contoso.com identisch.

### Windows Phone-Synchronisierung

Wenn Sie ein Windows Phone-Mobiltelefon mit einem Exchange-Postfach über Exchange ActiveSync synchronisiert konfigurieren, werden nur eine Teilmenge der postfachrichtlinieneinstellungen für mobile Geräte unterstützt. Diese Richtlinieneinstellungen sind in [unterstützt Gerät Postfach Richtlinien für Windows Mobiltelefonen und mobilen Geräten](#)ausführlich beschrieben.

Wenn Sie Einstellungen für Postfachrichtlinien für mobile Geräte, die für die Version von Windows Phone nicht unterstützt werden, die Sie verwenden konfigurieren, müssen Sie auch festlegen die Einstellung auf "true", oder erstellen Sie eine separate Mobilgerät-Postfachrichtlinie für **AllowNonProvisionableDevices** Windows Phone-Mobile-Telefone.

# Ausführen einer Remotezurücksetzung auf einem Mobiltelefon

18.12.2018 • 4 minutes to read

Ihre Benutzer ausführen vertrauliche Unternehmensinformationen in ihre Fächer täglich ausgeführt. Wenn eine der Adressen auf dem Mobiltelefon verliert, können Ihre Daten in die Hände von einer anderen Person beenden. Wenn ein Benutzer auf dem Mobiltelefon verliert, können die Exchange-Verwaltungskonsole (EAC) oder Exchange Online PowerShell Sie ihre Telefonnummer Bereinigen der alle im Unternehmen und Benutzerinformationen Wischen.

## NOTE

Dieses Thema enthält auch Informationen zur Microsoft Outlook Web App verwenden Sie zum Ausführen einer Remotezurücksetzung auf einem Telefon. Der Benutzer muss Outlook Web App anmelden, um zum Ausführen einer Remotezurücksetzung.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Mobilgeräte" im Thema [Berechtigungen für Clients und mobile Geräte](#).
- Bei diesem Verfahren werden alle Daten auf dem Mobiltelefon einschließlich installierter Anwendungen, Fotos und persönlicher Daten gelöscht.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Was möchten Sie machen?

### Zurücksetzen des Telefons eines Benutzers über das Exchange Admin Center

Sie können über das EAC das Telefon eines Benutzers zurücksetzen oder eine noch nicht abgeschlossene Remotezurücksetzung abbrechen.

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Wählen Sie den Benutzer und unter **Mobilgeräte** den Befehl **Details anzeigen** aus.
3. Wählen Sie auf der Seite **Details des mobilen Geräts** das verlorene gegangene Mobilgerät aus, und klicken Sie auf **Daten zurücksetzen**.
4. Klicken Sie auf **Speichern**.

## **Verwenden von Exchange Online PowerShell, Telefon des Benutzers Wischen**

Sie können das Cmdlet **Clear-MobileDevice** im Exchange Online PowerShell verwenden Telefon des Benutzers zu löschen.

Über den folgenden Befehl wird das Gerät mit der Bezeichnung "WM\_TonySmith" zurückgesetzt und eine Bestätigungs Nachricht an "admin@contoso.com" gesendet.

```
Clear-MobileDevice -Identity WM_TonySmith -NotificationEmailAddresses "admin@contoso.com"
```

## **Verwenden Sie Outlook Web App löschen Telefon des Benutzers**

Ihre Benutzer können ihre eigenen Telefon mit Outlook Web App löschen.

1. Wählen Sie in Outlook Web App **Einstellungen > Telefon > Mobile Geräte**.
2. Wählen Sie das Mobiltelefon aus.
3. Klicken oder tippen Sie auf das Symbol **Gerät zurücksetzen**.

## **Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Es gibt mehrere Möglichkeiten zum Überprüfen, ob das Remotezurücksetzen erfolgt ist.

- Führen Sie das Cmdlet **Clear-MobileDevice**, mit dem *NotificationEmailAddresses* - Parameter konfiguriert. Eine Nachricht wird nach Abschluss der Remotezurücksetzung an die angegebene e-Mail-Adresse gesendet.
- Überprüfen Sie in der Exchange-Verwaltungskonsole den Status des mobilen Geräts. Der Status ändert sich von **Zurücksetzen steht aus in Remotegerätezurücksetzung war erfolgreich**.
- Überprüfen Sie in Outlook Web App den Status des mobilen Geräts. Der Status wird von **Ausstehenden Wischen für Erfolgreiche Wischen** geändert.

# Outlook Web App in Exchange Online

18.12.2018 • 2 minutes to read

In der Standardeinstellung Outlook im Web (vormals Outlook Web App) ist aktiviert in Exchange Online, und ermöglicht Benutzern, die von nahezu jedem beliebigen Webbrowser auf ihr Postfach zugreifen.

Informationen zu Methoden für den Clientzugriff Postfach in Exchange Online finden Sie unter [Clients und Mobilgeräte in Exchange Online](#).

## Übersicht über Outlook im Web

Vollständig unterstützte Webbrowser Benutzern Zugriff auf Features wie beispielsweise Unterhaltungsansicht, Posteingang Regeln, die im Lesebereich und der Terminplanung. Browzern, die nicht vollständig unterstützte können weiterhin verwendet werden, aber die Benutzer sehen die light-Version von Outlook im Web, die weniger Features verfügt.

## Verwalten von Outlook im Web

In Exchange Online kann das am häufigsten verwendete Outlook auf dem Web-Verwaltungsaufgaben in der Exchange-Verwaltungskonsole (EAC) ausgeführt werden. Alle diese Aufgaben und viele andere können mithilfe von Exchange Online PowerShell erreicht werden.

# Outlook auf dem Web-Postfachrichtlinien in Exchange Online

18.12.2018 • 2 minutes to read

In Exchange Online Outlook auf dem Web-Postfachrichtlinien steuern die Verfügbarkeit der Einstellungen und Features in Outlook im Web (vormals Outlook Web App). Ein Postfach kann nur eine Outlook auf die Web-Postfachrichtlinie angewendet haben. Sie können verschiedene Richtlinien für verschiedene Arten von Benutzern in Ihrer Exchange Online-Organisation erstellen.

Alle Exchange Online-Organisation verfügt über eine standardmäßige Outlook auf die Web-Postfachrichtlinie mit dem Namen OwaMailboxPolicy-Default, die auf alle Benutzerpostfächer angewendet wird. Sie können diese Richtlinie verwenden oder zusätzliche Richtlinien nach Bedarf an den Bedürfnissen Ihrer Organisation erstellen.

Die Verfahren, die Sie in Outlook auf dem Web-Postfachrichtlinien erledigen können, finden Sie unter [Outlook auf das Postfach Web Verfahren in Exchange Online](#).

# Outlook für die Web Postfach Richtlinie Prozeduren in Exchange Online

18.12.2018 • 2 minutes to read

[Erstellen einer Outlook auf die Web-Postfachrichtlinie in Exchange Online](#)

[Zuweisen oder Entfernen einer Outlook auf die Web-Postfachrichtlinie für ein Postfach in Exchange Online](#)

[Entfernen einer Outlook auf die Web-Postfachrichtlinie aus Exchange Online](#)

[Anzeigen oder Konfigurieren der Eigenschaften von Outlook im Web-Postfachrichtlinien](#)

# Erstellen einer Outlook auf die Web-Postfachrichtlinie in Exchange Online

18.12.2018 • 5 minutes to read

Sie können Outlook im Web-Postfachrichtlinien auf Einstellungen gelten für Benutzer in Outlook im Web (vormals Outlook Web App) erstellen. Outlook auf dem Web-Postfachrichtlinien eignen sich zum Anwenden und Standardisierung Einstellungen, beispielsweise für Anlagen, für bestimmte Gruppen von Benutzern.

Weitere Informationen zu Outlook auf dem Web-Postfachrichtlinien finden Sie unter [Outlook Web App-Postfachrichtlinien](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Outlook auf dem Web-Postfachrichtlinien" im Thema [Feature Permissions in Exchange Online](#).
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Erstellen einer Outlook auf die Web-Postfachrichtlinie

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Outlook Web App-Richtlinien**, und klicken Sie auf **neu**
2. Konfigurieren Sie in der neuen Richtlinienfenster, das geöffnet wird die folgenden Einstellungen:
  - **Richtliniename:** Geben Sie einen eindeutigen Namen für die Richtlinie ein.
  - Verwenden Sie die Kontrollkästchen, um Funktionen zu aktivieren oder zu deaktivieren. Standardmäßig werden die gängigsten Funktionen angezeigt. Klicken Sie auf **Weitere Optionen**, um alle Funktionen anzuzeigen, die aktiviert oder deaktiviert werden können.
3. **Hinweis:** Sie können Einstellungen für einzelne Benutzer mithilfe des **Set-CASMailbox** -Cmdlets in Exchange Online PowerShell konfigurieren.
5. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

# Verwenden Sie Exchange Online PowerShell, um ein Outlook auf die Web-Postfachrichtlinie zu erstellen

In Exchange Online PowerShell umfasst Erstellen einer Outlook auf die Web-Postfachrichtlinie zwei Schritte aus:

1. Erstellen Sie die Richtlinie mithilfe der folgenden Syntax ein:

```
New-OwaMailboxPolicy -Name "<Unique Name>"
```

Dieses Beispiel erstellt eine Outlook auf die Web-Postfachrichtlinie mit der Bezeichnung "Executives".

```
New-OwaMailboxPolicy -Name Policy1
```

Informationen zur Syntax und Parametern finden Sie unter [New-OwaMailboxPolicy](#).

2. Ändern Sie die Standardeinstellungen der Richtlinie.

Weitere Informationen finden Sie unter [Verwenden von Exchange Online PowerShell, Outlook auf dem Web-Postfachrichtlinien zu ändern](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

So stellen Sie sicher, dass Sie eine Outlook Web App-Postfachrichtlinie erfolgreich erstellt haben:

- Klicken Sie in der Exchange-Verwaltungskonsole auf **Berechtigungen > Outlook Web App-Richtlinien**, und suchen Sie nach der neuen Postfachrichtlinie.

Führen Sie zum Überprüfen, ob eine Outlook auf die Web-Postfachrichtlinie erfolgreich erstellt wurde, entweder über die folgenden Schritte aus:

- Klicken Sie in der Exchange-Verwaltungskonsole auf **Berechtigungen > Outlook Web App-Richtlinien**, und überprüfen Sie die Richtlinie wird aufgeführt. Sie können die Richtlinie auswählen und klicken Sie auf **Bearbeiten** So überprüfen Sie die Eigenschaften der Richtlinie.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl überprüfen, ob die Richtlinie aufgeführt wird:

```
Get-OwaMailboxPolicy | Format-Table Name
```

- Ersetzen Sie in Exchange Online PowerShell <Richtlinienname> mit dem Namen der Richtlinie, und führen den folgenden Befehl, um die Einstellungen zu überprüfen:

```
Get-OwaMailboxPolicy -Identity "<Policy Name>"
```

## Nächste Schritte

Zum Ändern einer vorhandenen Outlook auf die Web-Postfachrichtlinie finden Sie unter [anzeigen oder Konfigurieren von Outlook auf die Eigenschaften der Web-Postfachrichtlinie in Exchange Online](#).

# Zuweisen oder Entfernen einer Outlook auf die Web-Postfachrichtlinie für ein Postfach in Exchange Online

18.12.2018 • 11 minutes to read

Zuweisen einer Outlook auf die Web-Postfachrichtlinie an ein Postfach steuert das Outlook auf (vormals Outlook Web App) für die Webbenutzeroberfläche für den Benutzer. Sie können ein oder mehrere Postfächer Outlook auf dem Web-Postfachrichtlinien zuweisen oder entfernen die zugewiesenen Richtlinien in der Exchange-Verwaltungskonsole (EAC) oder Exchange Online PowerShell.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Outlook auf dem Web-Postfachrichtlinien" im Thema [Feature Permissions in Exchange Online](#).
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Anwenden von Outlook auf dem Web-Postfachrichtlinien auf Postfächer

### Anwenden eine Outlook auf die Web-Postfachrichtlinie auf ein Postfach mithilfe der Exchange-Verwaltungskonsole

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**.
2. Führen Sie einen der folgenden Schritte aus:
  - Wählen Sie ein Postfach aus, und klicken Sie dann auf **Bearbeiten** .
  - a. Klicken Sie in den Eigenschaften des Fensters Postfach, das geöffnet wird auf **Postfachfunktionen**.
  - b. Im Abschnitt **E-Mail-Konnektivität** unter **Outlook im Web: aktiviert**, klicken Sie auf **Details anzeigen**.
  - c. **Outlook Web App-Postfachrichtlinie** im Fenster Richtlinie, das geöffnet wird, klicken Sie auf **Durchsuchen**, suchen und wählen Sie die Richtlinie angewendet, und klicken Sie dann auf **OK**, wenn Sie fertig sind. Standardmäßig ist die Standardrichtlinie **OwaMailboxPolicy-Default** angewendet.

- d. Wenn Sie fertig sind, klicken Sie auf **Speichern** mehrmals.
- Wählen Sie mehrere Postfächer aus.
  1. Klicken Sie im Detailbereich suchen Sie **Outlook im Web**, und klicken Sie auf **eine Richtlinie zuweisen**.
  2. Weisen Sie in der Massen Fenster zu, das geöffnet wird, klicken Sie auf **Durchsuchen**, suchen und wählen Sie die Richtlinie angewendet und klicken Sie dann auf **OK**, wenn Sie fertig sind.
  3. Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

### **Verwenden von Exchange Online PowerShell anwenden eine Outlook auf die Web-Postfachrichtlinie auf ein Postfach**

Es gibt drei grundlegende Methoden, die Sie verwenden können, um eine Outlook auf die Web-Postfachrichtlinie auf Postfächer anzuwenden:

- **Einzelne Postfächer:** Verwenden Sie die folgende Syntax:

```
Set-CasMailbox -Identity <MailboxIdentity> -OwaMailboxPolicy "<Policy Name>"
```

In diesem Beispiel wird das Outlook auf die Web-Postfachrichtlinie tony@contoso.com namens Sales zugeordnet.

```
Set-CASMailbox -Identity tony@contoso.com -OwaMailboxPolicy "Sales Associates"
```

- **Filtern von Postfächern von Attributen:** Diese Methode erfordert, dass alle Postfächer ein eindeutiges filterbaren Attribut gemeinsam verwenden. Zum Beispiel:
  - Titel, Abteilung oder Adressinformationen für Benutzerkonten, die vom Cmdlet **Get-User** Ressourcenverfügbarkeitsdaten.
  - CustomAttribute1 über CustomAttribute15 für Postfächer von als gesehen, das Cmdlet **Get-Mailbox**.

Die Syntax verwendet die folgenden zwei Befehle (eins zum Identifizieren der Postfächer, und ein weiterer die Richtlinie auf die Postfächer angewendet):

```
$<VariableName> = <Get-User | Get-Mailbox> -ResultSize unlimited -Filter <Filter>
```

```
$<VariableName> | foreach {Set-CasMailbox -Identity $_.MicrosoftOnlineServicesID -OwaMailboxPolicy "<Policy Name>"}
```

Dieses Beispiel weist die Richtlinie namens-Manager und Führungskräfte auf alle Postfächer, deren **Title** - Attribut "Manager" oder "Executive" enthält.

```
$Mgmt = Get-User -ResultSize unlimited -Filter {(RecipientType -eq 'UserMailbox') -and (Title -like '*Manager*' -or Title -like '*Executive*')}
```

```
$Mgmt | foreach {Set-CasMailbox -Identity $_.MicrosoftOnlineServicesID -OwaMailboxPolicy "Managers and Executives"}
```

- **Verwenden einer Liste von bestimmte Postfächer:** Diese Methode erfordert eine Textdatei, um die

Postfächer zu identifizieren. Werte, die keine Leerzeichen (beispielsweise das Benutzerkonto) enthalten am besten. Die Textdatei muss ein Benutzerkonto in jeder Zeile wie die folgende enthalten:

```
akol@contoso.com
```

```
tjohnston@contoso.com
```

```
kakers@contoso.com
```

Die Syntax verwendet die folgenden zwei Befehle (eine, um die Benutzerkonten und andere anwenden die Richtlinie auf die Benutzer identifizieren):

```
$<VariableName> = Get-Content "<text file>"
```

```
$<VariableName> | foreach {Set-CasMailbox -Identity $_ -OwaMailboxPolicy "<Policy Name>"}
```

In diesem Beispiel wird die Richtlinie namens-Manager und Führungskräfte auf die Postfächer in der Datei C:\My Documents\Management.txt angegeben.

```
$Mgrs = Get-Content "C:\My Documents\Management.txt"
```

```
$Mgrs | foreach {Set-CasMailbox -Identity $_ -OwaMailboxPolicy "Managers and Executives"}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-CASMailbox](#).

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Verwenden Sie zum bestätigen, dass Sie eine Outlook auf die Web-Postfachrichtlinie an ein Postfach angewendet haben, können die folgenden Schritte aus:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer** und wählen Sie das Postfach. Im Bereich Details wechseln Sie zur **E-Mail-Konnektivität**, klicken Sie auf **Details anzeigen**, und überprüfen Sie den Namen der Richtlinie in **Outlook Web App**-Richtlinie im Postfachfenster, das angezeigt wird.
- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**, wählen Sie das Postfach aus, und klicken Sie auf **Bearbeiten**. Klicken Sie in den Eigenschaften des Fensters Postfach, das geöffnet wird auf **Postfachfunktionen**. Im Abschnitt **E-Mail-Konnektivität** unter **Outlook im Web: aktiviert**, klicken Sie auf **Details anzeigen**, und überprüfen Sie den Namen der Richtlinie in **Outlook Web App**-Richtlinie im Postfachfenster, das angezeigt wird.
- Ersetzen Sie in Exchange Online PowerShell <MailboxIdentity> mit dem Namen alias, e-Mail-Adresse oder den Kontonamen des Postfachs und führen Sie den folgenden Befehl aus, um den Wert der Eigenschaft **OwaMailboxPolicy** überprüfen:

```
Get-CasMailbox -Identity "<MailboxIdentity>" | Format-List OwaMailboxPolicy
```

- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um den Wert der Eigenschaft **OwaMailboxPolicy** überprüfen:

```
Get-CasMailbox -ResultSize unlimited | Format-Table -Auto Name,OwaMailboxPolicy
```

# Entfernen einer Outlook auf das Web Postfach richtlinienzuweisungen von Postfächern

## Verwenden der Exchange-Verwaltungskonsole zum Entfernen einer Outlook auf die Web Postfach Richtlinie-Zuordnung aus einem Postfach

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**, und wählen Sie das Postfach, das Sie ändern möchten.

2. Führen Sie einen Bildlauf bis **E-Mail-Konnektivität** durch, und klicken Sie auf **Details anzeigen**.

Wenn Sie eine Postfachrichtlinie zugewiesen wurde, klicken Sie auf **Clear X**, um die richtlinienzuweisung aus dem Postfach zu entfernen.

3. Wenn Sie fertig sind, klicken Sie auf **Speichern**, um zu speichern.

## Verwenden Sie Exchange Online PowerShell, um ein Outlook auf die Web Postfach Richtlinie Zuordnung aus einem Postfach entfernen

Wenn die Richtlinie-Zuordnung aus dem Postfach entfernen möchten, verwenden Sie die folgende Syntax:

```
Set-CasMailbox -Identity "<MailboxIdentity>" -OwaMailboxPolicy $null
```

Dieses Beispiel entfernt das Outlook auf die Web-Postfachrichtlinie aus den Benutzer tony@contoso.com-Postfach.

```
Set-CASMailbox -Identity tony@contoso.com -OwaMailboxPolicy $null
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-CASMailbox](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Verwenden Sie zum bestätigen, dass Sie eine Outlook auf die Web Postfach Richtlinie Zuordnung von einem Postfach entfernt haben, können die folgenden Schritte aus:

- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer** und wählen Sie das Postfach. Im Bereich Details wechseln Sie zur **E-Mail-Konnektivität**, klicken Sie auf **Details anzeigen**, und stellen Sie sicher, dass die Richtlinie im Richtlinienfenster **Outlook Web App**-Postfach, das angezeigt wird leer ist.
- Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger > Postfächer**. Klicken Sie in den Eigenschaften des Fensters Postfach, das geöffnet wird auf **Postfachfunktionen**. Im Abschnitt **E-Mail-Konnektivität** unter **Outlook im Web: aktiviert**, klicken Sie auf **Details anzeigen**, und überprüfen Sie die Richtlinie ist leer in **Outlook Web App**-Richtlinie im Postfachfenster, das angezeigt wird.
- Ersetzen Sie in Exchange Online PowerShell <MailboxIdentity> mit dem Namen alias, e-Mail-Adresse oder den Kontonamen des Postfachs und führen Sie den folgenden Befehl aus, um den Wert der Eigenschaft **OwaMailboxPolicy** überprüfen:

```
Get-CasMailbox -Identity "<MailboxIdentity>" | Format-List OwaMailboxPolicy
```

- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um den Wert der Eigenschaft **OwaMailboxPolicy** überprüfen:

```
Get-CasMailbox -ResultSize unlimited | Format-Table -Auto Name,OwaMailboxPolicy
```

# Entfernen einer Outlook auf die Web-Postfachrichtlinie aus Exchange Online

18.12.2018 • 3 minutes to read

Sie können eine Microsoft Outlook auf die Web-Postfachrichtlinie mithilfe der Exchange-Verwaltungskonsole (EAC) oder Exchange Online PowerShell aus einer Exchange-Organisation entfernen.

**Hinweis:** die integrierten Postfachrichtlinie mit dem Namen OwaMailboxPolicy-Default nicht entfernen.

Weitere Verwaltungsaufgaben im Zusammenhang mit Outlook auf dem Web-Postfachrichtlinien finden Sie unter [Outlook auf dem Web-Postfachrichtlinien](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Outlook auf dem Web-Postfachrichtlinien" im Thema [Feature Permissions in Exchange Online](#).
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden der Exchange-Verwaltungskonsole zum Entfernen einer Outlook auf die Web-Postfachrichtlinie

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Outlook Web App-Richtlinien**, wählen Sie die Richtlinie, die Sie entfernen möchten, und klicken Sie dann auf **Löschen**

2. Klicken Sie im Bestätigungsfenster klicken Sie auf **Ja**, um die Postfachrichtlinie zu entfernen, oder klicken Sie auf **Nein**, um abzubrechen.

## Verwenden Sie Exchange Online PowerShell, um eine Outlook auf die Web-Postfachrichtlinie zu entfernen

Verwenden Sie die folgende Syntax, um ein Outlook auf die Web-Postfachrichtlinie zu entfernen:

```
Remove-OwaMailboxPolicy -Identity "<Policy Name>"
```

Dieses Beispiel entfernt das Outlook auf die Web-Postfachrichtlinie mit dem Namen Sales zugeordnet.

```
Remove-OwaMailboxPolicy -Identity "Sales Associates"
```

Informationen zur Syntax und Parametern finden Sie unter [Remove-OwaMailboxPolicy](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum bestätigen, dass Sie eine Outlook auf die Web-Postfachrichtlinie erfolgreich entfernt haben, führen Sie die folgenden Schritte aus:

- Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Outlook Web App-Richtlinien** und überprüfen Sie die Richtlinie nicht mehr aufgeführt wird.
- Führen Sie in Exchange Online PowerShell den folgenden Befehl aus, um sicherzustellen, dass die Richtlinie nicht mehr aufgeführt wird:

```
Get-OwaMailboxPolicy
```

# Anzeigen oder Konfigurieren von Outlook auf die Eigenschaften der Web-Postfachrichtlinie in Exchange Online

18.12.2018 • 6 minutes to read

Nachdem ein Outlook auf die Web-Postfachrichtlinie erstellt wurde, können Sie eine Vielzahl von Optionen zum Steuern von den Funktionen für Benutzer in Outlook im Web (vormals Outlook Web App) konfigurieren. Sie können beispielsweise aktivieren oder Deaktivieren von Regeln für den Posteingang oder erstellen Sie eine Liste der zulässigen Dateitypen für Anlagen.

Weitere Informationen zu Outlook auf dem Web-Postfachrichtlinien finden Sie unter [Outlook Web App-Postfachrichtlinien](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 3 Minuten.
- Sie müssen Berechtigungen zugewiesen werden, bevor Sie dieses Verfahren oder Verfahren ausführen können. Welche Berechtigungen Sie benötigen, finden Sie unter den Eintrag "Outlook auf dem Web-Postfachrichtlinien" im Thema [Feature Permissions in Exchange Online](#).
- Um die Exchange-Verwaltungskonsole (EAC) zu öffnen, finden Sie unter [Exchange Admin center in Exchange Online](#). Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Anzeigen oder Konfigurieren von Outlook im Web-Postfachrichtlinien mithilfe der Exchange-Verwaltungskonsole

1. Wechseln Sie in der Exchange-Verwaltungskonsole zu **Berechtigungen > Outlook Web App-Richtlinien** und wählen Sie die Richtlinie, die Sie anzeigen oder konfigurieren möchten.
2. Im Detailbereich die aktivierte Features in der Richtlinie anzeigen. Klicken Sie auf **Bearbeiten**, um weitere Informationen finden Sie unter,  In den Eigenschaften können Sie daraufhin geöffneten Fenster anzeigen und konfigurieren Sie die folgenden Einstellungen:
  - Auf der Registerkarte **Allgemein** können Sie den Namen der Richtlinie anzeigen und ändern.
  - Verwenden Sie die Kontrollkästchen auf der Registerkarte **Features**, um Features zu aktivieren oder zu deaktivieren. Standardmäßig werden die gängigsten Funktionen angezeigt. Klicken Sie auf **Weitere Optionen**, um alle Funktionen anzuzeigen, die aktiviert oder deaktiviert werden können.

**Hinweis:** Sie können Einstellungen für einzelne Benutzer mithilfe des **Set-CASMailbox**-Cmdlets in

Exchange Online PowerShell konfigurieren.

- Verwenden Sie die Kontrollkästchen für den **direkten Dateizugriff** so konfigurieren Sie den Zugriff auf und Anzeigen von Optionen für Benutzer, klicken Sie auf der Registerkarte **Zugriff auf die Datei**. Dateizugriff ermöglicht dem Benutzer öffnen oder Anzeigen des Inhalts der Dateien, die an eine e-Mail-Nachricht angehängt.

Der Dateizugriff kann basierend darauf gesteuert werden, ob sich ein Benutzer bei einem öffentlichen oder privaten Computer angemeldet hat. Die Benutzeroption zur Auswahl des privaten oder öffentlichen Computerzugriffs steht nur zur Verfügung, wenn Sie mit der formularbasierten Authentifizierung arbeiten. Bei allen weiteren Formen der Authentifizierung wird von einem Zugriff auf einen privaten Computer ausgegangen.

- Verwenden Sie auf der Registerkarte **Offlinezugriff** die Optionsfelder, um die Verfügbarkeit des Offlinezugriffs zu konfigurieren.

3. Wenn Sie fertig sind, klicken Sie auf **Speichern**, um die Richtlinie zu aktualisieren.

## Verwenden Sie Exchange Online PowerShell, um Outlook auf dem Web-Postfachrichtlinien zu ändern.

Verwenden Sie die folgende Syntax, um eine Outlook auf die Web-Postfachrichtlinie zu ändern:

```
Set-OwaMailboxPolicy -Identity "<Policy Name>" [Settings]
```

In diesem Beispiel wird der Kalenderzugriff in der Standardpostfachrichtlinie geändert.

```
Set-OwaMailboxPolicy -Identity Default -CalendarEnabled $true
```

Informationen zur Syntax und Parametern finden Sie unter [Set-OwaMailboxPolicy](#).

## Verwenden von Exchange Online PowerShell zum Anzeigen von Outlook auf dem Web-Postfachrichtlinien

Um eine Outlook auf die Web-Postfachrichtlinie anzuzeigen, verwenden Sie die folgende Syntax:

```
Get-OwaMailboxPolicy [-Identity "<Policy Name>"]
```

In diesem Beispiel wird eine Übersichtsliste aller Richtlinien in der Organisation zurückgegeben.

```
Get-OwaMailboxPolicy | Format-Table Name
```

In diesem Beispiel werden detaillierte Informationen für die Richtlinie mit dem Namen "Executives" abgerufen.

```
Get-OwaMailboxPolicy -Identity Executives
```

Informationen zur Syntax und Parametern finden Sie unter [Get-OwaMailboxPolicy](#).

## Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Zum Überprüfen, ob eine Outlook auf die Web-Postfachrichtlinie erfolgreich geändert haben, führen Sie einen der folgenden Schritte aus:

- Klicken Sie in der Exchange-Verwaltungskonsole auf **Berechtigungen** > **Outlook Web App-Richtlinien**, wählen Sie die Richtlinie, klicken Sie auf **Bearbeiten** , und überprüfen Sie die Eigenschaften der Richtlinie.
- Ersetzen Sie in Exchange Online PowerShell <Richtlinienname> mit dem Namen der Richtlinie, und führen den folgenden Befehl, um die Einstellungen zu überprüfen:

```
Get-OwaMailboxPolicy -Identity "<Policy Name>"
```

# OWA for Devices contact sync

18.12.2018 • 4 minutes to read

Office 365-Benutzer können ihre Outlook Web App-Kontakte mit dem Adressbuch auf ihrem iPhone oder iPad synchronisieren, indem sie die Funktion „OWA für Geräte - Kontakte synchronisieren“ verwenden. Sie ist bereits für Benutzer von Outlook Web App aktiviert. Als Office 365-Administrator können Sie die Funktion deaktivieren, wenn Sie Probleme haben, die Synchronisierung der Kontakte des Benutzers für dessen iPhone oder iPad zu ermöglichen. Diese Einstellung gilt für alle Postfächer.

## Wie können Sie das ändern?

Wechseln Sie im Office 365-Portal zu **Admin > Dienstinstellungen > Mobiler Zugriff**.

- Aktivieren Sie die Funktion **OWA für Geräte - Kontakte synchronisieren**, damit Benutzer ihre Outlook Web App-Kontakte mit dem Adressbuch auf ihrem iPhone oder iPad synchronisieren können.
- Deaktivieren Sie die Funktion „OWA für Geräte - Kontakte synchronisieren“, damit Benutzer ihre Outlook Web App-Kontakte nicht mit dem Adressbuch auf ihrem iPhone oder iPad synchronisieren können.

## Was ist „OWA für Geräte - Kontakte synchronisieren“?

OWA für Geräte bezieht sich auf die Apps OWA für iPhone und OWA für iPad. Mit diesen beiden Apps können Benutzer ihr iPhone oder iPad zur Synchronisierung ihrer Outlook Web App-Kontakte mit dem Adressbuch des mobilen Geräts einrichten.

Office 365-Administratoren können die Funktion „OWA für Geräte - Kontakte synchronisieren“ verwenden, um zu steuern, ob Benutzer ihre Kontakte aus Outlook Web App synchronisieren können. Diese Funktion ist bereits aktiviert, wenn das Postfach eines Benutzers erstellt wird und Benutzern ermöglicht wird, ihre Geschäftskontakte auf mehreren iOS-Geräten kinderleicht zu verwalten. Wenn Sie allerdings Bedenken hinsichtlich des Datenschutzes oder der Sicherheit haben und die Kontaktinformationen für Ihre Organisation nicht für die iOS-Geräte Ihrer Benutzer oder die Dienste, die sie zum Speichern von Daten verwenden, freigegeben möchten, können Sie die Funktion „OWA für Geräte - Kontakte synchronisieren“ deaktivieren.

Wenn Sie die Funktion „OWA für Geräte - Kontakte synchronisieren“ deaktivieren, wird der Inhalt des Ordners mit den Outlook Web App-Kontakten eines Benutzers nicht in das Adressbuch des iOS-Geräts kopiert. Alle Kontaktinformationen, die zuvor mit den iOS-Geräten des Benutzers synchronisiert wurden, werden entfernt. Allerdings kann der Benutzer die Datenschutzeinstellung des iOS-Geräts so ändern, dass kein Zugriff auf Outlook Web Access möglich ist. In diesem Fall können die Daten nicht geändert oder entfernt werden. Nachdem Sie die Funktion „OWA für Geräte - Kontakte synchronisieren“ deaktiviert haben, kann es bis zu acht Stunden dauern, bis die Änderung wirksam wird.

„OWA für Geräte - Kontakte synchronisieren“ steuert die Synchronisierung nur für Benutzer, die mithilfe der Apps OWA für iPhone oder OWA für iPad eine Verbindung mit ihren Postfächern herstellen. Wenn Sie Exchange ActiveSync in Ihrer Organisation aktiviert haben und Benutzer ein ActiveSync-Konto eingerichtet haben, können Benutzer weiterhin ihre Kontakte mit einem mobilen Gerät synchronisieren. Exchange ActiveSync wird auf vielen mobilen Geräten angeboten und kann unterschiedliche Sicherheitsstufen für die Daten Ihrer Organisation bereitstellen.

# Öffentliche Anlagenverarbeitung in Exchange Online

18.12.2018 • 13 minutes to read

Als Administrator können Sie Einrichten von privaten und öffentlichen anlagenverarbeitung in Outlook im Web (vormals Outlook Web App), je nachdem, wie Sie Ihre Outlook Web App-Postfachrichtlinien konfigurieren. Die Einstellungen für (intern) privat und öffentlich (extern) Netzwerke definieren, wie Benutzer können öffnen, anzeigen, senden oder Empfangen von Anlagen, je nachdem, ob ein Benutzer bei Outlook Web App auf einem Computer angemeldet ist, die Teil einer privaten oder über ein öffentliches Netzwerk ist.

## Wie kann ich die öffentliche Anlagenverarbeitung steuern?

Es gibt, zwar sowohl Private (internes Netzwerk) und öffentliche (externe Netzwerke) Einstellungen für Anlagen mit Outlook Web App-Postfachrichtlinien zu steuern Admins erfordern konsistenter und zuverlässiger Anlage verarbeiten, wenn ein Benutzer bei Outlook Web App aus anmeldet ein Computer in einem öffentlichen Netzwerk wie in einem Café oder Bibliothek. Informationen zum Einrichten von externen Netzwerken für eine ganze Organisation in Exchange Online anlagenverarbeitung durchsetzen zuerst verwenden Sie das Cmdlet [Set-OrganizationConfig](#), legen Sie den Parameter *PublicComputersDetectionEnabled* auf `$true`, Konfigurieren Sie der richtigen Outlook Web App-Postfachrichtlinie mithilfe der Exchange-Verwaltungskonsole (EAC) oder das Cmdlet [Set-OwaMailboxPolicy](#), und Erstellen von Anspruchsregeln in AD FS. Durch Aktivieren dieser Einstellung die auf das [Set-OrganizationConfig](#) Cmdlet und die Anspruchsregeln erstellen aktivieren Exchange Online zum feststellen, ob ein Benutzer in Outlook Web App aus einem privaten und öffentlichen Netzwerk oder Computer anmelden.

Auf der Outlook Web App-postfachrichtlinienparameter in der folgenden Tabelle festgelegt werden sollte `$true` zum Aktivieren der Administrator die anlagenverarbeitung für öffentliche Computer und Netzwerke steuern.

PARAMETER*	BESCHREIBUNG
<i>DirectFileAccessOnPublicComputersEnabled</i>	Gibt an, mit der linken Maustaste und zu weiteren Optionen für Anlagen, wenn der Benutzer in Outlook Web App von einem Computer außerhalb eines Netzwerks privaten oder Firmennetzwerk angemeldet hat. Wenn dieser Parameter festgelegt ist, dass <code>\$true</code> , <b>Öffnen</b> und andere Optionen zur Verfügung stehen. Wenn diese Liste festgelegt ist, <code>\$false</code> , die Option <b>Öffnen</b> ist deaktiviert.
<i>ForceWacViewingFirstOnPublicComputers</i>	Gibt an, ob ein Benutzer, der sich von einem Computer außerhalb des privaten bzw. Unternehmensnetzwerks bei Outlook Web App angemeldet hat, eine Office-Datei direkt öffnen kann, ohne sie zuerst als Webseite anzuzeigen.
<i>ForceWebReadyDocumentViewingFirstOnPublicComputers</i>	Gibt an, ob ein Benutzer, der sich bei Outlook Web App angemeldet hat, ein Dokument direkt öffnen kann, ohne es zuerst als Webseite anzuzeigen.
<i>WacViewingOnPublicComputersEnabled</i>	Gibt an, ob ein Benutzer, der sich von einem Computer außerhalb des privaten bzw. Unternehmensnetzwerks bei Outlook Web App angemeldet hat, unterstützte Office-Dateien mit Outlook Web App anzeigen kann.

PARAMETER*	BESCHREIBUNG
<i>WebReadyDocumentViewingOnPublicComputersEnabled</i>	Gibt an, ob WebReady Document Viewing aktiviert ist, wenn der Benutzer sich von einem Computer außerhalb des Unternehmensnetzwerks angemeldet hat.

## Was sollten Sie wissen, bevor Sie beginnen?

- Für die Verfahren in diesem Thema sind bestimmte Berechtigungen erforderlich. Informationen zu den Berechtigungen finden Sie in den einzelnen Verfahren.
- [Erstellen Sie ein oder mehrere Postfächer für Benutzer](#).
- [Aktivieren Sie die Outlook Web App für das Benutzerpostfach](#), falls sie deaktiviert war.
- Stellen Sie sicher, dass für alle Benutzer im Unternehmen Cookies im Webbrowser zulässig sind.
- Erstellen und konfigurieren Sie einmaliges Anmelden (SSO) mithilfe von AD FS:
  - [Prüfliste: Implementieren und Verwalten des einmaligen Anmeldens mit AD FS](#)
  - [Einrichten der einmaligen Anmeldung bei Office 365 mithilfe von AD FS 2.0](#)
  - [Konfigurieren der einmaligen Anmeldung](#)
- Wie Sie mit Windows PowerShell eine Verbindung mit Exchange Online herstellen, können Sie unter [Herstellen einer Verbindung mit Exchange Online PowerShell](#) nachlesen.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Aufgabe 1 - Aktivieren öffentlicher Anlagenverarbeitung für Ihre Organisation

Führen Sie den folgenden Befehl aus:

```
Set-OrganizationConfig -PublicComputersDetectionEnabled $true
```

**Hinweis:** Wenn dieser Parameter auf `$true` hat keinen Einfluss auf die Einstellungen für die folgenden Parameter:

- *ForceWacViewingFirstOnPublicComputers*
- *Wssaccessonpubliccomputersenabled* steht
- *Uncaccessonpubliccomputersenabled* steht

## Aufgabe 2 - Hinzufügen und Erstellen von Anspruchsregeln in AD FS 2.0

Sie müssen eine benutzerdefinierte Anspruchsregel erstellen, da das Vorhandensein ein AD FS-Servers beruht die `x-ms-proxy` Forderung von erkennen, ob Benutzer von einer internen oder externen Netzwerk stammt. Wenn Sie

ein AD FS-Proxy für den externen oder öffentlichen Zugriff bereitgestellt wird und wenn der Benutzer über ein privates Netzwerk stammt, wird ein `x-ms-proxy` Anspruch von AD FS-Proxy an einen AD FS-Server gesendet. Weitere Informationen zum Anspruchsregeln in AD FS finden Sie unter [Erstellen einer Regel zum Send Claims Using a Custom Rule](#)

1. Geben Sie auf dem **Startbildschirm** den Befehl **AD FS Management** ein, und drücken Sie die **Eingabetaste**.
2. In AD FS Konsolenstruktur unter **AD Fs\vertrauensstellungen > Relying Party Trusts** und wählen **O365-Identity-Plattform**.
3. Klicken Sie in **O365 Identity Platform** auf **Edit Claim Rules > Add Rule > Issuance Transform Rules**.
4. Wählen Sie auf der Seite **Select Rule Template** unter **Claim rule template** den Eintrag **Send Claims Using a Custom Rule** aus der Liste aus, und klicken Sie auf **Next**.
5. Geben Sie auf der Seite **Configure Rule** unter **Claim rule name** den Anzeigenamen für diese Regel ein.
6. Geben Sie unter **Custom rule** Folgendes ein:  

```
exists ([Type == "http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy"]) => issue(Type = "http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork", Value = "false");
```
7. Im nächsten Schritt geben Sie Folgendes ein:  

```
NOT exists ([Type == "http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy"]) => issue(Type = "http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork", Value = "true");
```
8. Klicken Sie auf **Finish**.
9. Klicken Sie im Dialogfeld **Edit Claim Rules** auf **OK**, um die Regel zu speichern.

## Aufgabe 3 - Aktivieren der öffentlichen Anlagenverarbeitung in einer Outlook Web App-Postfachrichtlinie

### Verwenden der Exchange-Verwaltungskonsole zum Aktivieren der Einstellungen für die öffentliche Anlagenverarbeitung

1. Klicken Sie in der Exchange-Verwaltungskonsole auf **Berechtigungen > Outlook Web App-Richtlinien**.
2. Wählen Sie im Ergebnisbereich die Postfachrichtlinie aus, die Sie anzeigen oder konfigurieren möchten, und klicken Sie dann auf **Bearbeiten**.
3. Verwenden Sie die Kontrollkästchen für **Dateizugriff**, um die Optionen für den Zugriff und die Anzeige von Dateien für die Benutzer zu konfigurieren. Mit der Dateizugriffsoption kann ein Benutzer alle an eine E-Mail-Nachricht angehängten Dateien öffnen oder anzeigen.

Der Dateizugriff kann basierend darauf gesteuert werden, ob sich ein Benutzer bei einem öffentlichen oder privaten Computer angemeldet hat. Die Benutzeroption zur Auswahl des privaten oder öffentlichen Computerzugriffs steht nur zur Verfügung, wenn Sie mit der formularbasierten Authentifizierung arbeiten. Bei allen weiteren Formen der Authentifizierung wird von einem Zugriff auf einen privaten Computer ausgegangen.

- **Direkter Dateizugriff:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie den direkten Dateizugriff aktivieren möchten. Direkter Dateizugriff ermöglicht Benutzern das Öffnen von Dateien, e-Mail-Nachrichten zugeordnet ist.
- **WebReady Document Viewing:** Wählen Sie dieses Kontrollkästchen, wenn Sie aktivieren möchten, unterstützter Dokumente in HTML konvertiert werden soll, und in einem Webbrowser angezeigt.
- **WebReady Document erzwingen Viewing werden, wenn ein Konverter verfügbar ist:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie Dokumente in HTML konvertiert und in einem Webbrowser angezeigt

werden, bevor sie Benutzer in der Anwendung anzeigen öffnen können erzwingen möchten. Dokumente können in der Anwendung anzeigen geöffnet werden nur, wenn Direkter Dateizugriff aktiviert wurde.

4. Klicken Sie auf **Speichern**, um die Richtlinie zu aktualisieren.

#### **Verwenden Sie Exchange Online PowerShell, um Einstellungen für die öffentliche anlagenverarbeitung aktivieren**

Führen Sie den folgenden Befehl aus:

```
Set-OwaMailboxPolicy -Identity MyOWAPublicPolicy -DirectFileAccessOnPublicComputersEnabled $true -  
ForceWacViewingFirstOnPublicComputers $true -WacViewingOnPublicComputersEnabled $true -  
WebReadyDocumentViewingOnPublicComputersEnabled $true
```

## Was müssen Sie über Anlagen wissen?

Eine Anlage kann eine Datei sein, die in einem beliebigen Programm erstellt wurde, z. B. ein Word-Dokument, eine Excel-Kalkulationstabelle, eine WAV-Datei oder eine Bitmapdatei. Benutzer können eine oder mehrere Dateien an/in jedes Objekt, das sie in ihrem Postfach erstellen, anhängen oder einfügen, beispielsweise E-Mail-Nachrichten, Kalendereinträge oder Kontakte. Outlook Web App ermöglicht das Senden und Empfangen vieler allgemeiner Dateitypen. Fortlaufend

Einige Anlagen entfernt oder durch Antivirensoftware verwendet von Ihrer Organisation, von der Organisation der Empfänger der Ihre e-Mail-Adresse, blockiert oder Sie müssen, auf dem Computer speichern, bevor Sie geöffnet werden können. Standardmäßig können mit Outlook Web App angefügte Word, Excel, PowerPoint, Textdateien und viele Media-Dateien direkt geöffnet werden. Die Dateien, die beim Öffnen von Outlook Web App variieren je nach Ihrer kontoeinstellungen. Die folgende Liste beschreibt die Standard-Dateinamenerweiterungen, die Sie in Outlook Web App öffnen können.

#### **Standardmäßig zugelassene Dateinamenerweiterungen:**

- .AVI
- BMP
- DOC
- DOC
- DOCM
- DOCX
- GIF
- JPEG
- MP3
- ONE
- PDF
- PNG
- PPSM
- PPSX
- PPT
- PPTM

- PPTX
- pub
- .RPMMSG
- RTF
- TIF
- TXT
- VSD
- WAV
- WMA
- .wmv
- XLS
- XLS
- XLSB
- XLSM
- XLSX

# Vermehrung des von Posteingangsregeln verwendeten Speicherplatzes

18.12.2018 • 2 minutes to read

Outlook Web App- und Outlook-Posteingangsregeln sind auf 64 KB beschränkt. Jede Regel, die Sie erstellen, nimmt Speicherplatz in Ihrem Postfach in Anspruch. Der tatsächliche Speicherplatz, den eine Regel benötigt, hängt von mehreren Faktoren ab, z. B. der Länge des Namens und der Anzahl der Bedingungen, die Sie einbezogen haben. Wenn Sie die Grenze von 64 KB erreicht haben, erscheint die Warnmeldung, dass Sie keine weiteren Regeln mehr erstellen können oder dass Sie eine Regel nicht aktualisieren können. Allerdings können Sie den Speicherplatz, der von Posteingangsregeln in Anspruch genommen wird, für einen Benutzer in Ihrer Organisation vermehren.

## NOTE

Es gibt keine maximale Anzahl von Regeln, die erstellt werden können.

## Erhöhen des Grenzwerts für Posteingangsregeln

So erhöhen Sie die Begrenzung:

1. [Herstellen einer Verbindung mit Exchange Online PowerShell](#). Sie können nur Exchange Online PowerShell verwenden, um dieses Verfahren auszuführen.
2. Führen Sie den folgenden Befehl aus:

```
Set-Mailbox -Identity -douglas@contoso.com -RulesQuota 256kb
```

## Was muss ich sonst noch wissen?

- Posteingangsregeln werden von oben nach unten in der Reihenfolge angewendet, in der sie im Fenster **Regeln** angezeigt werden. Wenn Sie die Reihenfolge der Regeln ändern möchten, klicken Sie auf die Regel, die Sie verschieben möchten. Klicken Sie anschließend auf den Pfeil "Nach oben" oder "Nach unten", um die Regel an die gewünschte Position in der Liste zu verschieben.
- Wenn Sie eine Weiterleitungsregel erstellen, können Sie für die Weiterleitung mehr als eine Adresse hinzufügen. Die Anzahl der Adressen, an die Sie weiterleiten können, kann abhängig von den Einstellungen für Ihr Konto beschränkt sein. Wenn Sie mehr Adressen hinzufügen, als zulässig sind, funktioniert Ihre Weiterleitungsregel nicht. Wenn Sie eine Weiterleitungsregel mit mehr als einer Adresse erstellen, testen Sie die Funktionsfähigkeit der Regel.

# MailTips

18.12.2018 • 17 minutes to read

E-Mail-Infos sind informative Meldungen, die Benutzern angezeigt wird, während sie eine Nachricht verfassen. Microsoft Exchange Server analysiert die Nachricht, einschließlich der Liste der Empfänger, die sie gerichtet ist, und wenn es sich um ein potenzielles Problem erkennt, benachrichtigt den Benutzer mit e-Mail-Infos vor dem Senden der Nachricht entsprechend. Mithilfe von e-Mail-Infos bereitgestellten Informationen können Absender die Nachricht, dass verfassen zur Vermeidung von unerwünschten Situationen oder Unzustellbarkeitsberichte (NDR) anpassen.

## Funktionsweise von E-Mail-Infos

E-Mail-Infos werden in Exchange als Webdienst implementiert. Beim Verfassen eines Absenders einer Nachricht macht die Clientsoftware einen Exchange web Service-Aufruf an den Client Access Server zum Abrufen der Liste der e-Mail-Infos. Der Server antwortet mit der Liste der e-Mail-Infos, die auf diese Nachricht anwenden, und die Clientsoftware zeigt die e-Mail-Infos an den Absender.

Die folgenden unproduktiven Messagingszenarien treten in allen Messagingumgebungen häufig auf:

- Unzustellbarkeitsberichte aufgrund von Nachrichten, die in einer Organisation konfigurierte Einschränkungen verletzen, z. B. Einschränkungen der Nachrichtengröße oder der maximalen Anzahl von Empfängern pro Nachricht.
- Unzustellbarkeitsberichte aufgrund von Nachrichten an Empfänger, die nicht vorhanden sind, für die Einschränkungen gelten oder deren Benutzerpostfächer voll sind.
- Senden von Nachrichten an Benutzer, für die automatische Antworten konfiguriert sind.

In allen diesen Szenarien sendet der Benutzer eine Nachricht, erwartet ihre Zustellung und erhält stattdessen eine Antwort, die besagt, dass die Nachricht nicht zugestellt wurde. Sogar im Best-Case-Szenario, wie bei der automatischen Antwort, führen diese Ereignisse zu Produktivitätsverlusten. Im Fall eines Unzustellbarkeitsberichts kann es zu einem teuren Anruf beim Helpdesk kommen.

Des Weiteren gibt es mehrere Szenarien, in denen das Senden einer Nachricht nicht zu einem Fehler führt, aber unerwünschte und sogar peinliche Konsequenzen haben kann:

- An extrem große Verteilergruppen gesendete Nachrichten.
- An ungeeignete Verteilergruppen gesendete Nachrichten.
- Versehentlich an Empfänger außerhalb Ihrer Organisation gesendete Nachrichten.
- Auswählen von **Allen antworten** für eine Nachricht, bei der Sie Bcc-Empfänger waren.

Alle diese problematischen Szenarien können vermieden werden, indem die Benutzer über die möglichen Konsequenzen des Sendens der Nachricht informiert werden, während sie sie verfassen. Wenn Absender beispielsweise wissen, dass die Größe der zu sendenden Nachricht die Vorgaben der Unternehmensrichtlinie übersteigt, versuchen sie nicht, sie zu senden. Wenn Absender benachrichtigt werden, dass die zu sendende Nachricht an Personen außerhalb der Organisation zugestellt wird, stellen sie eher sicher, dass der Inhalt und der Tonfall der Nachricht geeignet sind.

Die folgenden Messagingclients unterstützen E-Mail-Infos:

- Outlook Web App

- Microsoft Outlook 2010 oder höher

## E-Mail-Infos in Exchange

Die folgende Tabelle enthält die verfügbaren e-Mail-Infos in Exchange Server.

E-MAIL-INFO	VERFÜGBARKEIT	SZENARIO
Ungültiger interner Empfänger	Outlook	<p>Die E-Mail-Info zu einem ungültigen internen Empfänger wird angezeigt, wenn der Absender einen organisationsinternen Empfänger hinzufügt, der jedoch nicht vorhanden ist.</p> <p>Dieser Fall kann eintreten, wenn der Absender eine Nachricht an einen Benutzer richtet, der nicht mehr Mitglied des Unternehmens ist, dessen Adresse jedoch über den Namensauflösungs-Cache oder über einen Eintrag im Kontaktordner des Absenders aufgelöst wird. Oder wenn der Absender eine SMTP-Adresse mit einer Domäne eingibt, für die Exchange autoritativ ist, und die Adresse nicht in einen vorhandenen Absender aufgelöst wird.</p> <p>Die E-Mail-Info zeigt den ungültigen Empfänger an und ermöglicht es dem Absender, den Empfänger aus der Nachricht zu entfernen.</p>
Postfach voll	Outlook Outlook Web App	<p>Die E-Mail-Info zu einem vollen Postfach wird angezeigt, wenn der Absender einen Empfänger hinzufügt, dessen Postfach voll ist, und Ihre Organisation eine Richtlinie implementiert hat, mit der verhindert wird, dass Postfächer über einer angegebenen Größe Nachrichten empfangen.</p> <p>Die E-Mail-Info zeigt den Empfänger an, dessen Postfach voll ist, und ermöglicht es dem Absender, den Empfänger aus der Nachricht zu entfernen.</p> <p>Die E-Mail-Info ist zu dem Zeitpunkt, zu dem sie angezeigt wird, aktuell. Wenn die Nachricht nicht sofort gesendet wird, wird die E-Mail-Info alle zwei Stunden aktualisiert. Dies gilt auch für Nachrichten, die im Ordner "Entwürfe" gespeichert und nach zwei Stunden erneut geöffnet werden.</p>

E-MAIL-INFO	VERFÜGBARKEIT	SZENARIO
Automatische Antworten	Outlook Outlook Web App	<p>Die E-Mail-Info für automatische Antworten wird angezeigt, wenn der Absender einen Empfänger hinzufügt, der automatische Antworten aktiviert hat.</p> <p>Die E-Mail-Info gibt an, dass der Empfänger "Automatische Antworten" aktiviert hat, und zeigt auch die ersten 175 Zeichen der vom Empfänger konfigurierten automatischen Antwort. Die E-Mail-Info ist zu dem Zeitpunkt, zu dem sie angezeigt wird, aktuell. Wenn die Nachricht nicht sofort gesendet wird, wird die E-Mail-Info alle zwei Stunden aktualisiert. Dies gilt auch für Nachrichten, die im Ordner "Entwürfe" gespeichert und nach zwei Stunden erneut geöffnet werden.</p> <p>Wenn ein Teil Ihrer Benutzerpostfächer in Exchange Online gehostet wird und Sie die Koexistenz mit Exchange Online eingerichtet haben, hat die Einstellung für das Remotedomänenobjekt, das den Remotebereich Ihrer Organisation darstellt, direkte Auswirkungen auf die Verarbeitung dieser E-Mail-Info.</p> <p>In Exchange Server, Benutzer können verschiedene automatische Antworten für interne und externe Absender konfigurieren. Wenn die Remotedomäne als interne Domäne konfiguriert ist (durch Festlegen des Parameters <i>IsInternal</i> auf das remotedomänenobjekt an <code>\$true</code> ), interne automatische Antwort wird zurückgegeben, um alle Benutzer in der Organisation, unabhängig davon, in dem sich ihr Postfach befindet. Wenn die Remotedomäne als interne Domäne nicht konfiguriert wurde, interne automatische Antwort an alle Benutzer, deren Postfächer befinden sich in der lokalen Domäne, zurückgegeben und die externe automatische Antwort an Benutzer, deren Postfächer befinden sich in der Remotedomäne, zurückgegeben.</p>

E-MAIL-INFO	VERFÜGBARKEIT	SZENARIO
Benutzerdefiniert	Outlook Outlook Web App	<p>Eine benutzerdefinierte E-Mail-Info wird angezeigt, wenn der Absender einen Empfänger hinzufügt, für den eine benutzerdefinierte E-Mail-Info konfiguriert ist.</p> <p>Eine benutzerdefinierte E-Mail-Info kann hilfreich sein, um spezielle Informationen zu einem Empfänger bereitzustellen. Beispielsweise können Sie eine benutzerdefinierte E-Mail-Info für eine Verteilergruppe erstellen, in der Sie den Zweck der Verteilergruppe erläutern, damit sie seltener falsch verwendet wird. Weitere Informationen finden Sie unter <a href="#">Konfigurieren benutzerdefinierter E-Mail-Infos für Empfänger</a>.</p> <p>Standardmäßig werden benutzerdefinierte E-Mail-Infos nicht angezeigt, wenn der Absender keine Nachrichten an diesen Empfänger senden darf. In diesem Fall wird die E-Mail-Info für eingeschränkte Empfänger angezeigt. Sie können diese Konfiguration jedoch ändern und auch die benutzerdefinierte E-Mail-Info anzeigen.</p>
Eingeschränkter Empfänger	Outlook Outlook Web App	<p>Die E-Mail-Info für eingeschränkte Empfänger wird angezeigt, wenn der Absender einen Empfänger hinzufügt, für den Zustellungseinschränkungen konfiguriert sind, sodass dieser Absender am Senden von Nachrichten gehindert wird.</p> <p>In der E-Mail-Info wird der Empfänger angezeigt, an den der Absender keine Nachrichten senden darf, und der Absender erhält die Option, den Empfänger aus der Nachricht zu entfernen. Außerdem wird der Absender informiert, dass die Nachricht nicht übermittelt wird.</p> <p>Wenn es sich bei dem eingeschränkten Empfänger um einen externen Empfänger oder um eine Verteilergruppe mit externen Empfängern handelt, wird auch diese Information dem Absender bereitgestellt. Die folgenden E-Mail-Infos werden jedoch ggf. unterdrückt:</p> <ul style="list-style-type: none"> <li>Automatische Antworten</li> <li>Postfach voll</li> <li>Benutzerdefinierte E-Mail-Infos</li> <li>Moderierter Empfänger</li> <li>Übergroße Nachricht</li> </ul>

E-MAIL-INFO	VERFÜGBARKEIT	SZENARIO
Externe Empfänger	Outlook Outlook Web App	<p>Die E-Mail-Info zu externen Empfängern wird angezeigt, wenn der Absender einen externen Empfänger oder eine Verteilergruppe mit externen Empfängern hinzufügt.</p> <p>Mit dieser E-Mail-Info werden Absender informiert, wenn eine Nachricht, die sie schreiben, die Organisation verlassen wird. So können sie die richtigen Entscheidungen hinsichtlich Formulierungen, Tonfall und Inhalt treffen.</p> <p>Standardmäßig ist diese E-Mail-Info deaktiviert. Sie können sie mit dem Cmdlet <b>Set-OrganizationConfig</b> aktivieren. Weitere Informationen finden Sie unter <a href="#">E-Mail-Infos über Organisationsbeziehungen</a>.</p> <p>Wenn ein Teil Ihrer Benutzerpostfächer in Exchange Online gehostet wird und Sie die Koexistenz mit Exchange Online eingerichtet haben, hat die Einstellung für das Remotedomänenobjekt, das den Remotebereich Ihrer Organisation darstellt, direkte Auswirkungen auf die Verarbeitung dieser E-Mail-Info.</p> <p>Wenn die Remotedomäne als interne Domäne konfiguriert ist (durch Festlegen des Parameters <i>IsInternal</i> auf das remotedomänenobjekt an <code>\$true</code> ), keinem Empfänger in der diese Remotedomäne als intern behandelt und daher nicht die externe e-Mail-Empfänger Info angezeigt. Jedoch, wenn die Remotedomäne als interne Domäne nicht konfiguriert wurde, die Empfänger, Domäne externe betrachtet und diese e-Mail-Info wird angezeigt, wenn eine Nachricht wird besteht aus an diesen Empfänger.</p> <p>&gt; [!NOTE]&gt; Diese E-Mail-Info wird nicht ausgewertet, wenn eine Nachricht an eine Verteilergruppe in der Remotedomäne verfasst wird.</p>

E-MAIL-INFO	VERFÜGBARKEIT	SZENARIO
Große Benutzergruppe	Outlook Outlook Web App	<p>Die E-Mail-Info zu großer Benutzergruppe wird angezeigt, wenn der Absender eine Verteilergruppe hinzufügt, die mehr Mitglieder enthält, als für die Größe einer großen Benutzergruppe für Ihre Organisation konfiguriert ist. Standardmäßig wird diese E-Mail-Info in Exchange für Nachrichten an Verteilergruppen mit mehr als 25 Mitgliedern angezeigt. Weitere Informationen finden Sie unter <a href="#">Konfigurieren einer großen Benutzergruppe für Ihre Organisation</a>.</p> <p>Die Größe der Verteilergruppen wird nicht jedes Mal berechnet. Stattdessen werden die Verteilergruppeninformationen aus den Gruppenmetrikdaten gelesen.</p>
Moderierter Empfänger	Outlook Outlook Web App	<p>Die E-Mail-Info zu moderiertem Empfänger wird angezeigt, wenn der Absender einen moderierten Empfänger hinzufügt.</p> <p>Die E-Mail-Info zeigt an, welcher Empfänger moderiert ist, und informiert den Absender, dass dies zu Verzögerungen bei der Zustellung führen kann.</p> <p>Wenn der Absender zugleich der Moderator ist, wird diese E-Mail-Info nicht angezeigt. Ebenso wird sie nicht angezeigt, wenn dem Absender explizit gestattet wurde, Nachrichten an den Empfänger zu senden (indem der Name des Absenders zur Liste "Nachrichten annehmen von" des Empfängers hinzugefügt wurde).</p> <p>Anweisungen zum Konfigurieren moderierter Empfänger in Exchange Server finden Sie unter <a href="#">Allgemeine Nachricht Genehmigung Szenarien</a>.</p> <p>Anweisungen zum Konfigurieren moderierter Empfänger in Exchange Online finden Sie unter <a href="#">Konfigurieren moderierten Empfänger in Exchange Online</a>.</p>
Antwort an alle bei Bcc	Outlook Web App	<p>Die E-Mail-Info zur Antwort an alle bei Bcc wird angezeigt, wenn der Absender eine Bcc-Kopie einer Nachricht enthält und <b>Allen antworten</b> auswählt.</p> <p>Wenn ein Benutzer für eine solche Nachricht <b>Allen antworten</b> auswählt, erfahren alle anderen Empfänger, an die die Nachricht gesendet wurde, dass dieser Benutzer eine Bcc-Kopie erhalten hat. Das dies in den seltensten Fällen erwünscht ist, wird der Benutzer mit dieser E-Mail-Info auf die Situation hingewiesen.</p>

E-MAIL-INFO	VERFÜGBARKEIT	SZENARIO
Übergroße Nachricht	Outlook	<p>Die E-Mail-Info zu übergroßer Nachricht wird angezeigt, wenn die vom Absender verfasste Nachricht die konfigurierten Einschränkungen der Nachrichtengröße in Ihrer Organisation übersteigt.</p> <p>Die E-Mail-Info wird angezeigt, wenn die Nachrichtengröße eine der folgenden Größeneinschränkungen verletzt:</p> <ul style="list-style-type: none"> <li>Einstellung für maximale Sendegröße für das Postfach des Absenders</li> <li>Einstellung für maximale Empfangsgröße für das Postfach des Absenders</li> <li>Einschränkung für die maximale Nachrichtengröße für die Organisation</li> </ul> <p>&gt; [!NOTE]&gt; Aufgrund der Komplexität der Implementierung werden die Einschränkungen der Nachrichtengröße für die Connectors in Ihrer Organisation nicht berücksichtigt.</p>

## Einschränkungen von E-Mail-Infos

Für die E-Mail-Info gelten die folgenden Einschränkungen:

- E-Mail-Infos werden bei der Arbeit im Offlinemodus von Outlook nicht unterstützt.
- Wenn eine Nachricht an eine Verteilergruppe adressiert ist, werden die E-Mail-Infos für einzelne Empfänger, die Mitglieder dieser Verteilergruppe sind, nicht ausgewertet. Wenn es sich bei einem der Mitglieder jedoch um einen externen Empfänger handelt, wird die E-Mail-Info für externe Empfänger angezeigt, in der dem Absender die Anzahl externer Empfänger in der Verteilergruppe angezeigt wird.
- Wenn die Nachricht an mehr als 200 Empfänger adressiert ist, werden aus Leistungsgründen keine E-Mail-Infos für einzelne Postfächer ausgewertet.
- Benutzerdefinierte E-Mail-Infos sind auf 175 Zeichen beschränkt.
- Während ältere Versionen von Exchange Server e-Mail-Infos vollständig füllen würde, wird der Exchange Online nur bis zu 1000 Zeichen angezeigt.
- Wenn der Absender beginnt, eine Nachricht zu erstellen, und sie für einen längeren Zeitraum geöffnet lässt, werden die E-Mail-Infos zu automatischen Antworten und vollem Postfach alle zwei Stunden ausgewertet.

# Konfigurieren einer großen Benutzergruppe für Ihre Organisation

18.12.2018 • 2 minutes to read

Exchange Online PowerShell können Sie um verschiedene Einstellungen zu konfigurieren, die definieren, wie Sie e-Mail-Infos in Ihrer Organisation verwenden.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 5 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "E-Mail-Infos" im Thema [Berechtigungen für den Nachrichtenfluss](#).
- Sie können nur Exchange Online PowerShell verwenden, um dieses Verfahren ausführen.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell, die große Benutzergruppe für Ihre Organisation konfigurieren

Sie verwenden das Cmdlet **Set-OrganizationConfig**, um die Größe einer großen Benutzergruppe für Ihre Organisation zu konfigurieren. Wenn Absender Nachrichten an eine größere Gruppe von Empfängern senden, als Sie konfiguriert haben, werden diese in der E-Mail-Info zu einer großen Benutzergruppe angezeigt. Die Größe einer großen Benutzergruppe ist standardmäßig auf 25 festgelegt. In diesem Beispiel wird die Größe einer großen Benutzergruppe in Ihrer Organisation auf 50 konfiguriert.

```
Set-OrganizationConfig -MailTipsLargeAudienceThreshold 50
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [set-OrganizationConfig](#).

# Konfigurieren benutzerdefinierter E-Mail-Infos für Empfänger

18.12.2018 • 6 minutes to read

Bei der E-Mail-Info handelt es sich um informative Meldungen, die auf der Infoleiste in Outlook Web App und Microsoft Outlook 2010 oder höher Benutzern angezeigt werden, wenn sie beim Verfassen einer E-Mail eine der folgenden Aktionen ausführen:

- Empfänger hinzufügen
- Anlage hinzufügen
- Antworten oder allen antworten
- Nachricht im Ordner "Entwürfe" öffnen, die bereits an Empfänger adressiert ist

Zusätzlich zu den verfügbaren vordefinierten E-Mail-Infos können Sie für alle Empfängertypen benutzerdefinierte E-Mail-Infos erstellen. Weitere Informationen zu den vordefinierten E-Mail-Infos finden Sie unter [E-Mail-Infos](#).

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen des Vorgangs: 10 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "E-Mail-Infos" im Thema [Berechtigungen für den Nachrichtenfluss](#).
- Sie können die primäre e-Mail-Info in der Exchange-Verwaltungskonsole (EAC) oder in Exchange Online PowerShell konfigurieren. Sie können jedoch nur zusätzliche e-Mail-Info-Übersetzungen in Exchange Online PowerShell konfigurieren.
- Wenn Sie einem Empfänger eine E-Mail-Info hinzufügen, passieren zwei Dinge:
  - HTML-Tags werden automatisch auf den Text hinzugefügt. Beispielsweise, wenn Sie den Text eingeben: `This mailbox is not monitored`, automatisch die e-Mail-Info wird:  
`<html><body>This mailbox is not monitored</body></html>`. Zusätzliche HTML-Tags in die e-Mail-Info werden nicht unterstützt.
  - Der Text wird der Eigenschaft *MailTipTranslations* des Empfängers automatisch als Standardwert hinzugefügt. Wenn Sie den E-Mail-Infotext ändern, wird der Standardwert automatisch in der Eigenschaft *MailTipTranslations* aktualisiert.
- Die Länge einer E-Mail-Info darf 175 angezeigte Zeichen nicht überschreiten.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

# Was möchten Sie machen?

## Konfigurieren von E-Mail-Infos für Empfänger

Verwenden der Exchange-Verwaltungskonsole zum Konfigurieren von E-Mail-Infos für Empfänger

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Empfänger**.

2. Wählen Sie basierend auf dem Empfängertyp eine der folgenden Empfängerregisterkarten aus:

- **Postfächer**
- **Gruppen**
- **Ressourcen**
- **Contacts**
- **Shared**

3. Wählen Sie auf der empfängerregisterkarte den Empfänger, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

4. Klicken Sie auf der angezeigten Seite mit den Empfängereigenschaften auf **E-Mail-Infos**.

5. Geben Sie den Text der E-Mail-Info ein. Klicken Sie nach Abschluss des Vorgangs auf **Speichern**.

## Verwenden von Exchange Online PowerShell zum Konfigurieren von e-Mail-Infos für Empfänger

Verwenden Sie folgende Syntax, um eine E-Mail-Info für einen Empfänger zu konfigurieren.

```
Set-<RecipientType> <RecipientIdentity> -MailTip "<MailTip text>"
```

\_ <RecipientType> \_ kann jede Art von Empfänger sein. Beispielsweise **Mailbox**, **MailUser**, **MailContact**, **DistributionGroup**, oder **DynamicDistributionGroup**.

Angenommen, Sie haben ein Postfach mit dem Namen "Help Desk", an das Benutzer Supportanfragen senden können, und die zugesagte Antwortzeit ist zwei Stunden. Führen Sie den folgenden Befehl aus, um eine benutzerdefinierte E-Mail-Info zu konfigurieren, in der dies erläutert wird:

```
Set-Mailbox "Help Desk" -MailTip "A Help Desk representative will contact you within 2 hours."
```

## Verwenden von Exchange Online PowerShell zum Konfigurieren zusätzlicher e-Mail-Infos in verschiedenen Sprachen

Zum Konfigurieren zusätzlicher Übersetzungen von E-Mail-Infos ohne Beeinträchtigung des vorhandenen E-Mail-Infotexts oder anderer vorhandener E-Mail-Info-Übersetzungen verwenden Sie die folgende Syntax:

```
Set-<RecipientType> -MailTipTranslations @'{Add="<culture1>:<localized text 1>","<culture2>:<localized text 2>..."; Remove="<culture1>:<localized text 1>","<culture2>:<localized text 2>..."}
```

<culture> ist ein gültiger aus zwei Buchstaben bestehender ISO 639-Kulturcode der Sprache.

Angenommen, das Postfach mit dem Namen "Benachrichtigungen" hat derzeit beispielsweise die E-Mail-Info: "Dieses Postfach wird nicht überwacht." Führen Sie den folgenden Befehl aus, um die spanische Übersetzung hinzuzufügen:

```
Set-Mailbox -MailTipTranslations @'{Add="ES:Esta caja no se supervisa."}
```

**Woher wissen Sie, dass dieses Verfahren erfolgreich war?**

Gehen Sie folgendermaßen vor, um sicherzustellen, dass eine E-Mail-Info erfolgreich für einen Empfänger konfiguriert wurde:

1. Verfassen Sie in Outlook Web App oder Outlook 2010 oder höher eine an den Empfänger adressierte E-Mail-Nachricht, ohne Sie zu senden.
2. Überprüfen Sie, ob die E-Mail-Info in der Infoleiste angezeigt wird.
3. Wenn Sie weitere E-Mail-Info-Übersetzungen konfiguriert haben, verfassen Sie die Nachricht in Outlook Web App. Zum Überprüfen der Ergebnisse muss die Spracheinstellung der Sprache der E-Mail-Info-Übersetzung entsprechen.

# E-Mail-Infos über Organisationsbeziehungen

18.12.2018 • 4 minutes to read

Microsoft Exchange Server können Sie zum Konfigurieren von organisationsbeziehungen mit Microsoft Exchange Online oder anderen Exchange-Organisationen. Einrichten einer organisationsbeziehung können Sie die Benutzer-Erlebnis beim Umgang mit der anderen Organisation. Sie können beispielsweise Freigabe von Frei / Gebucht-Daten, konfigurieren sichere Nachrichtenfluss und nachrichtenverfolgung für beide Organisationen aktivieren.

## Steuern der Zugriffsebene für E-Mail-Infos

Möglicherweise möchten bestimmte Typen von e-Mail-Infos zu beschränken. Sie können entweder alle e-Mail-Infos, damit nur eine begrenzte Auswahl, die Unzustellbarkeitsberichte verhindern würden oder zurückgegeben werden. Sie können diese Einstellung mit dem Parameter *MailTipsAccessLevel* im Cmdlet **Set-OrganizationRelationship** konfigurieren. Die folgende Tabelle zeigt die e-Mail-Infos über die organisationsbeziehung zurückgegeben werden.

E-MAIL-INFO	IST DIE E-MAIL-INFO VERFÜGBAR, WENN FÜR DIE ZUGRIFFSEBENE "ALL" FESTGELEGT IST?	IST DIE E-MAIL-INFO VERFÜGBAR, WENN FÜR DIE ZUGRIFFSEBENE "LIMITED" FESTGELEGT IST?
Große Benutzergruppe	Ja	Nein
Automatische Antworten	Ja Wenn die Remotedomäne des Empfängers als intern festgelegt ist, wird die interne automatische Antwort angezeigt. Andernfalls wird die externe automatische Antwort angezeigt.	Ja Die externe automatische Antwort wird angezeigt.
Moderierter Empfänger	Ja	Nein
Übergroße Nachricht	Ja	Ja
Eingeschränkter Empfänger	Ja	Ja
Postfach voll	Ja	Nein
Benutzerdefinierte E-Mail-Infos	Ja	Nein
Externe Empfänger	Ja Wenn die Remotedomäne des Empfängers als intern festgelegt ist, wird diese E-Mail-Info unterdrückt. Andernfalls wird die externe E-Mail-Info zurückgegeben.	Ja Wenn die Remotedomäne des Empfängers als intern festgelegt ist, wird diese E-Mail-Info unterdrückt. Andernfalls wird die externe E-Mail-Info zurückgegeben.

Genaue Anweisungen zum Konfigurieren von Zugriffsebenen für E-Mail-Infos finden Sie unter [Verwalten von E-Mail-Infos für Organisationsbeziehungen](#).

## Steuern des Zugriffsbereichs für E-Mail-Infos

Wenn Sie e-Mail-Infos über eine organisationsbeziehung aktivieren, und legen Sie den Zugriff auf  A11 , die Empfänger-spezifischen e-Mail-Infos, Postfach voll, automatische Antworten und benutzerdefinierte e-Mail-Infos, werden für alle Benutzer zurückgegeben. Möglicherweise möchten Sie nur diese e-Mail-Infos für eine bestimmte Gruppe von Benutzern zu ermöglichen. Wenn Sie eine organisationsbeziehung mit einem Partner eingerichtet haben, sollten Sie diese e-Mail-Infos nur für die Benutzer zu ermöglichen, die mit diesem Partner arbeiten.

Um dies zu erreichen, müssen Sie zuerst eine Gruppe erstellen und ihr alle Benutzer hinzufügen, denen Sie empfängerspezifische E-Mail-Infos an diese Gruppe senden möchten. Sie können diese Gruppe dann für die Organisationsbeziehung angeben.

Nachdem Sie diese Einschränkung implementiert haben, überprüfen Ihre Clientzugriffsserver zuerst, ob der Empfänger, für den sie eine E-Mail-Info-Abfrage erhalten haben, Mitglied dieser Gruppe ist. Wenn der Empfänger Mitglied dieser Gruppe ist, senden die Clientzugriffsserver als Proxys alle E-Mail-Infos zurück, einschließlich der empfängerspezifischen E-Mail-Infos. Andernfalls werden die empfängerspezifischen E-Mail-Infos nicht in die Antwort eingeschlossen.

Genaue Anweisungen zum Konfigurieren von Zugriffsebenen für E-Mail-Infos finden Sie unter [Verwalten von E-Mail-Infos für Organisationsbeziehungen](#).

# Verwalten von E-Mail-Infos für Organisationsbeziehungen

18.12.2018 • 5 minutes to read

Exchange Online PowerShell können Sie benutzerdefinierte Einstellungen für e-Mail-Infos zwischen verschiedenen Organisationen konfigurieren.

Durch das Einrichten einer Organisationsbeziehung können Sie die Benutzererfahrung für beide Organisationen verbessern, indem Frei/Gebucht-Daten freigegeben, der sichere Meldungsfluss konfiguriert und die Nachverfolgung von Nachrichten aktiviert wird. Weitere Informationen zu Organisationsbeziehungen finden Sie unter [E-Mail-Infos über Organisationsbeziehungen](#).

Sie können mithilfe von verschiedenen Einstellungen steuern, wie E-Mail-Infos zwischen Organisationen verwendet werden, für die eine Organisationsbeziehung eingerichtet wurde. Die Verfahren in diesem Abschnitt veranschaulichen diese verschiedenen Steuermöglichkeiten. In sämtlichen Beispielen wird "contoso.com" als lokale Organisation und "online.contoso.com" als Remoteorganisation verwendet, und die Organisationsbeziehung wird als "Contoso Online" bezeichnet.

Verwenden Sie das Cmdlet **Set-OrganizationRelationship**, um diese Einstellungen zu konfigurieren.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit bis zum Abschließen der einzelnen Verfahren: 5 Minuten
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "E-Mail-Infos" im Thema [Berechtigungen für den Nachrichtenfluss](#).
- Sie können nur Exchange Online PowerShell verwenden, um dieses Verfahren auszuführen.
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

### TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Was möchten Sie tun?

### Verwenden von Exchange Online PowerShell aktivieren oder Deaktivieren von e-Mail-Infos zwischen den beiden Organisationen

In diesem Beispiel wird die Organisationsbeziehung so konfiguriert, dass E-Mail-Infos an Absender in der Remoteorganisation zurückgegeben werden, wenn Nachrichten für Empfänger in Ihrer Organisation erstellt werden.

```
Set-OrganizationRelationship "Contoso Online" -MailTipsAccessEnabled $true
```

In diesem Beispiel wird die Organisationsbeziehung so konfiguriert, dass keine E-Mail-Infos an Absender in der Remoteorganisation zurückgegeben werden, wenn Nachrichten für Empfänger in Ihrer Organisation erstellt werden.

werden.

```
Set-OrganizationRelationship "Contoso Online" -MailTipsAccessEnabled $false
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-OrganizationRelationship](#).

### Verwenden von Exchange Online PowerShell so konfigurieren Sie die e-Mail-Infos an die Remoteorganisation zurückgegeben werden

Sie können für jede Organisationsbeziehung bestimmen, welche Gruppe von E-Mail-Infos an Absender in der anderen Organisation zurückgegeben werden. In diesem Beispiel für die Organisationsbeziehung so konfiguriert, dass alle E-Mail-Infos zurückgegeben werden.

```
Set-OrganizationRelationship "Contoso Online" -MailTipsAccessLevel All
```

In diesem Beispiel wird die Organisationsbeziehung so konfiguriert, dass nur die E-Mail-Infos für automatische Antworten, übergroße Nachrichten, eingeschränkte Empfänger und volle Postfächer zurückgegeben werden.

```
Set-OrganizationRelationship "Contoso Online" -MailTipsAccessLevel Limited
```

In diesem Beispiel für die Organisationsbeziehung so konfiguriert, dass keine E-Mail-Infos zurückgegeben werden.

#### NOTE

Verwenden Sie diese Methode nicht zum e-Mail-Infos für diese Beziehung zu deaktivieren. Um e-Mail-Infos deaktivieren möchten, legen Sie den Parameter *MailTipsAccessEnabled* auf `$false`.

```
Set-OrganizationRelationship "Contoso Online" -MailTipsAccessLevel None
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-OrganizationRelationship](#).

### Verwenden von Exchange Online PowerShell so konfigurieren Sie eine bestimmte Gruppe von Benutzern für den Empfänger-spezifischen e-Mail-Infos zurückgegeben werden

Sie können die Rückgabe empfängerspezifischer E-Mail-Infos nicht auf eine bestimmte Gruppe von Benutzern einschränken. Bei der Aktivierung von E-Mail-Infos für eine Organisationsbeziehung werden standardmäßig die folgenden empfängerspezifischen E-Mail-Infos für alle Benutzer zurückgegeben:

- Automatische Antworten
- Postfach voll
- Benutzerdefinierte E-Mail-Infos

Sie können eine E-Mail-Info-Zugriffsgruppe für die Organisationsbeziehung festlegen. Nachdem sie eine Gruppe angegeben haben, werden die empfängerspezifischen E-Mail-Infos nur für Postfächer, E-Mail-Kontakte und E-Mail-Benutzer zurückgegeben, die Mitglied dieser Gruppe sind. In diesem Beispiel wird die Organisationsbeziehung so konfiguriert, dass die empfängerspezifischen E-Mail-Infos nur für Mitglieder der Gruppe "ShareMailTips@contoso.com" zurückgegeben werden.

```
Set-OrganizationRelationship "Contoso Online" -MailTipsAccessScope ShareMailTips@contoso.com
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-OrganizationRelationship](#).

# Apps für Outlook

18.12.2018 • 7 minutes to read

**Zusammenfassung:** Eine Übersicht der Add-Ins für Outlook, die zusammen mit Outlook auf Windows- und Macintosh-Computern, auf mobilen Geräten und in Outlook Web App sowie Outlook im Web verwendet werden können.

Add-Ins für Outlook sind Anwendungen, die den Nutzen von Outlook-Clients durch zusätzliche Informationen oder Tools erweitern, die Ihre Benutzer verwenden können, ohne Outlook beenden zu müssen. Add-Ins werden von Drittanbieterentwicklern erstellt und können aus einer Datei oder einer URL oder aus dem Office Store installiert werden. Standardmäßig können alle Benutzer Add-Ins installieren. Exchange-Administratoren können Rollen verwenden, um die Installation von Add-Ins durch Benutzer zu steuern.

## TIP

Informationen zu Add-Ins für Outlook aus der Sicht des Endbenutzers finden Sie im Hilfethema [Installierte Add-Ins](#) auf Office.com. Dieses Thema bietet einen Überblick über Add-Ins für Outlook und zeigt Ihnen außerdem einige Add-Ins für Outlook, die standardmäßig installiert werden können.

## Office Store-Add-Ins und benutzerdefinierte Add-Ins

Outlook-Clients unterstützen eine Vielzahl von Add-Ins, die über den Office Store zur Verfügung stehen. Outlook unterstützt außerdem benutzerdefinierte Add-Ins, die Sie erstellen und an Benutzer in Ihrer Organisation verteilen können.

## NOTE

Zugriff auf den Office Store wird für Postfächer oder Organisationen in bestimmten Regionen nicht unterstützt. Wenn Sie nicht **aus den Office Store hinzufügen** als Option in der **Exchange-Verwaltungskonsole** unter **Organisation** sehen > - **Add-ins > New**  , möglicherweise ein Add-In für Outlook installieren können von einem Speicherort URL oder einen Dateinamen. Weitere Informationen wenden Sie sich an Ihren Dienstanbieter.

## NOTE

Einige Add-Ins für Outlook werden standardmäßig installiert. Standard-Add-Ins für Outlook werden nur für englischsprachige Inhalte aktiviert. Beispielsweise wird durch deutsche Postadressen im Nachrichtentext das Bing Maps-Add-In nicht aktiviert.

## Add-Ins-Zugriff und -Installation

Standardmäßig können alle Benutzer Add-Ins installieren und entfernen. Exchange-Administratoren haben eine Reihe von Steuerungsmöglichkeiten für die Verwaltung von Add-Ins und den Benutzerzugriff auf diese Add-Ins. Administratoren können das Installieren von Add-Ins, die nicht aus dem Office Store heruntergeladen wurden, durch Benutzer deaktivieren (stattdessen werden sie per „Side-Loading“ aus einer Datei oder URL geladen). Administratoren können auch das Installieren von Office Store-Add-Ins und das Installieren von Add-Ins im Auftrag anderer Benutzer deaktivieren. Es ist auch möglich, Benutzer einer Rolle zuzuweisen, die es ihnen ermöglicht, Add-Ins für Ihre Organisation oder für einen Teil der Benutzer in Ihrer Organisation zu installieren.

Um zu verhindern, dass Benutzer ein Add-In, das nicht aus dem Office Store stammt, installieren, entfernen Sie die Rolle **Eigene benutzerdefinierte Apps**. Um zu verhindern, dass Benutzer Add-Ins aus dem Office Store

installieren, entfernen Sie die Rolle **Eigene Marketplace-Apps**. Weitere Informationen finden Sie unter [Festlegen der Administratoren und Benutzer, die Add-Ins für Outlook installieren und verwalten dürfen](#)

Informationen zum Installieren von Add-Ins für einige oder alle Benutzer in Ihrer Organisation finden Sie unter [Installieren oder Entfernen von Apps für Outlook für Ihre Organisation](#).

Bei Bedarf können Sie die Verfügbarkeit eines Add-Ins auf bestimmte Benutzer in der Organisation beschränken. Weitere Informationen finden Sie unter [Manage user access to add-ins for Outlook](#).

### Gängige Verwaltungsaufgaben für Outlook-Add-Ins

Es gibt verschiedene gängige Szenarien, mit denen Sie als Exchange-Administrator in Ihrer Organisation häufig konfrontiert sind.

**Wenn Sie verhindern möchten, dass Endbenutzer Add-Ins für Outlook auf Outlook-Clients installieren, müssen Sie die Rollen der betreffenden Benutzer im Exchange Admin Center wie folgt anpassen:**

- Damit Benutzer keine Add-Ins aus dem Office Store installieren können, müssen Sie die Rolle **My Marketplace** für die betreffenden Benutzer entfernen.
- Damit Benutzer keine Add-Ins aus anderen Quellen als dem Office Store laden können, müssen Sie die Rolle **My Custom Apps** für die betreffenden Benutzer entfernen.
- Damit Benutzer keinerlei Add-Ins mehr installieren können, müssen Sie für die betreffenden Benutzer beide Rollen entfernen.

Weitere Informationen finden Sie unter [Festlegen der Administratoren und Benutzer, die Add-Ins für Outlook installieren und verwalten dürfen](#).

\*\* Wenn Ihre Endbenutzer derzeit-add-ins zugreifen können und Sie entfernen möchten, dass der Zugriff, verwenden Sie die `Get-App` -Cmdlet zum welche-add-ins finden Sie unter jedem Benutzer installiert. \*\*

Verwenden Sie als Nächstes die `Remove-App` Cmdlet, um alle Add-Ins von einem oder mehreren Benutzern zu entfernen.

Weitere Informationen finden Sie [hier](#).

## Zulassen der Installation von Add-Ins durch Administratoren und Benutzer

Sie können angeben, welche Administratoren in Ihrer Organisation die Berechtigung zum Installieren und Verwalten von Add-Ins für Outlook haben. Außerdem können Sie angeben, welche Benutzer in Ihrer Organisation die Berechtigung zum Installieren und Verwalten von Add-Ins zur eigenen Verwendung besitzen. Weitere Informationen finden Sie unter [Festlegen der Administratoren und Benutzer, die Add-Ins für Outlook installieren und verwalten dürfen](#).

# Remoteverbindungsuntersuchungstests für Exchange Online

18.12.2018 • 3 minutes to read

Microsoft Exchange Remote Connectivity Analyzer (ExRCA) hilft Ihnen, sicherzustellen, dass-Konnektivität für die Exchange-Server ordnungsgemäß eingerichtet ist. Wenn Probleme auftreten, kann es auch Ihnen suchen und diese Probleme beheben. Die Website ExRCA kann Tests zu prüfen, ob Microsoft Exchange ActiveSync, Exchange-Webdienste, Microsoft Outlook und Internet-e-Mail-Verbindung ausführen.

## Tests der Remoteverbindungsuntersuchung

Sie können mehrere Tests mithilfe von ExRCA ausführen. Die folgenden Tests können mit Exchange 2007 und höher verwendet werden.

- Exchange ActiveSync
- Exchange-Webdienste
- Outlook
- Internet-E-Mail

### Exchange ActiveSync-Tests

Folgende Tests für Exchange ActiveSync können ausgeführt werden:

- **Exchange ActiveSync:** Bei diesem Test Schritte, die ein mobiles Gerät verwendet, um die Verbindung mit eines Exchange-Servers mit Exchange ActiveSync simuliert.
- **Exchange ActiveSync-AutoErmittlung:** führt dies durch die Exchange ActiveSync-Gerät verwendet, um Einstellungen vom AutoErmittlungsdienst abzurufen.

### Verbindungstests für die Exchange-Webdienste

Mit den Tests für die Exchange-Webdienste werden die Einstellungen für viele der Exchange-Webdienste überprüft. Sie können die folgenden Tests für Exchange-Webdienste ausführen:

- **Synchronisierung, Benachrichtigung, Verfügbarkeit und automatische Antworten:** Diese Tests Aufgaben schrittweise durchgehen viele einfache Exchange-Webdienste zu bestätigen, dass sie arbeiten. Dies ist hilfreich für IT-Administratoren, die mit externen Zugriff mit Entourage EWS oder andere Webdienste Clients beheben möchten.
- **Dienstkontenzugriff (für Entwickler):** Bei diesem Test wird überprüft, ob ein Dienstkonto ein angegebenes Postfach zugreifen, erstellen und Löschen von Elementen im es und darauf zugreifen, über den Exchange-Identitätswechsel. Bei diesem Test wird hauptsächlich durch Anwendungsentwickler So testen Sie den Zugriff auf Postfächer mit alternativen Anmeldeinformationen verwendet.

### Microsoft Office Outlook-Konnektivitätstests

Zum Überprüfen der Outlook-Konnektivität können Sie die folgenden Tests ausführen:

- **Outlook Anywhere (RPC über HTTP):** in diesem Test die Outlook verwendet, um eine Verbindung herstellen über Outlook Anywhere (RPC über HTTP) Schritte durchlaufen.
- **Outlook-AutoErmittlung:** Bei diesem Test führt durch die Outlook verwendet, um Einstellungen vom AutoErmittlungsdienst abzurufen. Bei diesem Test wird nicht tatsächlich an ein Postfach verbinden.

## Internet-E-Mail-Tests

Für Internet-E-Mail- können folgende Tests ausgeführt werden:

- **Eingehende SMTP E-Mail:** Bei diesem Test die Schritte durchlaufen einer Internet e-Mail-Server verwendet, um eingehende SMTP-e-Mail an Ihre Domäne zu senden.
- **Ausgehenden SMTP-e-Mail:** Bei diesem Test überprüft die ausgehende IP-Adresse für bestimmte Anforderungen. Dazu gehören Reverse-DNS, Absender-ID und RBL überprüft.
- **POP-e-Mail:** in diesem Test werden die Schritte, die ein e-Mail-Client wird verwendet, um die Verbindung mit einem Postfach über POP3 durchlaufen.
- **IMAP-e-Mail:** in diesem Test werden die Schritte, die ein e-Mail-Client wird verwendet, um die Verbindung mit einem Postfach über IMAP durchlaufen.

# Clientzugriffsregeln in Exchange Online

18.12.2018 • 16 minutes to read

**Zusammenfassung:** Hier erfahren Sie, wie Administratoren Clientzugriffsregeln verwenden können, um verschiedene Arten von Clientverbindungen mit Exchange Online zuzulassen oder zu blockieren.

Clientzugriffsregeln helfen Ihnen bei der Steuerung des Zugriffs auf Ihre Exchange Online-Organisation basierend auf Clienteigenschaften oder Clientzugriffsanforderungen. Clientzugriffsregeln sind wie E-Mail-Flussregeln (auch bekannt als Transportregeln) für Clientverbindungen mit Ihrer Exchange Online-Organisation. Sie können verhindern, dass Clients eine Verbindung mit Exchange Online herstellen, basierend auf IP-Adresse, Authentifizierungstyp und Eigenschaftswerten des Benutzers und Protokoll, Anwendung, Dienst oder Ressource, die sie verwenden, um eine Verbindung herzustellen. Beispiel:

- Lassen Sie den Zugriff auf Exchange ActiveSync-Clients von bestimmten IP-Adressen zu und blockieren Sie alle anderen ActiveSync-Clients.
- Sperren Sie den Zugriff auf Exchange-Webdienste (EWS) für Benutzer in bestimmten Abteilungen, Städten oder Ländern.
- Blockieren Sie den Zugriff auf ein Offlineaddressbuch (OAB) für bestimmte Benutzer basierend auf ihren Benutzernamen.
- Verhindern des Clientzugriffs über Verbundauthentifizierung.
- Verhindern des Clientzugriffs mit Exchange Online PowerShell.
- Sperren des Zugriffs auf die Exchange-Verwaltungskonsole (EAC) für Benutzer in einem bestimmten Land oder einer bestimmten Region.

Die Verfahren in Bezug auf Clientzugriffsregeln finden Sie unter [Verfahren für Clientzugriffsregeln in Exchange Online](#).

## Clientzugriffsregeln - Komponenten

Eine Regel besteht aus Bedingungen, Ausnahmen, einer Aktion und einem Eigenschaftswert:

- **Bedingungen:** Identifiziert die Clientverbindungen, auf die die Aktion angewendet werden soll. Eine vollständige Liste der Bedingungen finden Sie im Abschnitt [Clientzugriffsregel-Bedingungen und -Ausnahmen](#) weiter unten in diesem Thema. Wenn eine Clientverbindung den Bedingungen einer Regel entspricht, wird die Aktion auf die Clientverbindung angewendet und die Regelauswertung gestoppt. (Es werden keine weiteren Regeln auf die Verbindung angewendet.)
- **Ausnahmen:** Identifiziert optional die Clientverbindungen, auf die die Aktion nicht angewendet werden soll. Mit Ausnahmen werden Bedingungen außer Kraft gesetzt, und es wird verhindert, dass die Regelaktion auf eine Verbindung angewendet wird, und zwar auch dann, wenn die Verbindung allen konfigurierten Bedingungen entspricht. Die Regelauswertung wird für Clientverbindungen fortgesetzt, die von der Ausnahme zugelassen werden, aber eine nachfolgende Regel könnte sich auf die Verbindung auswirken.
- **Aktion:** Gibt an, welche Aufgaben für Clientverbindungen durchgeführt werden, die den Bedingungen in der Regel entsprechen und keiner Ausnahme entsprechen. Gültige Aktionen sind:
  - Verbindung zulassen (die `AllowAccess` Wert für den Parameter `Action` ).
  - Verbindung blockieren (die `DenyAccess` Wert für den Parameter `Action` ).

**Hinweis:** Wenn Sie Verbindungen für ein bestimmtes Protokoll blockieren, sind möglicherweise auch andere Anwendungen betroffen, die auf dasselbe Protokoll zugreifen.

- **Priorität:** Zeigt die Reihenfolge an, in der die Regeln auf Clientverbindungen angewendet werden. Die standardmäßige Priorität basiert auf dem Erstellungsdatum der Regel (ältere Regeln haben eine höhere Priorität als neuere Regeln), und Regeln mit höherer Priorität werden vor Regeln mit niedrigerer Priorität verarbeitet. Die Regelbearbeitung wird beendet, wenn die Clientverbindung den Bedingungen in der Regel entspricht.

Weitere Informationen zum Festlegen der Prioritätswerte für Regeln finden Sie unter [Verwenden von Exchange Online PowerShell zum Festlegen der Priorität von Clientzugriffsregeln](#).

### Auswertung von Clientzugriffsregeln

In der folgenden Tabelle wird beschrieben, wie mehrere Regeln mit derselben Bedingung ausgewertet werden und wie eine Regel mit mehreren Bedingungen, Bedingungswerten und Ausnahmen ausgewertet wird.

KOMPONENTE	LOGIK	KOMMENTARE
Mehrere Regeln, die dieselbe Bedingung enthalten	Die erste Regel wird angewendet , und nachfolgende Regeln werden ignoriert.	Wenn beispielsweise die Regel mit der höchsten Priorität Outlook im Web-Verbindungen blockiert und Sie eine andere Regel erstellen, die Outlook im Web-Verbindungen für einen speziellen IP-Adressbereich zulässt, werden alle Outlook im Web-Verbindungen weiterhin durch die erste Regel blockiert. Statt eine weitere Regel für Outlook im Web zu erstellen, müssen Sie eine Ausnahme zur vorhandenen Outlook im Web-Regel hinzufügen, um Verbindungen vom angegebenen IP-Adressbereich zuzulassen.
Mehrere Bedingungen in einer Regel	UND	Eine Clientverbindung muss allen Bedingungen in der Regel entsprechen. Beispielsweise EWS-Verbindungen von Benutzern in der Buchhaltung.
Eine Bedingung mit mehreren Werten in einer Regel	ODER	Für Bedingungen, die mehrere Werte zulassen, muss die Verbindung einer (nicht allen) der angegebenen Bedingungen entsprechen. Beispielsweise EWS- oder IMAP4-Verbindungen.
Mehrere Ausnahmen in einer Regel	ODER	Wenn eine Clientverbindung einer der Ausnahmen entspricht, werden die Aktionen nicht auf die Clientverbindung angewendet. Die Verbindung muss nicht allen Ausnahmen entsprechen. Beispielsweise IP-Adresse 19.2.168.1.1 oder Standardauthentifizierung.

Sie können testen, wie Clientzugriffsregeln sich auf eine bestimmte Clientverbindung auswirken würden (welche Regeln übereinstimmen würden und daher Einfluss auf die Verbindung hätten). Weitere Informationen finden Sie unter [Verwenden von Exchange Online PowerShell zum Testen von Clientzugriffsregeln](#).

### Wichtige Hinweise:

**Clientverbindungen aus dem internen Netzwerk**

Verbindungen aus Ihrem lokalen Netzwerk dürfen Clientzugriffsregeln nicht automatisch umgehen. Daher müssen Sie beim Erstellen von Clientzugriffsregeln, die Clientverbindungen mit Exchange Online blockieren, berücksichtigen, wie sich dies evtl. auf Verbindungen von Ihrem internen Netzwerk auswirkt. Die bevorzugte Methode zum Zulassen interner Clientverbindungen zum Umgehen von Clientzugriffsregeln ist das Erstellen einer Regel mit höchster Priorität, die Clientverbindungen aus Ihrem internen Netzwerk zulässt (alle oder bestimmte IP-Adressen). Auf diese Weise werden die Clientverbindungen immer zugelassen, unabhängig von weiteren Blockierungsregeln, die Sie in Zukunft erstellen.

#### **Client-Zugriffsregeln und Anwendungen auf mittlerer Ebene**

Viele Anwendungen, die Zugriff auf Exchange Online verwenden eine Middle-Tier-Architektur (Clients sprechen Sie mit der Anwendung der mittleren Ebene und der Anwendung der mittleren Schicht kommuniziert mit Exchange Online). Eine Client Zugriff zulässt, dass nur der Zugriff über Ihr lokales Netzwerk möglicherweise Middle-Tier-Anwendungen blockieren. Daher müssen Ihre Regeln die IP-Adressen von Middle-Tier-Anwendungen zu ermöglichen.

Anwendungen auf mittlerer Ebene, die sich im Besitz von Microsoft befinden (z. B. Outlook für iOS und Android), umgehen das Blockieren durch Client-Zugriffsregeln und sind immer zulässig. Um zusätzliche Kontrolle über diese Anwendungen bereitzustellen, müssen Sie die Funktionen des Steuerelements verwenden, das in den Anwendung verfügbar ist.

#### **Anzeigedauer für Regeländerungen**

Um die allgemeine Leistung zu verbessern, verwenden Client-Zugriffsregeln einen Zwischenspeicher, was bedeutet, dass Änderungen an Regeln nicht sofort wirksam werden. Bei der ersten Regel, die Sie in Ihrer Organisation erstellen, kann es bis zu 24 Stunden dauern, bis sie wirksam wird. Danach kann es bis zu einer Stunde dauern, bis das Ändern, Hinzufügen oder Entfernen von Regeln wirksam wird.

#### **Administration**

Sie können nur Remote-PowerShell verwenden, um Client-Zugriffsregeln zu verwalten, deshalb müssen Sie bei Regeln vorsichtig sein, die Ihren Zugriff auf Remote-PowerShell blockieren. Wenn Sie eine Regel erstellen, die Ihren Zugriff auf Remote-PowerShell blockiert, oder Sie eine Regel erstellen, die alle Protokolle für alle Benutzer blockiert, verlieren Sie die Möglichkeit, die Regeln selbst zu reparieren. Sie müssen sich an den Microsoft-Kundendienst und-Support wenden, die daraufhin eine Regel erstellen, mit deren Hilfe Sie Remote-PowerShell-Zugriff von einem beliebigen Ort haben, sodass Sie Ihre eigenen Regeln reparieren können. Beachten Sie, dass es bei dieser neuen Regel bis zu einer Stunde dauern kann, bis sie wirksam wird.

Als bewährte Methode erstellen Sie eine Clientzugriffsregel mit der höchsten Priorität, um den Zugriff auf Remote-PowerShell zu erhalten. Beispiel:

```
New-ClientAccessRule -Name "Always Allow Remote PowerShell" -Action Allow -AnyOfProtocols RemotePowerShell -Priority 1
```

#### **Authentifizierungsarten und Protokolle**

Nicht alle Authentifizierungstypen werden für alle Protokolle unterstützt. In dieser Tabelle werden die unterstützten Authentifizierungstypen pro Protokoll beschrieben:

	ADFS AUTHENTICATION	BASIC AUTHENTICATION	CERTIFICATEBASED AUTHENTICATION	NONBASIC AUTHENTICATION	OAuth AUTHENTICATION
Exchange ActiveSync	N/V	unterstützt	unterstützt	N/V	unterstützt
Exchange Admin Center	unterstützt	unterstützt	N/V	N/V	N/V
Exchange Web Services	N/V	N/V	N/V	N/V	N/V

	ADFS AUTHENTICATION	BASIC AUTHENTICATION	CERTIFICATE BASED AUTHENTICATION	NON BASIC AUTHENTICATION	OAUTH AUTHENTICATION
IMAP4	N/V	N/V	N/V	N/V	N/V
OfflineAddressBook	N/V	N/V	N/V	N/V	N/V
OutlookAnywhere	N/V	N/V	N/V	N/V	N/V
OutlookWebApp	unterstützt	unterstützt	N/V	N/V	N/V
POP3	N/V	N/V	N/V	N/V	N/V
PowerShellWebService	N/V	N/V	N/V	N/V	N/V
RemotePowerShell	N/V	unterstützt	N/V	unterstützt	N/V
REST	N/V	N/V	N/V	N/V	N/V
UniversalOutlook	N/V	N/V	N/V	N/V	N/V

## Clientzugriffsregel-Bedingungen und -Ausnahmen

Bedingungen und Ausnahmen in Clientzugriffsregeln identifizieren die Clientverbindungen, auf die die Regel angewendet oder nicht angewendet wird. Wenn beispielsweise die Regel den Zugriff durch Exchange ActiveSync-Clients blockiert, können Sie die Regel so konfigurieren, dass sie Exchange ActiveSync-Verbindungen von einem bestimmten Bereich von IP-Adressen zulässt. Die Syntax ist für eine Bedingung und die entsprechende Ausnahme identisch. Der einzige Unterschied ist: Bedingungen geben die einzuschließenden Clientverbindungen an, während Ausnahmen auszuschließende Clientverbindungen angeben.

Diese Tabelle beschreibt die Bedingungen und Ausnahmen, die in Clientzugriffsregeln zur Verfügung stehen:

BEDINGUNGSPARAMETER IN EXCHANGE ONLINE POWERSHELL	AUSNAHMENPARAMETER IN EXCHANGE ONLINE POWERSHELL	BESCHREIBUNG
AnyOfAuthenticationTypes	ExceptAnyOfAuthenticationTypes	<p>Gültige Werte sind:</p> <ul style="list-style-type: none"> <li>• AdfsAuthentication</li> <li>• BasicAuthentication</li> <li>• CertificateBasedAuthentication</li> <li>• NonBasicAuthentication</li> <li>• OAuthAuthentication</li> </ul> <p>Mehrere Werte können durch Kommata getrennt angegeben werden. Sie können die einzelnen Werte in Anführungszeichen einschließen ("value1","value2"), jedoch nicht alle Werte (Verwenden Sie nicht "value1,value2").</p>

BEDINGUNGSPARAMETER IN EXCHANGE ONLINE POWERSHELL	AUSNAHMENPARAMETER IN EXCHANGE ONLINE POWERSHELL	BESCHREIBUNG
<code>AnyOfClientIPAddressesOrRanges</code>	<code>ExceptAnyOfClientIPAddressesOrRanges</code>	<p>Gültige Werte sind:</p> <ul style="list-style-type: none"> <li>• <b>Eine einzelne IP-Adresse:</b> beispielsweise <code>192.168.1.1</code>.</li> <li>• <b>Eine IP-Adressbereich:</b> beispielsweise <code>192.168.0.1-192.168.0.254</code>.</li> <li>• <b>Classless Inter-Domain Routing (CIDR) IP:</b> beispielsweise <code>192.168.3.1/24</code>.</li> </ul> <p>Mehrere Werte können durch Kommas getrennt angegeben werden.</p>
<code>AnyOfProtocols</code>	<code>ExceptAnyOfProtocols</code>	<p>Gültige Werte sind:</p> <ul style="list-style-type: none"> <li>• <code>ExchangeActiveSync</code></li> <li>• <code>ExchangeAdminCenter</code></li> <li>• <code>ExchangeWebServices</code></li> <li>• <code>IMAP4</code></li> <li>• <code>OfflineAddressBook</code></li> <li>• <code>OutlookAnywhere</code> (einschließlich MAPI über HTTP)</li> <li>• <code>OutlookWebApp</code> (Outlook im Web)</li> <li>• <code>POP3</code></li> <li>• <code>PowerShellWebServices</code></li> <li>• <code>RemotePowerShell</code></li> <li>• <code>REST</code></li> <li>• <code>UniversalOutlook</code> (App e-Mail und Ihren Kalender)</li> </ul> <p>Sie können mehrere Werte durch Kommas getrennt angeben. Können Sie jedem einzelnen Wert in Anführungszeichen ("value1", "Wert2"), aber nicht um alle Werte ("Wert1, Wert2" nicht verwenden).</p> <p><b>Hinweis:</b> Wenn Sie diese Bedingung in einer Regel nicht verwenden, wird die Regel auf Alle Protokolle angewendet.</p>
<code>Scope</code>	n/v	<p>Gibt den Typ der Verbindungen an, auf die die Regel angewendet wird. Gültige Werte sind:</p> <ul style="list-style-type: none"> <li>• <code>Users</code>: Die Regel gilt nur für Endbenutzer Verbindungen.</li> <li>• <code>All</code>: Die Regel gilt für alle Arten von Verbindungen (Endbenutzer und Middle-Tier-apps).</li> </ul>
<code>UsernameMatchesAnyOfPatterns</code>	<code>ExceptUsernameMatchesAnyOfPatterns</code>	<p>Akzeptiert Text und das Platzhalterzeichen (*) zum Identifizieren des Benutzers Kontonamen im Format <code>&lt;Domain&gt;\&lt;UserName&gt;</code> (beispielsweise <code>contoso.com\jeff</code> oder <code>*jeff*</code> , aber nicht <code>jeff*</code> ). Nicht alphanumerische Zeichen erfordern keine Escapezeichen.</p> <p>Mehrere Werte können durch Kommas getrennt angegeben werden.</p>

BEDINGUNGSPARAMETER IN EXCHANGE ONLINE POWERSHELL	AUSNAHMENPARAMETER IN EXCHANGE ONLINE POWERSHELL	BESCHREIBUNG
<code>UserRecipientFilter</code>	n/v	<p>Verwendet OPath-Filter-Syntax zum Identifizieren des Benutzers, dem die Regel angewendet wird. Beispielsweise <code>{City -eq 'Redmond'}</code>. Die filterbaren Attribute sind:</p> <ul style="list-style-type: none"> <li>• <code>City</code></li> <li>• <code>Company</code></li> <li>• <code>CountryOrRegion</code></li> <li>• <code>CustomAttribute1</code> an <code>CustomAttribute15</code></li> <li>• <code>Department</code></li> <li>• <code>Office</code></li> <li>• <code>PostalCode</code></li> <li>• <code>StateOrProvince</code></li> <li>• <code>StreetAddress</code></li> </ul> <p>Die Suchkriterien verwendet die Syntax <code>{&lt;Property&gt; -&lt;Comparison operator&gt; '&lt;Value&gt;'}</code></p> <p>.</p> <ul style="list-style-type: none"> <li>• <code>&lt;Property&gt;</code> gefiltert wird.</li> <li>• <code>-&lt;Comparison Operator&gt;</code> ist ein Vergleichsoperator OPATH. Beispielsweise <code>-eq</code> nach genauen Übereinstimmungen (Platzhalter werden nicht unterstützt) und <code>-like</code> für Zeichenfolgenvergleiche (die mindestens ein Platzhalter in der Eigenschaftswert erforderlich ist). Weitere Informationen zu Vergleichsoperatoren finden Sie unter <a href="#">About_Comparison_Operators</a>.</li> <li>• <code>&lt;Value&gt;</code> ist der Wert der Eigenschaft. Textwerte mit oder ohne Leerzeichen oder Werte mit Platzhaltern (*) müssen in Anführungszeichen eingeschlossen werden (beispielsweise <code>'&lt;Value&gt;'</code> oder <code>'*&lt;Value&gt;'</code>).</li> </ul> <p>Verwenden Sie nicht mit dem Systemwert Anführungszeichen <code>\$null</code> (für leere Werte) oder ganzen Zahlen. Sie können mehrere Suchkriterien zusammen mit den logischen Operatoren verketten <code>-and</code> und <code>-or</code>. Beispielsweise</p> <pre><code>{&lt;Criteria1&gt;} -and {&lt;Criteria2&gt;}</code></pre> <p>oder</p> <pre><code>{(&lt;Criteria1&gt; -and &lt;Criteria2&gt;) -or &lt;Criteria3&gt;}</code></pre> <p>.</p>

# Verfahren für Clientzugriffsregeln in Exchange Online

18.12.2018 • 13 minutes to read

**Zusammenfassung:** Erfahren Sie, wie Sie Clientzugriffsregeln in Exchange Online erstellen, anzeigen, ändern, löschen und testen.

Clientzugriffsregeln ermöglichen oder blockieren Clientverbindungen mit Ihrer Exchange Online-Organisation basierend auf den Eigenschaften der Verbindung. Weitere Informationen zu Clientzugriffsregeln finden Sie unter [Clientzugriffsregeln in Exchange Online](#).

## TIP

Stellen Sie sicher, dass Ihre Regeln wie erwartet arbeiten. Testen Sie alle Regeln und die Interaktionen zwischen Regeln sorgfältig. Weitere Informationen finden Sie unter [Verwenden von Exchange Online PowerShell zum Testen von Clientzugriffsregeln](#) weiter unten in diesem Thema.

## Was sollten Sie wissen, bevor Sie beginnen?

- Geschätzte Zeit zum Abschließen der einzelnen Verfahren: Weniger als 5 Minuten
- Die Vorgehensweisen in diesem Thema sind nur in Exchange Online PowerShell verfügbar. Wie Sie mit Windows PowerShell eine Verbindung mit Exchange Online herstellen, können Sie unter [Herstellen einer Verbindung mit Exchange Online PowerShell](#) nachlesen.
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Nachrichtenübermittlung" in [Featureberechtigungen in Exchange Online](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#).

## Verwenden von Exchange Online PowerShell Access-Client-Regeln anzeigen

Führen Sie den folgenden Befehl aus, um zu einer Zusammenfassung aller Clientzugriffsregeln zurückzukehren:

```
Get-ClientAccessRule
```

Verwenden Sie die folgende Syntax, um detaillierte Informationen zu einer bestimmten Regel zurückzugeben:

```
Get-ClientAccessRule -Identity "<RuleName>" | Format-List [<Specific properties to view>]
```

In diesem Beispiel werden alle Eigenschaftswerte für die Regel namens "Block Client Connections from 192.168.1.0/24" zurückgegeben.

```
Get-ClientAccessRule -Identity "Block Client Connections from 192.168.1.0/24" | Format-List
```

In diesem Beispiel werden nur die angegebenen Eigenschaften für die gleiche Regel zurückgegeben.

```
Get-ClientAccessRule -Identity "Block Client Connections from 192.168.1.0/24" | Format-List  
Name,Priority,Enabled,Scope,Action
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Get-ClientAccessRule](#).

## Verwenden von Exchange Online PowerShell zum Erstellen von Clientzugriffsregeln

Verwenden Sie die folgende Syntax zum Erstellen von Clientzugriffsregeln in Exchange Online PowerShell:

```
New-ClientAccessRule -Name "<RuleName>" [-Priority <PriorityValue>] [-Enabled <$true | $false>] -Action  
<AllowAccess | DenyAccess> [<Conditions>] [<Exceptions>]
```

In diesem Beispiel wird eine Clientzugriffsregel mit der Bezeichnung "Block ActiveSync" erstellt, die den Zugriff für Exchange ActiveSync-Clients außerhalb des IP-Adressbereichs 192.168.10.1/24 blockiert.

```
New-ClientAccessRule -Name "Block ActiveSync" -Action DenyAccess -AnyOfProtocols ExchangeActiveSync -  
ExceptAnyOfClientIPAddressesOrRanges 192.168.10.1/24
```

### Hinweise:

- Es empfiehlt sich erstellen Sie eine Access-Client-Regel mit der höchsten Priorität den Administratorzugriff auf remote-PowerShell beibehalten. Beispiel:

```
New-ClientAccessRule -Name "Always Allow Remote PowerShell" -Action Allow -AnyOfProtocols  
RemotePowerShell -Priority 1
```

- Die Regel verwendet den Standardwert Priorität, da wir den Parameter *Priority* verwendet haben. Weitere Informationen finden Sie im Abschnitt "[Use Exchange Online PowerShell festlegen die Priorität von Access-Client-Regeln](#)" weiter unten in diesem Thema.
- Die Regel aktiviert ist, da es nicht der Parameter *Enabled* gibt verwenden, und der Standardwert ist `$true`.

Dieses Beispiel erstellt eine neue Client-Zugriffsregel mit der Exchange-Verwaltungskonsole Zugriff beschränken, die Blöcke für die Exchange-Verwaltungskonsole, mit Ausnahme von zugreifen, wenn der Client eine IP-Adresse im Bereich 192.168.10.1/24 stammt oder der Namen des Benutzerkontos "Tanyas" enthält.

```
New-ClientAccessRule -Name "Restrict EAC Access" -Action DenyAccess -AnyOfProtocols ExchangeAdminCenter -  
ExceptAnyOfClientIPAddressesOrRanges 192.168.10.1/24 -ExceptUsernameMatchesAnyOfPatterns *tanyas*
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [New-ClientAccessRule](#).

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Verwenden Sie eines der folgenden Verfahren, um sich zu vergewissern, dass Sie die Clientzugriffsregel erfolgreich erstellt haben:

- Führen Sie diesen Befehl im Exchange Online PowerShell, um die neue Regel in der Liste der Regeln finden Sie unter:

```
Get-ClientAccessRule
```

- Ersetzen Sie \_ <RuleName> \_ mit dem Namen der Regel, und führen dies Befehl aus, um die Details der Regel anzuzeigen:

```
Get-ClientAccessRule -Identity "<RuleName>" | Format-List
```

- Mithilfe des **Test-ClientAccessRule** -Cmdlets können Sie erfahren, welche Clientzugriffsregeln sich auf eine bestimmte Clientverbindung mit Exchange Online auswirken würden. Weitere Informationen finden Sie unter [Verwenden von Exchange Online PowerShell zum Testen von Clientzugriffsregeln](#) weiter unten in diesem Thema.

## Verwenden von Exchange Online PowerShell zum Ändern von Clientzugriffsregeln

Beim Ändern einer Clientzugriffsregel stehen keine zusätzlichen Einstellungen zur Verfügung. Es sind die gleichen Einstellungen, die bei der Erstellung der Regel verfügbar waren:

Verwenden Sie die folgende Syntax zum Ändern einer Clientzugriffsregel in Exchange Online PowerShell:

```
Set-ClientAccessRule -Identity "<RuleName>" [-Name "<NewName>"] [-Priority <PriorityValue>] [-Enabled <$true | $false>] -Action <AllowAccess | DenyAccess> [<Conditions>] [<Exceptions>]
```

In diesem Beispiel wird die vorhandene Clientzugriffsregel mit dem Namen „IMAP4 zulassen“ deaktiviert.

```
Set-ClientAccessRule -Identity "Allow IMAP4" -Enabled $false
```

Eine wichtige Überlegung beim Ändern von Clientzugriffsregeln ist das Ändern von Bedingungen oder Ausnahmen, die mehrere Werte akzeptieren:

- Die Werte, die Sie angeben können Sie alle vorhandenen Werte werden, *Ersetzen* .
- Verwenden Sie zum Hinzufügen oder entfernen Sie Werte ohne Auswirkungen auf andere vorhandene Werte, die folgende Syntax: `@{Add=<Value1>,"<Value2>"...; Remove=<Value1>,"<Value2>"...}`

In diesem Beispiel wird der IP-Adressbereich 172.17.17.27/16 der bestehenden Clientzugriffsregel mit der Bezeichnung "IMAP4 zulassen" hinzugefügt, ohne dabei bestehende IP-Adresswerte zu beeinflussen.

```
Set-ClientAccessRule -Identity "Allow IMAP4" -AnyOfClientIPAddressesOrRanges @{Add="172.17.17.27/16"}
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Set-ClientAccessRule](#).

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Verwenden Sie eines der folgenden Verfahren, um sich zu vergewissern, dass Sie die Clientzugriffsregel erfolgreich geändert haben:

- Ersetzen Sie \_ <RuleName> \_ mit dem Namen der Regel, und führen dies Befehl aus, um die Details der Regel anzuzeigen:

```
Get-ClientAccessRule -Identity "<RuleName>" | Format-List
```

- Mithilfe des **Test-ClientAccessRule** -Cmdlets können Sie erfahren, welche Clientzugriffsregeln sich auf

eine bestimmte Clientverbindung mit Exchange Online auswirken würden. Weitere Informationen finden Sie unter [Verwenden von Exchange Online PowerShell zum Testen von Clientzugriffsregeln](#) weiter unten in diesem Thema.

## Verwenden von Exchange Online PowerShell zum Festlegen der Priorität von Clientzugriffsregeln

Standardmäßig erhalten Clientzugriffsregeln eine Priorität, die auf der Reihenfolge ihrer Erstellung basiert (neuere Regeln haben eine niedrigere Priorität als ältere). Eine niedrigere Prioritätsnummer gibt eine höhere Priorität für die Regel an, und Regeln werden in der Reihenfolge der Priorität verarbeitet (Regeln mit einer höheren Priorität werden vor Regeln mit einer niedrigeren Priorität verarbeitet). Zwei Regeln können nicht dieselbe Priorität haben.

Die höchste Priorität, die Sie für eine Regel festlegen können, ist 1. Der niedrigste Wert, den Sie festlegen können, hängt von der Anzahl von Regeln ab. Wenn Sie z. B. fünf Regeln haben, können Sie die Prioritätswerte 1 bis 5 verwenden. Das Ändern der Priorität einer vorhandenen Regel kann sich entsprechend auf andere Regeln auswirken. Wenn Sie z. B. fünf Regeln haben (Priorität 1 bis 5), und Sie ändern die Priorität einer Regel von 5 in 2, so wird die vorhandene Regel mit Priorität 2 in Priorität 3 geändert, die Regel mit Priorität 3 wird in Priorität 4 geändert, und die Regel mit Priorität 4 wird in Priorität 5 geändert.

Verwenden Sie die folgende Syntax, um die Priorität einer Regel in Exchange Online PowerShell festzulegen:

```
Set-ClientAccessRule -Identity "<RuleName>" -Priority <Number>
```

In diesem Beispiel wird die Priorität der Regel namens „IMAP4 deaktivieren“ auf 2 festgelegt. Alle vorhandenen Regeln mit Priorität kleiner oder gleich 2 werden um 1 verringert (die Prioritätswerte werden um 1 erhöht).

```
Set-ClientAccessRule -Identity "Disable IMAP" -Priority 2
```

**Hinweis:** Verwenden Sie den Parameter *Priority* im Cmdlet **New-ClientAccessRule**, um die Priorität einer neuen Regel bei ihrer Erstellung festzulegen.

### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Verwenden Sie eines der folgenden Verfahren, um sich zu vergewissern, dass Sie die Priorität einer Clientzugriffsregel erfolgreich festgelegt haben:

- Führen Sie den folgenden Befehl in Exchange Online PowerShell aus, um die Liste der Regeln und die zugehörigen **Priority** -Werte anzuzeigen:

```
Get-ClientAccessRule
```

- Ersetzen Sie \_ <RuleName> \_ mit dem Namen der Regel ein, und führen Sie diesen Befehl:

```
Get-ClientAccessRule -Identity "<RuleName>" | Format-List Name,Priority
```

## Verwenden von Exchange Online PowerShell zum Entfernen von Clientzugriffsregeln

Verwenden Sie die folgende Syntax zum Entfernen von Clientzugriffsregeln in Exchange Online PowerShell:

```
Remove-ClientAccessRule -Identity "<RuleName>"
```

In diesem Beispiel wird die Clientzugriffsregel mit dem Namen „POP3 blockieren“ entfernt.

```
Remove-ClientAccessRule -Identity "Block POP3"
```

**Hinweis:** um eine Access-Client-Regel deaktivieren, ohne Sie zu löschen, verwenden Sie der Parameter *Enabled* gibt mit dem Wert `$false` im Cmdlet **Set-ClientAccessRule**.

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Remove-ClientAccessRule](#).

#### Woher wissen Sie, dass dieses Verfahren erfolgreich war?

Um sich zu vergewissern, dass Sie eine Clientzugriffsregel erfolgreich entfernt haben, führen Sie den folgenden Befehl in Exchange Online PowerShell aus. So können Sie überprüfen, dass die Regel nicht mehr aufgeführt wird:

```
Get-ClientAccessRule
```

## Verwenden von Exchange Online PowerShell zum Testen von Clientzugriffsregeln

Verwenden Sie die folgende Syntax, um zu sehen, welche Clientzugriffsregeln sich auf eine bestimmte Clientverbindung mit Exchange Online auswirken würden:

```
Test-ClientAccessRule -User <MailboxIdentity> -AuthenticationType <AuthenticationType> -Protocol <Protocol> -  
RemoteAddress <ClientIPAddress> -RemotePort <TCPPortNumber>
```

In diesem Beispiel werden die Clientzugriffsregeln zurückgegeben, die einer Clientverbindung mit Exchange Online entsprechen würden, die die folgenden Eigenschaften aufweist:

- **Authentifizierungstyp:** grundlegende
- **Protokoll:** `OutlookWebApp`
- **Remote-Adresse:** 172.17.17.26
- **Remoteport:** 443
- **Benutzer:** julia@contoso.com

```
Test-ClientAccessRule -User julia@contoso.com -AuthenticationType BasicAuthentication -Protocol OutlookWebApp  
-RemoteAddress 172.17.17.26 -RemotePort 443
```

Ausführliche Informationen zu Syntax und Parametern finden Sie unter [Test-ClientAccessRule](#).

# Deaktivieren der Standardauthentifizierung in Exchange Online

18.12.2018 • 21 minutes to read

Standardauthentifizierung in Exchange Online verwendet einen Benutzernamen und ein Kennwort für Access-Clientanforderungen. Blockieren von Standardauthentifizierung hilft bei Ihrer Exchange Online-Organisation brute-Force- oder Kennwort Sprühende Angriffen zu schützen. Wenn Sie die Standardauthentifizierung für Benutzer in Exchange Online deaktivieren, müssen ihre e-Mail-Clients und apps modernen Authentifizierung unterstützen. Diese Clients sind:

- Outlook 2013 oder höher (Outlook 2013 [erfordert eine wichtige Änderung der Registrierung](#))
- Outlook-2016 für Mac oder höher
- Outlook für iOS und Android
- E-Mails für iOS 11.3.1 oder höher

Wenn Ihre Organisation keine legacy-e-Mail-Clients verfügt, können Sie Authentifizierungsrichtlinien für die in Exchange Online Standardauthentifizierung Anforderungen, deaktivieren die erzwingt, dass alle Access-Clientanforderungen, moderne Authentifizierung zu verwenden. Weitere Informationen zur modernen Authentifizierung finden Sie unter [Verwenden von Office 365 modernen Authentifizierung mit Office-Clients](#).

In diesem Thema wird erläutert, wie die Standardauthentifizierung verwendet wird und in Exchange Online und die entsprechenden Verfahren zur Authentifizierungsrichtlinien blockiert.

## Funktionsweise der Standardauthentifizierung in Exchange Online

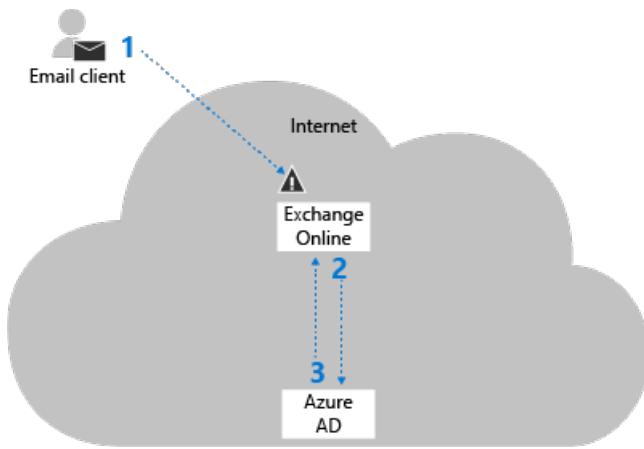
Die Standardauthentifizierung ist auch bekannt als *Proxy-Authentifizierung*, da der e-Mail-Client den Benutzernamen und das Kennwort zu Exchange Online und Exchange Online Weiterleitungen oder Proxys die Anmeldeinformationen an einen autorisierenden Identitätsanbieter (IdP überträgt) im Namen der e-Mail-Client oder die app. Die IdP hängt von Ihrer Organisation Authentifizierungsmodell:

- **Cloud-Authentifizierung:** die IdP Azure Active Directory ist.
- **Federated Authentifizierung:** die IdP ist eine lokale Lösung wie Active Directory-Verbunddienste (AD FS).

In den folgenden Abschnitten werden diese Authentifizierungsmodelle beschrieben.

### Cloud-Authentifizierung

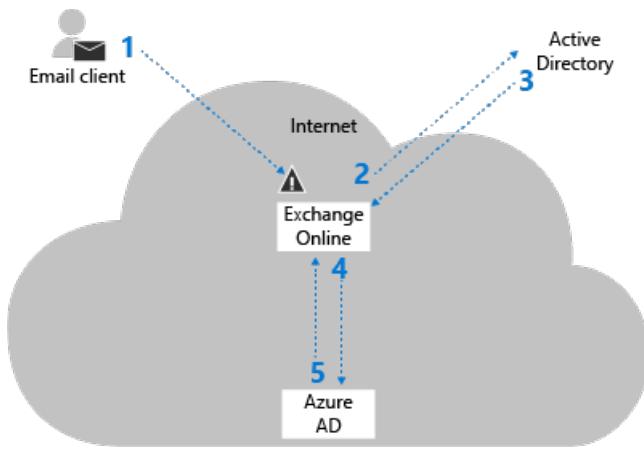
In der folgenden Abbildung werden die Schritte in der Cloud-Authentifizierung beschrieben:



1. Der e-Mail-Client sendet den Benutzernamen und das Kennwort zu Exchange Online.
- Hinweis:** Wenn die Standardauthentifizierung gesperrt ist, an dieser Stelle blockiert.
2. Exchange Online sendet Benutzername und Kennwort, zu Azure Active Directory.
  3. Azure Active Directory gibt ein Benutzerticket zu Exchange Online und der Benutzer authentifiziert.

### Verbundauthentifizierung

In der folgenden Abbildung werden die Schritte in Verbundauthentifizierung beschrieben:



1. Der e-Mail-Client sendet den Benutzernamen und das Kennwort zu Exchange Online.
- Hinweis:** Wenn die Standardauthentifizierung gesperrt ist, an dieser Stelle blockiert.
2. Exchange Online sendet Benutzername und Kennwort, an die lokalen IdP.
  3. Exchange Online empfängt ein Token Security Assertion Markup Language (SAML) von der lokalen IdP.
  4. Exchange Online sendet das SAML-Token an Azure Active Directory.
  5. Azure Active Directory gibt ein Benutzerticket zu Exchange Online und der Benutzer authentifiziert.

## Wie die Standardauthentifizierung in Exchange Online blockiert wird

Blockieren Sie Standardauthentifizierung in Exchange Online durch Erstellen und Zuweisen von Authentifizierungsrichtlinien für die für einzelne Benutzer. Die Richtlinien definieren der Clientprotokolle wobei Standardauthentifizierung wird blockiert und Zuweisen der Richtlinie auf einen oder mehrere Benutzer ihre Standardauthentifizierung Anforderungen für die angegebenen Protokolle blockiert.

Blockiert, wird der erste Schritt (Schritt 1 im vorherigen Diagramm) Vorauthentifizierung vor der Anforderung erreicht Azure Active Directory oder die lokale IdP Standardauthentifizierung in Exchange Online blockiert. Die Vorteile dieses Ansatzes ist brute-Force- oder Kennwort Sprühende Angriffen die IdP (das Konto Sperre aufgrund

von falschen Anmeldeversuchen auslösen kann) nicht erreichen kann.

Da Authentifizierungsrichtlinien für die auf Benutzerebene verwendet werden, können Exchange Online nur Standardauthentifizierung Anfragen für Benutzer zu blockieren, die in der Cloud-Organisation vorhanden sind. Für Verbundauthentifizierung Wenn ein Benutzer nicht im Exchange Online, vorhanden werden den Benutzernamen und das Kennwort an die lokalen IdP weitergeleitet. Betrachten Sie beispielsweise die folgenden Szenarios:

1. Eine Organisation hat die verbunddomäne "contoso.com" und Verwendungsmöglichkeiten der lokale AD FS für die Authentifizierung.
2. Die Benutzer ian@contoso.com vorhanden ist, in der lokalen Organisation verwenden, jedoch nicht in Office 365 (es ist kein Benutzerkonto in Azure Active Directory und keine Empfängerobjekt in der Exchange Online globale Adressliste).
3. Ein e-Mail-Client sendet eine Anforderung für die Anmeldung zu Exchange Online mit dem Benutzernamen ian@contoso.com. Eine Authentifizierungsrichtlinie nicht für den Benutzer angewendet werden, und die Authentifizierungsanforderung für ian@contoso.com wird gesendet, auf dem lokalen AD FS.
4. Lokale AD FS annehmen oder Ablehnen der Authentifizierungsanforderung für ian@contoso.com können. Wenn die Anforderung akzeptiert wird, wird ein SAML-Token zu Exchange Online zurückgegeben. Solange das SAML-Token **ImmutableId** Wert einen Benutzer in Azure Active Directory übereinstimmt, wird Azure AD ein Benutzerticket zu Exchange Online ausstellen, die (der Wert **ImmutableId** wird während des Setups Azure Active Directory verbinden festgelegt).

In diesem Szenario, wenn "contoso.com" Verwendungsmöglichkeiten der lokale AD FS-Server für die Authentifizierung der lokalen AD FS-Server noch erhalten Authentifizierungsanfragen für nicht vorhandene Benutzernamen aus Exchange Online während einer Kennwort Sprühbereichs Angriffs.

## Richtlinie Authentifizierungsverfahren in Exchange Online

Sie können alle Aspekte der in Exchange Online PowerShell Authentifizierungsrichtlinien verwalten. In der folgenden Tabelle werden die Protokolle und Dienste in der Exchange-Online, die Sie für die Standardauthentifizierung blockieren beschrieben.

PROTOKOLL ODER DIENST	BESCHREIBUNG	PARAMETERNAME
Exchange ActiveSync (EAS)	Wird von einigen e-Mail-Clients auf mobilen Geräten verwendet.	<i>AllowBasicAuthActiveSync</i>
AutoErmittlung	Outlook und EAS-Clients, die zum Suchen und Verbinden mit Postfächern in Exchange Online	<i>AllowBasicAuthAutodiscover</i>
IMAP4	Wird von IMAP-e-Mail-Clients verwendet.	<i>AllowBasicAuthImap</i>
MAPI über HTTP (MAPI/HTTP)	Von Outlook 2013 und höher verwendet.	<i>AllowBasicAuthMapi</i>
Offline Address Book (OAB)	Eine Kopie der Adresse Liste Websitesammlungen, die heruntergeladen und von Outlook verwendet werden.	<i>AllowBasicAuthOfflineAddressBook</i>
Outlook-Dienst	Wird von der app E-Mail und Ihren Kalender für Windows 10 verwendet.	<i>AllowBasicAuthOutlookService</i>

PROTOKOLL ODER DIENST	BESCHREIBUNG	PARAMETERNAME
POP3	Wird von POP-e-Mail-Clients verwendet.	<i>AllowBasicAuthPop</i>
-Webdiensten für Berichte	Zum Abrufen von Berichtsdaten in Exchange Online verwendet.	<i>AllowBasicAuthReportingWebServices</i>
Exchange Representational State Transfer (REST)	Eine Programmierung verbunden, die von Drittanbieter-apps verwendet wird.	<i>AllowBasicAuthRest</i>
Outlook Anywhere (RPC über HTTP)	Von Outlook 2016 und früher verwendet.	<i>AllowBasicAuthRpc</i>
Authentifizierte SMTP	Von POP- und IMAP-Client verwendet zum Senden von e-Mail-Nachrichten.	<i>AllowBasicAuthSsmtp</i>
Exchange-Webdienste (Exchange Web Services, EWS)	Eine Programmierschnittstelle, die von Outlook, Outlook für Mac und Drittanbieter-apps verwendet wird.	<i>AllowBasicAuthWebServices</i>
PowerShell	Verbindung mit Exchange Online mit remote-PowerShell verwendet. Wenn Sie die Standardauthentifizierung für Exchange Online PowerShell blockieren, müssen Sie mit der Exchange Online-PowerShell-Modul hergestellt werden soll. Eine Anleitung finden Sie unter <a href="#">Connect to Exchange Online PowerShell mehrstufige Authentifizierung verwenden</a> .	<i>AllowBasicAuthPowerShell</i>

In der Regel, wenn Sie die Standardauthentifizierung für einen Benutzer blockieren, sollten Sie die Standardauthentifizierung für alle Protokolle blockieren. Sie können jedoch die \*AllowBasicAuth\* \* Parameter (Optionen) in den Cmdlets **New-AuthenticationPolicy** und **Set-AuthenticationPolicy** selektiv zulassen oder blockieren Standardauthentifizierung für bestimmte Protokolle.

Für e-Mail-Clients und apps, die moderne Authentifizierung nicht unterstützen, müssen Sie für die Protokolle und Dienste, die sie benötigen Standardauthentifizierung zulassen. Diese Protokolle und Dienste werden in der folgenden Tabelle beschrieben:

CLIENT	PROTOKOLLE UND DIENSTE
Outlook 2013 und höher	<ul style="list-style-type: none"> <li>• Für die AutoErmittlung</li> <li>• Exchange-Webdienste (EWS)</li> <li>• MAPI über HTTP</li> <li>• Outlook im Anywhere (RPC über HTTP)</li> <li>• Des Offlineadressbuchs (OAB)</li> </ul>
Outlook für Mac 2016	<ul style="list-style-type: none"> <li>• Für die AutoErmittlung</li> <li>• EWS</li> </ul>
Exchange ActiveSync-Clients (beispielsweise iOS Mail 11.3.1)	<ul style="list-style-type: none"> <li>• Für die AutoErmittlung</li> <li>• ActiveSync (EAS)</li> </ul>
POP-clients	<ul style="list-style-type: none"> <li>• POP3</li> <li>• Authentifizierten SMTP</li> </ul>

CLIENT	PROTOKOLLE UND DIENSTE
IMAP-clients	<ul style="list-style-type: none"> <li>• IMAP4</li> <li>• Authentifizierten SMTP</li> </ul>

**Hinweis:** Standardauthentifizierung blockierende blockieren, app-Kennwörter in Exchange Online. Weitere Informationen zu app-Kennwörtern finden Sie unter [Erstellen eines app-Kennwort für Office 365](#).

### Was sollten Sie wissen, bevor Sie beginnen?

- Stellen Sie sicher, dass die moderne Authentifizierung in Ihrer Exchange Online-Organisation aktiviert ist (standardmäßig aktiviert). Weitere Informationen finden Sie unter [Aktivieren oder Deaktivieren der modernen Authentifizierung in Exchange Online](#).
- Überprüfen Sie Ihre e-Mail-Clients und apps modernen-Authentifizierung unterstützen (siehe die Liste am Anfang des Themas). Darüber hinaus stellen Sie sicher, dass Ihr Outlook-Desktopclients den mindestens erforderlichen kumulativen Updates ausgeführt werden. Weitere Informationen finden Sie unter [Outlook-Updates](#).
- Herstellen einer Verbindung mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online PowerShell](#).

### Erstellen und Anwenden von Authentifizierungsrichtlinien für die

Die Schritte zum Erstellen und Anwenden von Authentifizierungsrichtlinien für, um die Standardauthentifizierung in Exchange Online blockieren sind:

1. Erstellen Sie die Authentifizierungsrichtlinie.
2. Die Authentifizierungsrichtlinie Benutzern zuweisen.
3. Warten Sie 24 Stunden für die Richtlinie auf Benutzer angewendet werden soll, oder erzwingen Sie die Richtlinie sofort angewendet werden soll.

Diese Schritte werden in den folgenden Abschnitten beschrieben.

#### Schritt 1: Erstellen der Authentifizierungsrichtlinie

Zum Erstellen einer Richtlinie der Blöcke Standardauthentifizierung für alle verfügbaren Clientprotokolle in Exchange Online (die empfohlene Konfiguration), verwenden Sie die folgende Syntax:

```
New-AuthenticationPolicy -Name "<Descriptive Name>"
```

Dieses Beispiel erstellt eine Authentifizierungsrichtlinie mit dem Namen grundlegende AUTH blockieren.

```
New-AuthenticationPolicy -Name "Block Basic Auth"
```

Ausführliche Parameterinformationen zu Syntax und finden Sie unter [New-AuthenticationPolicy](#).

#### Hinweise:

- Sie können nicht den Namen der Richtlinie ändern, nach der Erstellung (der Parameter *Name* nicht im Cmdlet **Set-AuthenticationPolicy** verfügbar).
- Um die Aktivierung der Standardauthentifizierung für bestimmte Protokolle in der Richtlinie, finden Sie im Abschnitt "Ändern Authentifizierungsrichtlinien" weiter unten in diesem Thema. Die gleichen Protokoll Einstellungen sind verfügbar in den Cmdlets **New-AuthenticationPolicy** und **Set-AuthenticationPolicy**, und die Schritte zur Aktivierung der Standardauthentifizierung für bestimmte Protokolle sind die gleichen für beide Cmdlets.

## Schritt 2: Die Authentifizierungsrichtlinie Benutzern zuweisen

Es gibt drei grundlegende Methoden, die Sie verwenden können, um Authentifizierungsrichtlinien Benutzern zuweisen:

- **Einzelne Benutzerkonten:** Verwenden Sie die folgende Syntax:

```
Set-User -Identity <UserIdentity> -AuthenticationPolicy <PolicyIdentity>
```

Dieses Beispiel weist die Richtlinie mit dem Namen der Benutzer Konto laura@contoso.com Standardauthentifizierung blockieren.

```
Set-User -Identity laura@contoso.com -AuthenticationPolicy "Block Basic Auth"
```

- **Filtern von Benutzerkonten durch Attribute:** Diese Methode erfordert, dass die Benutzerkonten, die alle ein eindeutigen filterbaren Attribut (z. B. Titel oder Abteilung), die Sie verwenden können freigeben, um die Benutzer zu identifizieren. Die Syntax verwendet die folgenden Befehle (zwei zum Identifizieren der Benutzerkonten und andere anwenden die Richtlinie auf die Benutzer):

```
$<VariableName1> = Get-User -ResultSize unlimited -Filter <Filter>
```

```
$<VariableName2> = $<VariableName1>.MicrosoftOnlineServicesID
```

```
$<VariableName2> | foreach {Set-User -Identity $_ -AuthenticationPolicy "Block Basic Auth"}
```

Dieses Beispiel weist die Richtlinie mit dem Namen Block Standardauthentifizierung für alle Benutzerkonten, deren **Title** -Attribut den Wert "Sales Associate" enthält.

```
$SalesUsers = Get-User -ResultSize unlimited -Filter {(RecipientType -eq 'UserMailbox') -and (Title -like '*Sales Associate*')}
```

```
$Sales = $SalesUsers.MicrosoftOnlineServicesID
```

```
$Sales | foreach {Set-User -Identity $_ -AuthenticationPolicy "Block Basic Auth"}
```

- **Verwenden einer Liste von bestimmten Benutzerkonten:** Diese Methode ist eine Textdatei, um die Benutzerkonten zu identifizieren. Werte, die keine Leerzeichen enthalten (beispielsweise die Office 365 arbeiten oder Schule Konto) am besten. Die Textdatei muss ein Benutzerkonto in jeder Zeile wie die folgende enthalten:

```
akol@contoso.com
```

```
tjohnston@contoso.com
```

```
kakers@contoso.com
```

Die Syntax verwendet die folgenden zwei Befehle (eine, um die Benutzerkonten und andere anwenden die Richtlinie auf die Benutzer identifizieren):

```
$<VariableName> = Get-Content "<text file>"
```

```
$<VariableName> | foreach {Set-User -Identity $_ -AuthenticationPolicy <PolicyIdentity>}
```

Dieses Beispiel weist die Richtlinie mit dem Namen Standardauthentifizierung Block mit den Benutzerkonten, die in der Datei C:\My Documents\BlockBasicAuth.txt angegeben.

```
$BBA = Get-Content "C:\My Documents\BlockBasicAuth.txt"
```

```
$BBA | foreach {Set-User -Identity $_ -AuthenticationPolicy "Block Basic Auth"}
```

**Hinweis:** Wenn die richtlinienzuweisung von Benutzern entfernen möchten, verwenden Sie den Wert `$null` für den Parameter *AuthenticationPolicy* im Cmdlet **Set-User**.

#### Schritt 3: (Optional) gelten sofort die Authentifizierungsrichtlinie für Benutzer

Standardmäßig werden die Änderungen beim Erstellen oder ändern Sie die Authentifizierung richtlinienzuweisung auf Benutzer oder aktualisieren die Richtlinie wirksam innerhalb von 24 Stunden. Wenn Sie die Richtlinie innerhalb von 30 Minuten wirksam möchten, verwenden Sie die folgende Syntax:

```
Set-User -Identity <UserIdentity> -STSRefreshTokensValidFrom $([System.DateTime]::UtcNow)
```

In diesem Beispiel wird die Authentifizierungsrichtlinie sofort für die Benutzer laura@contoso.com.

```
Set-User -Identity laura@contoso.com -STSRefreshTokensValidFrom $([System.DateTime]::UtcNow)
```

In diesem Beispiel wird die Authentifizierungsrichtlinie sofort zu mehreren Benutzern, die zuvor von filterbaren Attribute oder eine Textdatei angegeben wurden. Dieses Beispiel funktioniert, wenn Sie sich noch in der gleichen PowerShell-Sitzung und Sie nicht die Benutzer, die (nicht den gleichen Variablennamen anschließend zu einem anderen Zweck verwendet) verwendeten Variablen geändert haben. Zum Beispiel:

```
$Sales | foreach {Set-User -Identity $_ -STSRefreshTokensValidFrom $([System.DateTime]::UtcNow)}
```

oder

```
$BBA | foreach {Set-User -Identity $_ -STSRefreshTokensValidFrom $([System.DateTime]::UtcNow)}
```

#### Die Authentifizierungsrichtlinien anzeigen

Um eine Liste mit den Namen aller vorhandenen Authentifizierung-Richtlinien anzuzeigen, führen Sie den folgenden Befehl ein:

```
Get-AuthenticationPolicy | Format-Table -Auto Name
```

Um ausführliche Informationen zu einer bestimmten Authentifizierungsrichtlinie anzuzeigen, verwenden Sie folgende Syntax:

```
Get-AuthenticationPolicy -Identity <PolicyIdentity>
```

In diesem Beispiel werden detaillierte Informationen über die Richtlinie mit dem Namen Block grundlegende auth. zurückgegeben

```
Get-AuthenticationPolicy -Identity "Block Basic Auth"
```

Ausführliche Parameterinformationen zu Syntax und finden Sie unter [Get-AuthenticationPolicy](#).

### Ändern von Authentifizierungsrichtlinien für die

In der Standardeinstellung wird beim Erstellen einer neuen Authentifizierungsrichtlinie für die ohne Angabe von keine Protokolle Standardauthentifizierung für alle Clientprotokolle in Exchange Online blockiert. Anders ausgedrückt, der Standardwert von der \*AllowBasicAuth\* \* Parameter (Optionen) ist `False` für alle Protokolle.

- Um die Aktivierung der Standardauthentifizierung für ein bestimmtes Protokoll, das deaktiviert ist, geben Sie die Option ohne einen Wert ein.
- Wenn Sie die Standardauthentifizierung für ein bestimmtes Protokoll deaktivieren, die aktiviert ist, können Sie nur den Wert `:$false`.

Können Sie das Cmdlet **Get-AuthenticationPolicy** der aktuelle Status der finden Sie unter der \*AllowBasicAuth\* \* Switches in der Richtlinie.

In diesem Beispiel aktiviert die Standardauthentifizierung für das POP3-Protokoll und deaktiviert die Standardauthentifizierung für das IMAP4-Protokoll in der vorhandenen Authentifizierungsrichtlinie namens grundlegende AUTH blockieren.

```
Set-AuthenticationPolicy -Identity "Block Basic Auth" -AllowBasicAuthPop -AllowBasicAuthImap:$false
```

Ausführliche Parameterinformationen zu Syntax und finden Sie unter [Set-AuthenticationPolicy](#).

### Konfigurieren Sie die Standardrichtlinie für die Authentifizierung

Die Standardrichtlinie für die Authentifizierung wird für alle Benutzer zugewiesen, die nicht bereits eine bestimmte Richtlinie zugewiesen haben. Beachten Sie, dass Benutzer zugewiesenen Authentifizierungsrichtlinien der Standardrichtlinie Vorrang. Verwenden Sie folgende Syntax, um die Standardrichtlinie für die Authentifizierung für die Organisation zu konfigurieren:

```
Set-OrganizationConfig -DefaultAuthenticationPolicy <PolicyIdentity>
```

Das folgende Beispiel konfiguriert die Authentifizierungsrichtlinie namens Block Standardauthentifizierung als die Standardrichtlinie.

```
Set-OrganizationConfig -DefaultAuthenticationPolicy "Block Basic Auth"
```

**Hinweis:** Wenn die Standard-Authentifizierung Richtlinie Bezeichnung entfernen möchten, verwenden Sie den Wert `$null` für den Parameter *DefaultAuthenticationPolicy*.

### Entfernen von Authentifizierungsrichtlinien für die

Verwenden Sie folgende Syntax, um eine vorhandene Authentifizierungsrichtlinie zu entfernen:

```
Remove-AuthenticationPolicy -Identity <PolicyIdentity>
```

Dieses Beispiel entfernt die Richtlinie mit dem Namen Auth-Richtlinie testen.

```
Remove-AuthenticationPolicy -Identity "Test Auth Policy"
```

Ausführliche Parameterinformationen zu Syntax und finden Sie unter [Remove-AuthenticationPolicy](#).

### **Woher wissen Sie, dass Sie die Standardauthentifizierung in Exchange Online erfolgreich deaktiviert haben?**

Wenn eine Authentifizierungsrichtlinie Standardauthentifizierung Anfragen eines bestimmten Benutzers für ein bestimmtes Protokoll in Exchange Online blockiert, ist die Antwort `401 Unauthorized`. Keine zusätzlichen Informationen wird an den Client zur Vermeidung Speicherverluste verursachen, zusätzliche Informationen über den blockierten Benutzer zurückgegeben. Ein Beispiel für die Antwort sieht folgendermaßen aus:

```
HTTP/1.1 401 Unauthorized
Server: Microsoft-IIS/10.0
request-id: 413ee498-f337-4b0d-8ad5-50d900eb1f72
X-CalculatedBETarget: DM5PR2101MB0886.namprd21.prod.outlook.com
X-BackEndHttpStatus: 401
Set-Cookie: MapiRouting=#####
X-ServerApplication: Exchange/15.20.0485.000
X-RequestId: {3146D993-9082-4D57-99ED-9E7D5EA4FA56}:8
X-ClientInfo: {B0DD130A-CDBF-4CFA-8041-3D73B4318010}:59
X-RequestType: Bind
X-DiagInfo: DM5PR2101MB0886
X-BEServer: DM5PR2101MB0886
X-Powered-By: ASP.NET
X-FEServer: MA1PR0101CA0031
WWW-Authenticate: Basic Realm="" ,Basic Realm=""
Date: Wed, 31 Jan 2018 05:15:08 GMT
Content-Length: 0
```

# Aktivieren oder Deaktivieren der modernen Authentifizierung in Exchange Online

18.12.2018 • 2 minutes to read

Die moderne Authentifizierung in Office 365 ermöglicht Authentifizierungsfeatures wie mehrstufige Authentifizierung (MFA) über Smartcards, zertifikatbasierte Authentifizierung (CBA) und SAML-Identitätsanbieter von Dritten. Moderne Authentifizierung basiert auf [Active Directory Authentication Library](#) (ADAL) und OAuth 2.0.

Wenn Sie die moderne Authentifizierung in Exchange Online, Outlook 2016 und Outlook 2013 (Version 15.0.4753 oder höher, mit einer erforderlichen Registrierungseinstellung) aktivieren, melden Sie sich bei Office 365-Postfächern mit der modernen Authentifizierung an. Weitere Informationen finden Sie unter [Funktionsweise der modernen Authentifizierung in Office 2013 und Office 2016](#).

Wenn Sie die moderne Authentifizierung in Exchange Online, Outlook 2016 und Outlook 2013 deaktivieren, melden Sie sich bei Office 365-Postfächern mit der Standardauthentifizierung an. Die moderne Authentifizierung wird nicht verwendet.

## Anmerkungen

- Die moderne Authentifizierung ist in Exchange Online, Skype for Business Online und SharePoint Online standardmäßig aktiviert.
- Andere in Office 365 verfügbare Outlook-Clients (z. B. Outlook Mobile und Outlook für Mac 2016) verwenden zum Anmelden bei Office 365-Postfächern immer die moderne Authentifizierung.
- Sie sollten den Status der modernen Authentifizierung in Exchange Online mit Skype for Business Online synchronisieren, um mehrere Anmeldeaufforderungen in Skype for Business-Clients zu verhindern. Anweisungen finden Sie unter <https://aka.ms/SkypeModernAuth>.

## Aktivieren oder Deaktivieren der modernen Authentifizierung in Exchange Online

1. Stellen Sie eine Verbindung mit Exchange Online PowerShell her, wie [hier](#) beschrieben.

2. Führen Sie einen der folgenden Schritte aus:

- Führen Sie diesen Befehl aus, um die modernen Authentifizierung in Exchange Online zu aktivieren:

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

- Führen Sie diesen Befehl aus, um die modernen Authentifizierung in Exchange Online zu deaktivieren:

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $false
```

3. Führen Sie den folgenden Befehl aus, um sich zu vergewissern, dass die Änderung erfolgreich war:

```
Get-OrganizationConfig | Format-Table -Auto Name,OAuth*
```

## Siehe auch

[Verwenden der modernen Authentifizierung in Office 365 mit Office-Clients](#)

# Überwachung, Berichterstellung und Nachrichtenablaufverfolgung in Exchange Online

18.12.2018 • 10 minutes to read

Exchange Online stellt viele verschiedene Berichte bereit, die Ihnen dabei helfen, den Gesamtstatus und die Integrität Ihres Unternehmens zu bestimmen. Außerdem gibt es Tools, mit denen Sie die Problembehebung für bestimmte Ereignisse (wenn beispielsweise eine Nachricht nicht beim gewünschten Empfänger ankommt) durchführen können, sowie Überwachungsberichte zur Einhaltung von Vorschriften. In der folgenden Tabelle sind die für Exchange Online-Administratoren verfügbaren Berichte und Problembehandlungstools beschrieben.

## NOTE

Informationen zur Zuordnung von Berichten aus dem alten Office 365 Admin Center finden Sie unter [Wo wurde mein Office 365-Bericht gespeichert?](#).

FEATURE	BESCHREIBUNG	VERFÜGBAR UNTER	WEITERE INFORMATIONEN
<b>Verwendungsberichte im Office 365 Admin Center</b>	<p><b>Office 365 Gruppen</b></p> <p><b>Aktivität:</b> Anzeigen von Informationen über die Anzahl der Office 365-Gruppen, die erstellt und verwendet werden.</p> <p><b>E-Mail-Aktivität:</b> Anzeigen von Informationen über die Anzahl der Nachrichten gesendet und empfangen sowie in der gesamten Organisation sowie von bestimmten Benutzern zu lesen.</p> <p><b>E-Mail-app-Nutzung:</b> Anzeigen von Informationen zu den e-Mail-apps, die eine Verbindung mit Exchange Online herstellen. Dazu gehören die Gesamtzahl der Verbindungen für die jeweilige app und die Versionen von Outlook, die eine Verbindung herstellen.</p> <p><b>Postfachnutzung:</b> Anzeigen von Informationen über Speicher verwendet, Kontingents, Elementanzahl und letzte Aktivität (senden oder Lesen Aktivität) für Postfächer.</p>	Im Office 365 Administrationscenter unter <a href="https://portal.office.com/adminportal/home">https://portal.office.com/adminportal/home</a> , klicken Sie auf Berichte > Usage. Klicken Sie am oberen Rand des Dashboards auswählen eines Berichts auf. In der in der Dropdown-Liste, die angezeigt wird, stellen Sie eine der folgenden Auswahlmöglichkeiten: Office 365-Abschnitt: Office 365 gruppiert ActivityExchange Abschnitt: E-Mail-ActivityEmail app UsageMailbox-Nutzung	<a href="#">Office 365-Berichte im Admin Center - Office 365-Gruppen</a> <a href="#">Office 365-Berichte im Admin Center - E-Mail-Aktivitäten</a> <a href="#">Office 365-Berichte im Admin Center - Nutzung der E-Mail-Apps</a> <a href="#">Office 365-Berichte im Admin Center - Postfachnutzung</a>

FEATURE	BESCHREIBUNG	VERFÜGBAR UNTER	WEITERE INFORMATIONEN
<b>Sicherheit und Compliance-Berichte im Office 365 Administrationscenter</b>	<p>Diese erweiterte Berichte bieten eine interaktive Berichte wünschen Informationen zu Exchange Online-Administratoren, die zusammenfassende Informationen und die Möglichkeit, Drilldown für weitere Details enthält.</p> <p><b>Verhinderung von Datenverlust (DLP):</b> Anzeigen von Informationen zu DLP-Richtlinien und Regeln, die Nachrichten, die vertrauliche Daten enthalten, geben Sie und Ihr Unternehmen auswirken.</p> <p><b>Hinweis:</b> Verhinderung von Datenverlust ist nur in bestimmten Exchange Online-Abonnementplänen verfügbar. Weitere Informationen dazu finden Sie in den Einträgen zu <b>Verhinderung von Datenverlust</b> in der <a href="#">Exchange Online Protection-Dienstbeschreibung</a>.</p> <p><b>Erweiterte Threat Protection (ATP):</b> Anzeigen von Informationen zu sicheren Links und sichere Anlagen, die Teil der ATP sind.</p> <p><b>Hinweis:</b> ATP steht in Office 365 Enterprise E5 zur Verfügung, Sie können ATP aber auch als Add-On bei anderen Abonnementplänen erwerben. Weitere Informationen finden Sie unter <a href="#">Office 365 Advanced Threat Protection-Dienstbeschreibung</a>.</p> <p><b>Exchange Online Protection (EOP):</b> Anzeigen von Informationen zu erkannte Schadsoftware, gefälschten Nachrichten, spamerkennungen und e-Mail-Fluss zu und von Ihrer Organisation.</p>	<p>In der Office 365-Sicherheit und Compliance Center unter <a href="https://protection.office.com">https://protection.office.com</a>, klicken Sie auf Berichte &gt; Dashboard. Wählen Sie eine der Berichte, die auf der Seite verfügbar sind: DLP-Berichte: DLP-Richtlinie Übereinstimmungen und DLP falsch positive Ergebnisse und überschreibt. ATP Berichte: ATP Dateitypen, ATP Nachricht Disposition und Bedrohung Schutzstatus. EOP-Berichte: erkannte Schadsoftware, wichtigste Schadsoftware, häufigste Absender und Empfänger Spoofing Mail, spamerkennungen und gesendet und Empfangen von e-Mail-Nachrichten.</p>	<p>Anzeigen der Berichte zur Verhinderung von Datenverlust Anzeigen der Berichte zu Advanced Threat Protection und Exchange Online Protection</p>
<b>Benutzerdefinierte Berichte mit Microsoft Graph</b>	Programmgesteuertes Erstellen der Berichte, die im Office 365 Administrationscenter verfügbar sind, mithilfe von Microsoft Graph	n/v	Arbeiten mit Office 365-Verwendungsberichte in Microsoft Graph die Unterthemen

FEATURE	BESCHREIBUNG	VERFÜGBAR UNTER	WEITERE INFORMATIONEN
<b>Benutzerdefinierte Berichte mit Berichtsdiensten</b>	<p>Programmgesteuertes Erstellen von Berichten aus der verfügbaren Exchange Online PowerShell berichterstellungs-Cmdlets mithilfe von REST/ODATA2 Abfrage filtern.</p> <p><b>Hinweis:</b> viele der ursprünglichen Exchange Online PowerShell reporting Cmdlets verworfen und durch ähnliche Berichte in Microsoft Graph ersetzt wurden. Weitere Informationen finden Sie unter <a href="#">Berichterstellungs-Cmdlets in Exchange Online</a>.</p>	<a href="https://reports.office365.com/ecp/reportingwebservice/reporting.svc">https://reports.office365.com/ecp/reportingwebservice/reporting.svc</a>	<a href="#">Webdienste für die Berichterstellung für Office 365</a>
<b>Nachrichtenablaufverfolgung</b>	<p>Folgt e-Mail-Nachrichten aus, wie sie über die Exchange Online-Organisation unterwegs sind. Sie können festlegen, ob eine e-Mail-Nachricht empfangen, abgelehnt, zurückgestellt oder vom Dienst übermittelt wurde. Außerdem wird gezeigt, welche Aktionen für die Nachricht ausgeführt wurden, bevor sie den letzten Status erreicht. Mit diesen Informationen können Sie in effizienter Weise Fragen der Benutzer beantworten, Probleme mit dem Nachrichtenfluss behandeln und Richtlinienänderungen überprüfen und müssen seltener den technischen Support um Unterstützung bitten.</p>	<p>Im Office 365 Administrationscenter unter <a href="https://portal.office.com/adminportal/home">https://portal.office.com/adminportal/home</a>, klicken Sie auf Admin Center &gt; Exchange. In der neuen Exchange Admin Center-Seite, die geöffnet wird, wechseln Sie zu Nachrichtenfluss &gt; Nachrichtenablaufverfolgung .</p>	<a href="#">Verfolgen einer E-Mail</a> Informationen zur Verwendung der Nachrichtenablaufverfolgung und anderen Tools zur Problembehandlung finden Sie in dem Video unter <a href="#">Suchen und Beheben von Problemen mit der E-Mail-Zustellung als Office 365 Business-Administrator</a> .
<b>Überwachungsprotokollierung</b>	<p>Verfolgt bestimmte Änderungen von Administratoren Ihrer Exchange Online-Organisation. Dank dieser Berichte können Sie gesetzliche Bestimmungen einhalten und Daten, die für Rechtsstreitigkeiten erforderlich sind, aufzubewahren.</p>	<p>Im Office 365 Administrationscenter unter <a href="https://portal.office.com/adminportal/home">https://portal.office.com/adminportal/home</a>, klicken Sie auf Admin Center &gt; Exchange Online Protection. In der neuen Exchange Admin Center-Seite, die geöffnet wird, wechseln Sie zu Verwaltung der Richtlinientreue &gt; Überwachung.</p>	<a href="#">Exchange-Überwachungsberichte</a>

## Datenverfügbarkeit und Latenz bei der Berichterstellung und Nachrichtenablaufverfolgung

In der folgenden Tabelle wird beschrieben, wann und wie lange Daten der Exchange Online-Berichterstellung und -Nachrichtenablaufverfolgung verfügbar sind.

BERICHTTYP	DATEN VERFÜGBAR FÜR (RÜCKWIRKUNGSFRIST)	LATENZ
Zusammenfassungsberichte für Postfächer	60 Tage	Aggregation der Nachrichtendaten ist innerhalb von 24 bis 48 Stunden weitgehend abgeschlossen. Kleinere inkrementelle, aggregierte Änderungen können bis zu 5 Tage lang auftreten.
Zusammenfassungsberichte zum E-Mail-Schutz	90 Tage	Die Aggregation von Nachrichtendaten ist meistens innerhalb von 24 bis 48 Stunden abgeschlossen. Kleinere inkrementelle, aggregierte Änderungen können bis zu 5 Tage lang auftreten.
Detailberichte zum E-Mail-Schutz	90 Tage	Bei Detaildaten, die weniger als 7 Tage alt sind, sollten Daten innerhalb von 24 Stunden erscheinen, sind aber möglicherweise erst 48 Stunden später abgeschlossen. Einige kleinere schrittweise Änderungen können bis zu 5 Tagen dauern. Zum Anzeigen von Detailberichten für Nachrichten, die älter als 7 Tage sind, kann es einige Stunden dauern, bis die Ergebnisse der Nachrichtenablaufverfolgung ausgegeben werden.
Daten der Nachrichtenablaufverfolgung	90 Tage	Wenn Sie eine Nachrichtenverfolgung für Nachrichten starten, die weniger als 7 Tage alt sind, sollten die Nachrichten innerhalb von 5-30 Minuten erscheinen. Wenn Sie eine Ablaufverfolgung für Nachrichten ausführen, die älter als 7 Tage sind, kann es einige Stunden dauern, bis Ergebnisse ausgegeben werden.

#### NOTE

Datenverfügbarkeit und Latenz sind gleich, unabhängig davon, ob Sie die Daten über das Office 365 Admin Center oder über Remote-PowerShell abrufen.

# Verwenden von Berichten zum E-Mail-Schutz in Office 365, um Daten über Schadsoftware, Spam und Regelerkennung anzuzeigen

18.12.2018 • 3 minutes to read

Wenn Sie ein Administrator für Exchange Online oder Exchange Online Protection (EOP) sind, vorhanden ist die Wahrscheinlichkeit, wie viel Spam überwachen sollen, und Schadsoftware erkannt wird, oder wie oft werden Ihre e-Mail-Flussregeln Transportregeln, die Abkürzung abgeglichen wird. Mit der interaktiven e-Mail-schutzberichte in der Office 365-Sicherheit und Compliance Center können Sie schnell einen Bericht zu visual Zusammenfassungsdaten erhalten möchten, und aufgliedern Details zu einzelnen Meldungen für bis 90 Tage zurück zum.

## Berichte stehen im Compliance Center & Sicherheit

Wenn Sie e-Mail-schutzberichte in der Exchange-Verwaltungskonsole anzeigen wurden, haben sie wurde aktualisiert, verbessert und zur Sicherheit & Compliance Center verschoben.

Um die Sicherheit und Compliance Center erhalten möchten, besuchen Sie <https://protection.office.com>, und melden Sie sich mit Ihrem Konto arbeiten oder Schule.

### NOTE

Sie müssen ein globaler Office 365-Administrator sein oder geeignet, verfügen über Berechtigungen, um die Sicherheit und Compliance Center verwenden. Weitere Informationen finden Sie unter [Berechtigungen in der Office 365-Sicherheit und Compliance Center](#).

## Übersicht über die Berichterstellung

Die folgende Tabelle beschreibt die Typen von Berichten, die verfügbar sind, wie Sie diese finden und, wo Sie weitere Informationen finden.

ART DER INFORMATION	NAVIGATION	ERHALTEN SIE WEITERE INFOS
<b>Threat Management dashboard</b> (Dies wird auch als das <b>Dashboard Sicherheit</b> und das <b>Dashboard Bedrohungsanalyse</b> bezeichnet). Erkannte Bedrohung, Malwaretrends, zielgerichteten Hauptbenutzer, Details zu gesendete und empfangene e-Mail-Nachrichten und mehr.	Wechseln Sie in die Sicherheit und Compliance Center zu <b>Threat Management</b> > <b>Dashboard</b> .	<a href="#">Übersicht über die Sicherheit-dashboard</a>
<b>Erweiterte Berichte zur e-Mail-Sicherheit und Schutz vor Angriffen</b> E-Mail-Sicherheit und Bedrohung schutzberichte (einschließlich Schadsoftware, Spam und Phishing und spoofing Berichte).	Wechseln Sie in die Sicherheit und Compliance Center auf <b>Berichte</b> > <b>Dashboard</b> .	<a href="#">Anzeigen von Berichten für Office 365 erweiterte Threat Protection E-Mail-Sicherheitsberichte anzeigen im Compliance Center &amp; Sicherheit</a>

ART DER INFORMATION	NAVIGATION	ERHALTEN SIE WEITERE INFOS
<p><b>Nachrichtenfluss</b> Informationen zum Senden und Empfangen von e-Mail-Nachrichten, letzten, häufigste Absender und Empfänger, e-Mail-Weiterleitung Berichte und vieles mehr.</p>	<p>Wechseln Sie in die Sicherheit und Compliance Center zu <b>Nachrichtenfluss &gt; Dashboard.</b></p>	<p><a href="#">Einblicke in die e-Mail-Fluss im Compliance Center &amp; Sicherheit in Office 365</a></p>

## Verwandte Themen

[Berichte und Einblicke in die Office 365-Sicherheit und Compliance Center](#)

# Anpassen und Einrichten, dass E-Mail-Schutzberichte in Office 365 automatisch an Ihren Posteingang gesendet werden

18.12.2018 • 2 minutes to read

Als Administrator Exchange Online oder Exchange Online Protection (EOP) möchten Sie wahrscheinlich auch Ihrer Organisation Mail Blick Ablauf, wie viel Spam und Malware wird gefunden wird, oder wie oft Ihrer Regeln und Richtlinien abgeglichen werden werden. Mithilfe von e-Mail-schutzberichte, erhalten Sie eine schnelle Zusammenfassung von Nachrichten, die Office 365 zugestellt oder abgelehnt hat basierend auf Spam oder Schadsoftware Merkmale, Regeln oder Data Loss Prevention (DLP) Richtlinien.

Sie können entweder Zeitplan e-Mail-schutzberichte automatisch an Ihren Posteingang gesendet werden, oder können sie jederzeit im Compliance Center & Sicherheit in Office 365.

Um die ersten Schritte beim Anpassen und Herunterladen von Berichten, finden Sie in den folgenden Ressourcen:

- [Einrichten von, und Laden Sie einen benutzerdefinierten Bericht im Compliance Center & Sicherheit](#)
- [Laden Sie vorhandene Berichte im Compliance Center & Sicherheit](#)
- [Verwalten Sie Zeitpläne für mehrere Berichte im Compliance Center & Sicherheit](#)

## Verwandte Themen

[Smart-Berichten und Einblicke in die im Compliance Center & Sicherheit](#)

[E-Mail-Sicherheitsberichte anzeigen im Compliance Center & Sicherheit](#)

[Einblicke in die e-Mail-Fluss im Compliance Center & Sicherheit in Office 365](#)

# Wo befindet sich in Office 365 Übermittlungsberichte?

18.12.2018 • 2 minutes to read

Übermittlungsberichte wurde ein Feature in Office 365, die Benutzern und Administratoren zum Erkennen und Anzeigen von Übermittlungsinformationen zu Nachrichten zulässig.

In Office 365 Übermittlungsberichte für Administratoren wurde ersetzt durch nachrichtenablaufverfolgung. Weitere Informationen finden Sie unter folgenden Themen:

- [Verwenden von Nachrichtenablaufverfolgung](#)
- [Verfolgen einer E-Mail](#)

Derzeit ist keine direkte Ersatz für Übermittlungsberichte für Benutzer, damit die Zustellung Bericht Links in Outlook und Outlook im Web nicht an einer beliebigen Stelle wechseln.

## Hinweise

- Übermittlungsberichte für Benutzer und Administratoren ist weiterhin verfügbar in lokalen Exchange-Umgebungen. Weitere Informationen finden Sie unter [Nachverfolgen von Nachrichten mit Übermittlungsberichten](#).
- Lesebestätigungen Übermittlung Benachrichtigungen werden nicht im Zusammenhang mit der Übermittlungsberichte und noch in Office 365 verfügbar sind. Weitere Informationen finden Sie unter [Hinzufügen und Lesen Einnahmen und Übermittlung Benachrichtigungen Anforderung](#).

# Verfolgen einer E-Mail

18.12.2018 • 2 minutes to read

Manchmal geht eine E-Mail-Nachricht während der Übermittlung verloren, oder Ihre Versendung dauert etwas länger, sodass Ihre Benutzer sich fragen, was passiert sein könnte. Als Administrator können Sie mithilfe des Features zur Nachrichtenablaufverfolgung Nachrichten beim Durchgang durch Ihren Exchange Online- oder Exchange Online Protection-Dienst verfolgen. Mit der Nachrichtenablaufverfolgung können Sie ermitteln, ob eine bestimmte E-Mail vom Dienst empfangen, abgelehnt, zurückgestellt oder zugestellt wurde. Außerdem werden die Ereignisse der Nachricht gezeigt, bevor diese ihren finalen Status erreicht hat. Mithilfe ausführlicher Informationen zu einer bestimmten Nachricht können Sie in effizienter Weise Fragen der Benutzer beantworten, Probleme mit dem Nachrichtenfluss behandeln und Richtlinienänderungen überprüfen, und Sie müssen seltener den technischen Support um Unterstützung bitten.

## TIP

Verwenden Sie zur Behandlung allgemeiner Probleme und Trends die in der Office 365-Verwaltungskonsole verfügbaren Berichte oder die Excel-Arbeitsmappe für Berichte. Verwenden Sie bei speziellen Besonderheiten, bei denen Details zu einer Nachricht erforderlich sind, das Tool für die Nachrichtenablaufverfolgung.

In [Ausführen einer Nachrichtenablaufverfolgung und Anzeigen der Ergebnisse](#) wird das Ausführen einer Nachrichtenablaufverfolgung zur Reduzierung Ihrer Suchkriterien beschrieben. Außerdem wird erläutert, wie die Ergebnisse der Nachrichtenablaufverfolgung sowie Details zu einer bestimmten Nachricht angezeigt werden.

Das Thema [Häufig gestellte Fragen zur Nachrichtenablaufverfolgung](#) geht auf häufig gestellte Fragen zu Nachrichten ein. Es wird erläutert, wie mithilfe der Nachrichtenablaufverfolgung die besten Antworten darauf gefunden werden können:

# Ausführen einer nachrichtenablaufverfolgung und Anzeigen der Ergebnisse in der Exchange-Verwaltungskonsole

18.12.2018 • 35 minutes to read

## NOTE

Nachricht Trace ist in der Office 365-Sicherheit und Compliance Center verfügbar. Weitere Informationen finden Sie unter [Message Trace in die Office 365-Sicherheit und Compliance Center](#).

Als Administrator können Sie herausfinden, wo sich eine e-Mail-Nachricht befindet durch Ausführen einer nachrichtenablaufverfolgung in der Exchange-Verwaltungskonsole (EAC) werden soll. Nach der Ausführung der nachrichtenablaufverfolgung, können Sie die Ergebnisse in einer Liste anzeigen und zeigen Sie die Details zu einer bestimmten Nachricht. Daten der nachrichtenablaufverfolgung werden für die letzten 90 Tage verfügbar. Wenn eine Nachricht älter als 7 Tage ist, können Sie die Ergebnisse nur in einer herunterladbaren anzeigen. CSV-Datei.

Ein Video zur Verwendung der Nachrichtenablaufverfolgung und anderer Tools zur Behandlung von Problemen mit dem Nachrichtenfluss finden Sie unter [Suchen und Beheben von Problemen bei der E-Mail-Übermittlung für Office 365 for Business-Administratoren](#).

## Was sollten Sie wissen, bevor Sie beginnen?

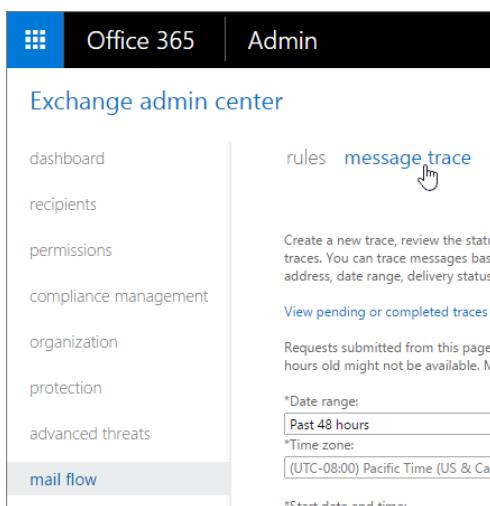
- Informationen zu, wenn Daten verfügbar sind und wie lange finden Sie im Abschnitt [Berichte und Nachricht datenverfügbarkeit und Latenz in Berichterstellung und nachrichtenablaufverfolgung in Exchange Online Protection](#).
- Zum Suchen und öffnen Sie die Exchange-Verwaltungskonsole, finden Sie unter [Exchange Admin center in Exchange Online](#).
- Bevor Sie diese Verfahren ausführen können, müssen Ihnen die entsprechenden Berechtigungen zugewiesen werden. Informationen zu den von Ihnen benötigten Berechtigungen finden Sie unter "Nachrichtenablaufverfolgung" im Thema [Featureberechtigungen in Exchange Online](#).
- Informationen zu Tastenkombinationen, die für die Verfahren in diesem Thema gelten, finden Sie unter [Tastenkombinationen für die Exchange-Verwaltungskonsole](#).

## TIP

Liegt ein Problem vor? Erhalten Sie in der Exchange-Foren. Besuchen Sie die Foren unter [Exchange Online](#) oder [Exchange Online Protection](#). Wenn Sie ein Office 365 für Unternehmen Admin sind, können Sie für [Office 365 für Unternehmen Support wenden](#).

## Ausführen einer Nachrichtenablaufverfolgung

1. Navigieren Sie in der Exchange-Verwaltungskonsole zu **Nachrichtenfluss > nachrichtenablaufverfolgung**.



2. Je nachdem, was Sie für suchen können Sie Werte in den folgenden Feldern eingeben. Keines der diese Felder sind erforderlich für Nachrichten, die weniger als 7 Tage alt sind. Sie können einfach klicken Sie auf **Durchsuchen**, um alle Daten der nachrichtenablaufverfolgung über das standardmäßige Zeitraum, abzurufen, das den letzten 48 Stunden ist.
3. **Datumsbereich:** Wählen Sie mithilfe der Dropdown-Liste Suchen nach Nachrichten innerhalb der letzten 24 Stunden, 48 Stunden oder 7 Tage gesendet oder empfangen. Sie können auch einen benutzerdefinierten Zeitrahmen auswählen, der einen beliebigen Bereich innerhalb der letzten 90 Tage enthält. Für die benutzerdefinierte Suche können Sie auch die Zeitzone in koordinierter Weltzeit (UTC) ändern.
4. **Zustellungsstatus:** mithilfe der Dropdown-Liste Wählen Sie den Status der Nachricht, die Sie Informationen anzeigen möchten. Übernehmen Sie den Standardwert **Alle** alle Statusarten decken. Andere Werte sind möglich:
  - **Übermittelte:** die Nachricht wurde erfolgreich an das vorgesehene Ziel übermittelt.
  - **Fehler:** die Nachricht wurde nicht übermittelt. Es wurde versucht und ist fehlgeschlagen oder aufgrund von Aktionen, die vom Filter-Dienst nicht übermittelt wurde. Wenn beispielsweise die Nachricht Schadsoftware erkannt wurde.

- **Ausstehende**: Zustellung der Nachricht wird versucht oder wird erneut versucht.
- **Erweiterter**: die Nachricht wurde an eine Verteilerliste gesendet und wurde erweitert, damit die Mitglieder der Liste einzeln angezeigt werden können.
- **Unbekannt**: Zustellungsstatus der Nachricht ist zu diesem Zeitpunkt nicht bekannt. Wenn die Ergebnisse der Abfrage aufgeführt sind, werden die Zustellung Detailfelder keine Informationen enthalten.

```
<span data-ttu-id="1b388-141"><sup>\*</sup>Wenn Sie nach Nachrichten, die älter als 7 Tage sind suchen, auswählen nicht Sie **weder ausstehend** noch  
**unbekannt**.</span><span class="sxs-lookup"><span data-stu-id="1b388-141"><sup>\*</sup>If you're searching for messages that are older than 7 days, you can't  
select **Pending** or **Unknown**.</span></span>
```

3. **Nachrichten-ID**: Dies ist die Internetnachrichten-ID (auch bekannt als die Client-ID) gefunden in der Kopfzeile der Nachricht in das **Nachrichten-ID**: Kopfzeilenfeld. Benutzer können mit diesen Informationen Sie angeben, um bestimmte Nachrichten untersuchen.

```
<span data-ttu-id="1b388-p111">Das Formular dieser-ID variiert je nach der sendenden e-Mail-System. Im folgenden ist ein Beispiel:  
'<08f1e0f6806a47b4ac103961109ae6ef@server.domain>.</span><span class="sxs-lookup"><span data-stu-id="1b388-p111">The form of this ID varies depending on the  
sending mail system. The following is an example: '<08f1e0f6806a47b4ac103961109ae6ef@server.domain>.</span></span>
```

<span data-ttu-id="1b388-p112">Diese ID muss eindeutig sein; nicht alle sendenden e-Mail-Systemen Verhalten sich jedoch die gleiche Weise aus. Daher besteht die Möglichkeit, dass Sie Ergebnisse für mehrere Nachrichten angezeigt werden, wenn bei einer einzelnen Nachrichten-ID Abfragen</span><span class="sxs-lookup"><span data-stu-id="1b388-p112">This ID should be unique; however, not all sending mail systems behave the same way. As a result, there's a possibility that you may  
get results for multiple messages when querying upon a single Message ID.</span></span>

<span data-ttu-id="1b388-p113">\*\*Hinweis\*\*: Achten Sie darauf, dass Sie die vollständige Nachrichten-ID-Zeichenfolge enthalten. Hierzu gehören möglicherweise spitze Klammern (<>).</span><span class="sxs-lookup"><span data-stu-id="1b388-p113">\*\*Note\*\*: Be sure to include the full Message ID string. This may include angle brackets (<>).</span></span>

4. **Absender**: Sie können die Suche nach bestimmten Absendern einschränken, indem Sie die Schaltfläche neben dem Feld **Absender Absender hinzufügen**. Wählen Sie in der daraufhin angezeigten Dialogfeld einen oder mehrere Absender in Ihrem Unternehmen aus der Liste der Personenauswahl, und klicken Sie dann auf **Hinzufügen**. Um Absender hinzuzufügen, die nicht in der Liste sind, geben Sie ihre e-Mail-Adressen, und klicken Sie auf **Namen überprüfen**. In diesem Feld werden Platzhalter für e-Mail-Adressen im Format unterstützt: \*@contoso.com. Wenn Sie einen Platzhalter angeben, können nicht andere Adressen verwendet werden. Wenn Sie mit Ihrer Auswahl fertig sind, klicken Sie auf **OK**.
  5. **Empfänger**: Sie können die Suche für bestimmte Empfänger einschränken, indem Sie auf die Schaltfläche **Hinzufügen Empfänger** neben dem Feld **Empfänger**. Wählen Sie in der daraufhin angezeigten Dialogfeld einen oder mehrere Empfänger aus Ihrem Unternehmen aus der Liste der Personenauswahl, und klicken Sie dann auf **Hinzufügen**. Um Empfänger hinzuzufügen, die nicht in der Liste sind, geben Sie ihre e-Mail-Adressen, und klicken Sie auf **Namen überprüfen**. In diesem Feld werden Platzhalter für e-Mail-Adressen im Format unterstützt: \*@contoso.com. Wenn Sie einen Platzhalter angeben, können nicht andere Adressen verwendet werden. Wenn Sie mit Ihrer Auswahl fertig sind, klicken Sie auf **OK**.
  6. Wenn Sie nach Nachrichten, die älter als 7 Tage sind suchen, konfigurieren Sie die folgenden Einstellungen: (andernfalls können Sie in diesem Schritt überspringen):
  7. **Include-Nachricht Ereignisse und Routingdetails mit Bericht**: Es wird empfohlen, wenn dieses Kontrollkästchen nur, wenn Sie für eine kleine Anzahl von Nachrichten suchen. Andernfalls werden die Ergebnisse zurückzugebenden länger dauern.
  8. **Richtung**: lassen Sie die Standardeinstellung **Alle** oder wählen Sie **eingehende** Nachrichten, die für Ihre Organisation oder **ausgehende** Nachrichten, die von Ihrer Organisation gesendet gesendet.
  9. **Ursprüngliche Client-IP-Adresse**: Geben Sie die IP-Adresse des Client des Absenders an.
  10. **Berichtstitel**: Geben Sie den eindeutigen Bezeichner für diesen Bericht. Dies wird auch als die Betreffzeile für die e-Mail-Benachrichtigung verwendet werden. Der Standardwert ist "Message Trace Bericht <Tag der Woche>, <aktuelles Datum> <aktuelle Uhrzeit>". Beispielsweise "nachrichtenablaufverfolgungsberichts Donnerstag, 17 Oktober 2018 7:21:09 h".
  11. **Benachrichtigung e-Mail-Adresse**: Geben Sie die e-Mail-Adresse, die Sie möchten eine Benachrichtigung, wenn die nachrichtenablaufverfolgung abgeschlossen ist. Diese Adresse muss innerhalb der Liste der akzeptierten Domänen befinden.
  12. Klicken Sie auf **Suche**: die nachrichtenablaufverfolgung ausführen. Sie werden gewarnt, wenn Sie den Schwellenwert für die Höhe der Spuren abgelaufen sind, die Sie in einem 24-Stunden-Zeitraum ausführen zulässig sind.
- Setzen Sie nach der Ausführung der nachrichtenablaufverfolgung Sie mit einem der nächsten Abschnitte, um zu erfahren, wie Sie das Ergebnis anzeigen.
- Hinweis**: um eine andere Nachricht zu suchen, können Sie klicken Sie auf die Schaltfläche **Löschen** und dann neue Suchkriterien eingeben.

## Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten weniger als 7 Tage

Nachdem Sie in der Exchange-Verwaltungskonsole eine nachrichtenablaufverfolgung ausführen, werden die Ergebnisse sortiert nach Datum, mit der neuesten Nachrichten an erster Stelle steht aufgelistet. Sie können auf eines der aufgelisteten Felder sortieren, indem Sie auf ihre Kopfzeilen. Klicken Sie auf eine Spaltenüberschrift ein zweites Mal wird die Sortierreihenfolge umzukehren. Bei der Anzeige der Ergebnisse der nachrichtenablaufverfolgung werden die folgenden Informationen zu jeder Nachricht bereitgestellt:

- **Datum**: Datum und Uhrzeit, an dem die Nachricht vom Dienst mithilfe der konfigurierten UTC-Zone empfangen wurde.
- **Absender**: die e-Mail-Adresse des Absenders im Format `alias@domain`.
- **Empfänger**: die e-Mail-Adresse des Empfängers oder Empfänger. Für Nachrichten, die an mehrere Empfänger gesendet ist eine Zeile pro Empfänger. Wenn der Empfänger eine Verteilerliste handelt, die Verteilerliste werden der ersten Empfänger, und jedes Mitglied der Verteilerliste wird dann in einer separaten Zeile enthalten sein, so, dass Sie den Status für alle Empfänger überprüfen können.
- **Betreff**: die Betreffzeile der Nachricht. Falls erforderlich, wird dies auf die ersten 256 Zeichen gekürzt.
- **Status**: Dieses Feld gibt an, ob die Nachricht an den Empfänger oder das vorgesehene Ziel, **könnte nicht** an den Empfänger übermittelt werden **geliefert** wurde (entweder, da es konnte nicht ihr Ziel erreicht oder da sie gefiltert wurde), wird **Ausstehende** Delivery (es ist entweder gerade Zustellung oder die Übermittlung zurückgestellt wurde jedoch erneut versucht wird), wurde **Erweiterter** (es wurde keine Übermittlung, da die Nachricht an eine Verteilerliste (DL)

gesendet wurde, die auf erweitert wurde die Empfänger der Verteilerliste) oder hat einen Status **None**, die (es ist kein Status der Übermittlung der Nachricht an den Empfänger, da die Nachricht abgelehnt oder an einen anderen Empfänger umgeleitet wurde).

#### NOTE

Die Nachrichtenablaufverfolgung kann maximal 500 Einträge anzeigen. Standardmäßig zeigt die Benutzeroberfläche 50 Einträge pro Seite an, und Sie können durch die Seiten navigieren. Sie können auch die Einträge auf jeder Seite bis auf 500 erhöhen.

### Anzeigen von Details zu einer bestimmten Nachricht weniger als 7 Tage

Nach dem Überprüfen der Liste von Elementen, die von der Nachrichtenablaufverfolgung in das EAC zurückgegeben wurden, können Sie auf eine einzelne Nachricht doppelklicken, um die folgenden zusätzlichen Details zu der Nachricht anzuzeigen:

- **Nachrichtengröße:** die Größe der Nachricht, einschließlich Anlagen, in Kilobyte (KB), oder wenn die Größe der Nachricht größer ist als 999 KB in Megabyte (MB).
- **Nachrichten-ID:** Dies ist die Internetnachrichten-ID (auch bekannt als die Client-ID) gefunden in der Kopfzeile der Nachricht mit der "Nachrichten-ID:" token. Die Form dieses variiert je nach der sendenden e-Mail-System. Im folgenden ist ein Beispiel: <08f1e0f6806a47b4ac103961109ae6ef@contoso.com> . Diese ID sollte eindeutig sein. Dies hängt allerdings von dem sendenden E-Mail-System für die Generierung ab, und nicht alle sendenden E-Mail-Systeme verhalten sich gleich. Es besteht folglich die Möglichkeit, dass Sie Ergebnisse für mehrere Nachrichten erhalten, wenn Sie eine einzelne Nachrichten-ID abfragen.
- Diese Informationen werden ausgegeben, damit Ablaufverfolgungseinträge und die fraglichen Nachrichten miteinander in Verbindung gebracht werden können.
- **Um-IP:** die IP-Adressen, dem der Dienst hat versucht, die Nachricht zu übermitteln. Wenn mehrere Empfänger vorhanden sind, werden diese angezeigt. Für eingehende Nachrichten zu Exchange Online gesendet beträgt dieser Wert leer.
- **Von IP-Adresse:** die IP-Adresse des Computers, der die Nachricht gesendet hat. Für ausgehende Nachrichten von Exchange Online beträgt dieser Wert leer.

Im Bereich "Ereignisse" liefern die folgenden Felder Informationen zu den Ereignissen, die für die Nachricht aufgetreten sind, während diese sich in der Messagingpipeline befand:

- **Datum:** Datum und Uhrzeit, die das Ereignis aufgetreten ist.
- **Ereignis:** Dieses Feld informiert Sie über Änderungen bei der beispielsweise, wenn die Nachricht vom Dienst empfangen wurde, wenn er übermittelt wurde oder konnte nicht an den gewünschten Empfänger übermittelt werden, usw., kurz. Es folgen Beispiele für Ereignisse, die enthalten sein können:
  - **Empfangen:** die Nachricht wurde vom Dienst empfangen.
  - **Senden:** die Nachricht wurde vom Dienst gesendet.
  - **Fehler:** die Nachricht konnte nicht zugestellt werden.
  - **Übermitteln:** die Nachricht wurde an ein Postfach zugestellt.
  - **Erweitern:** die Nachricht wurde an eine Verteilergruppe, die erweitert wurde gesendet.
  - **Übertragen:** Empfänger wurden aufgrund von inhaltskonvertierung, empfängerbeschränkungen oder Agents in eine verzweigte Nachricht verschoben.
  - **DEFER:** die Nachrichtübermittlung wurde verschoben und möglicherweise werden erneut zu einem späteren Zeitpunkt.
  - **Gelöst:** die Nachricht wurde umgeleitet, um eine neue Adresse des Empfängers basierend auf einer Active Directory zu suchen. In diesem Fall wird die ursprüngliche Empfängeradresse in einer separaten Zeile in der Nachricht Trace zusammen mit den Status der Übermittlung der Nachricht aufgeführt.

#### TIP

Es können weitere Ereignisse auftreten. Weitere Informationen hierzu finden Sie im Abschnitt "Ereignistypen im Nachrichtenverfolgungsprotokoll" in [Message Tracking](#).

- **Aktion:** Dieses Feld zeigt der ausgeführte Aktion aus, wenn die Nachricht aufgrund einer Malware oder Spam-Erkennung oder ein Abgleich gefiltert wurde. Beispielsweise können sie Sie darauf hingewiesen, wenn die Nachricht gelöscht wurde oder wenn es unter Quarantäne gestellt wurde.
- **Detail:** Dieses Feld enthält ausführliche Informationen, die eingeführten näher ausgeführt, auf was passiert ist. Beispielsweise kann es darüber informieren Sie welche bestimmten e-Mail-Fluss (auch bekannt als eine Transportregel) Regel entsprach und wo befindet sich die Nachricht als Ergebnis entsprechen. Es kann auch mitteilen, welche spezifischen Malware in welche bestimmte Anlage erkannt wurde, oder warum eine Nachricht als Spam erkannt wurde. Wenn die Nachricht erfolgreich übermittelt wurde, kann es Ihnen die IP-Adresse sagen, die sie übermittelt wurde.

### Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten mehr als 7 Tage

Wenn Sie eine nachrichtenablaufverfolgung für Elemente ausführen, die älter als 7 Tage sind beim Klicken auf **Suche** eine Meldung sollte angezeigt werden Sie darüber informiert, dass die Nachricht erfolgreich übermittelt wurde, und, die eine e-Mail-Benachrichtigung an den angegebenen Email gesendet beheben, wann die Ablaufverfolgung wurde abgeschlossen. (Falls die nachrichtenablaufverfolgung verarbeitet wird und Daten, die die Suchkriterien entsprechen erfolgreich abgerufen werden, muss diese Benachrichtigung Informationen zu den Ablauf- und einen Link zu den herunterladbaren enthalten. CSV-Datei. Wenn keine Daten gefunden wurde, die mit die Suchkriterien entsprechen, die Sie angegeben haben, werden Sie aufgefordert werden, senden eine neue Anforderung mit geänderten Kriterien in übereinstimmenden Reihenfolge um gültige Ergebnisse zu erhalten.)

In der Exchange-Verwaltungskonsole, Sie können klicken **ausstehende oder abgeschlossene Spuren anzeigen**, um eine Liste der Ablaufverfolgungen anzusehen, die für Elemente ausgeführt wurden, die älter als 7 Tage. In der Benutzeroberfläche des resultierenden wird die Liste der Spuren sortiert basierend auf Datum und Uhrzeit, die sie gesendet wurden, mit den neuesten Übermittlungen kann wie folgt aussehen. Neben dem Berichtstitel, das Datum und Uhrzeit, zu der Trace übermittelt wurde und die Anzahl der Nachrichten in den Bericht, sind die folgenden Statuswerte aufgeführt:

- **Nicht gestartet:** die Ablaufverfolgung wurde übermittelt, aber nicht noch ausgeführt wird. Zu diesem Zeitpunkt haben Sie die Möglichkeit, die Ablaufverfolgung abzubrechen.

- **Abgebrochen:** die Ablaufverfolgung wurde übermittelt, aber abgebrochen.
- **In Arbeit:** die Ablaufverfolgung wird ausgeführt, und Sie nicht den Trace abbrechen oder die Ergebnisse herunterladen.
- **Abgeschlossen:** Trace abgeschlossen ist und Sie können zum Abrufen der Ergebnisse in **diesem Bericht herunterladen** Klicken ein. CSV-Datei. Beachten Sie, dass bei der Ergebnisse der nachrichtenablaufverfolgung 5000 Nachrichten für einen Zusammenfassungsbericht überschreiten, es auf den ersten 5000 Nachrichten abgeschnitten wird. Wenn Ihre Ergebnisse der nachrichtenablaufverfolgung 3000 Nachrichten für einen detaillierten Bericht überschreiten, werden die auf der ersten 3000 Nachrichten Zahl gekürzt. Wenn nicht alle Ergebnisse, die Sie benötigen angezeigt werden, empfohlen, dass Break skalieren die Suche in mehreren Abfragen.

Wenn Sie eine bestimmte Nachrichtenablaufverfolgung auswählen, werden im rechten Bereich zusätzliche Informationen angezeigt. Abhängig von den angegebenen Suchkriterien, können hierzu Details zählen wie der Zeitraum, für den die Ablaufverfolgung ausgeführt wurde, und der Absender und die beabsichtigten Empfänger der Nachricht.

#### NOTE

Nachrichtenablaufverfolgungen, die Daten enthalten, die älter als 7 Tage sind, werden im EAC automatisch nach 10 Tagen gelöscht. Sie können nicht manuell gelöscht werden.

#### Zeigen Sie Details zu einer bestimmten Nachricht an mehr als 7 Tage

Wenn Sie herunterladen und ein nachrichtenablaufverfolgungsberichts von **ausstehende oder abgeschlossene Spuren anzeigen**, in der Exchange-Verwaltungskonsole oder aus einer e-Mail-Benachrichtigung anzeigen hängen seinen Inhalt, ob die **Nachricht Ereignisse und Routingdetails mit Bericht enthalten** ausgewählt haben Option.

#### IMPORTANT

Damit Sie den Nachrichtenablaufverfolgungsbericht anzeigen können, muss Ihrer Rollengruppe die RABC-Rolle "Empfänger (nur Anzeige)" zugewiesen sein. Standardmäßig ist diese Rolle folgenden Rollengruppen zugewiesen: Verwaltung der Richtlinientreue, Helpdesk, Verwaltung von Nachrichtenschutz, Organisationsverwaltung, Organisationsverwaltung (nur Leserechte).

#### Anzeigen eines Nachrichtenablaufverfolgungsberichts ohne Routingdetails

Wenn Sie keine Routingdetails beim Ausführen der Nachrichtenablaufverfolgung eingeschlossen haben, werden die folgenden Informationen in die CSV-Datei aufgenommen, die in einer Anwendung wie Microsoft Excel geöffnet werden kann:

- **Origin\_timestamp:** Datum und Uhrzeit, an dem die Nachricht vom Dienst mithilfe der konfigurierten UTC-Zeitzone empfangen wurde.
  - **Sender\_address:** die e-Mail-Adresse des Absenders im Formular *Alias@Domäne*.
  - **Recipient\_status:** der Status der Zustellung der Nachricht an den Empfänger. Wenn die Nachricht an mehrere Empfänger gesendet wurde, zeigt es alle Empfänger und den entsprechenden Status für jedes im Format: <e-Mail-Adresse>##<Status>. Beispiel: Status:
    - **##Receive, senden:** bedeutet, dass die Nachricht vom Dienst empfangen und an das vorgesehene Ziel gesendet wurde.
    - **##Receive, ein Fehler auftritt:** Mittel, die die Nachricht wurde vom Dienst empfangen, aber konnte nicht an das vorgesehene Ziel übermittelt werden.
    - **##Receive, bieten:** bedeutet, dass die Nachricht vom Dienst empfangen und an das Postfach des Empfängers übermittelt wurde.
  - **Betreff der Nachricht:** die Betreffzeile der Nachricht. Falls erforderlich, wird dies auf die ersten 256 Zeichen gekürzt.
  - **Total\_bytes:** die Größe der Nachricht, einschließlich Anlagen, in Byte.
  - **Message\_id:** Dies ist die Internetnachrichten-ID (auch bekannt als die Client-ID) gefunden in der Kopfzeile der Nachricht mit der "Nachrichten-ID:" token. Die Form dieses variiert je nach der sendenden e-Mail-System. Im folgenden ist ein Beispiel: <08f1e0f6806a47b4ac103961109ae6ef@Server.Domäne>.
- Diese ID sollte eindeutig sein. Dies hängt allerdings von dem sendenden E-Mail-System für die Generierung ab, und nicht alle sendenden E-Mail-Systeme verhalten sich gleich. Es besteht folglich die Möglichkeit, dass Sie Ergebnisse für mehrere Nachrichten erhalten, wenn Sie eine einzelne Nachrichten-ID abfragen.
- Diese Informationen werden ausgegeben, damit Ablaufverfolgungseinträge und die fraglichen Nachrichten miteinander in Verbindung gebracht werden können.
- **Network\_message\_id:** Dies ist eine eindeutige Nachrichten-ID-Wert, die über Kopien der Nachricht erhalten bleibt, die aufgrund der Erweiterung Verzweigung oder einer Verteilergruppe erstellt werden kann. Ein Beispiel für einen Wert ist 1341ac7b13fb42ab4d4408cf7f55890f.
  - **Original\_client\_ip:** die IP-Adresse des Client des Absenders an.
  - **richtungsabhängigkeit:** Dieses Feld gibt an, ob die Nachricht an (1) eingehend Ihrer Organisation gesendet wurde, oder ob sie ausgehende (2) von Ihrer Organisation gesendet wurde.
  - **Connector\_id:** der Name der Quell- oder Ziel Sendeconnector oder Empfangsconnector. Beispielsweise *ServerName\ConnectorName* oder *ConnectorName*.
  - **delivery\_priority zeigt:** Gibt an, ob die Nachricht mit **hoher, niedriger oder normaler** Priorität gesendet wurde.

#### Anzeigen eines Nachrichtenablaufverfolgungsberichts mit Routingdetails

Wenn Sie Routingdetails beim Ausführen der Nachrichtenablaufverfolgung eingeschlossen haben, werden alle Informationen aus den Nachrichtenablaufverfolgungsprotokollen in die CSV-Datei aufgenommen, die in einer Anwendung wie Microsoft Excel geöffnet werden kann. Einige in diesem Bericht enthaltenen Werte werden im vorangegangenen Abschnitt beschrieben. Andere Werte, die zu Untersuchungszwecken hilfreich sein können, werden im Abschnitt „Felder in den Protokolldateien für die Nachrichtenverfolgung“ im Thema [Message Tracking](#) beschrieben.

#### Das Feld custom\_data

Zusätzlich kann das Feld **custom\_data** Werte enthalten, die dem Filterdienst eigen sind. Das Feld **custom\_data** in einem AGENTINFO-Ereignis wird von einer Reihe verschiedener Agents verwendet, um Details der Nachrichtenverarbeitung des Agents zu protokollieren. Einige der mit dem Nachrichtendatenschutz im Zusammenhang stehenden Agents werden unten beschrieben.

## Spam Filter Agent (S:SFA)

Eine Zeichenfolge, die mit S:SFA beginnt, ist ein Eintrag vom Spam-Filter-Agent, der die folgenden wichtigen Details bereitstellt:

PROTOKOLLINFORMATIONEN	BESCHREIBUNG	
SFV=NSPM	Die Nachricht wurde als "Nicht-Spam" markiert und an die vorgesehenen Empfänger gesendet.	
SFV=SPM	Die Nachricht wurde vom Inhaltsfilter als Spam markiert.	
SFV=BLK	Die Filterung wurde übergangen, und die Nachricht wurde gesperrt, da sie von einem gesperrten Absender stammt.	
SFV=SKS	Die Nachricht wurde als Spam, bevor Sie vom Inhaltsfilter verarbeitet wird markiert. Dazu gehören Nachrichten, in dem die Nachricht eine e-Mail-Flussregel automatisch markieren sie als spam und alle zusätzlichen Filtern nach umgehen abgeglichen.	
SCL-Bewertung = <Anzahl>	Weitere Informationen zu den verschiedenen SCL-Werten und deren Bedeutung finden Sie unter <a href="#">Spam Confidence Levels</a> .	
PCL = <Anzahl>	Der PCL-Wert (Phishing Confidence Level) der Nachricht. Diese Werte können auf die gleiche Weise interpretiert werden wie die in <a href="#">Spam Confidence Levels</a> dokumentierten SCL-Werte.	
DI=SB	Der Absender der Nachricht wurde blockiert.	
DI=SQ	Die Nachricht wurde unter Quarantäne gestellt.	
DI=SD	Die Nachricht wurde gelöscht.	
DI=SJ	Die Nachricht wurde an den Ordner "Junk-E-Mail" des Empfängers gesendet.	
DI=SN	Die Nachricht wurde über den höheren Risk Delivery Pool weitergeleitet. Weitere Informationen finden Sie unter <a href="#">höhere Risk Delivery Pool für ausgehende Nachrichten</a> .	
DI=SO	Die Nachricht wurde durch den normalen Pool für ausgehende Zustellungen geleitet.	
SFS=[a]	SFS=[b]	Dies bedeutet, dass Übereinstimmungen mit den Spam-Regeln gefunden wurden.
IPV=CAL	Die Nachricht wurde durch die Spam-Filter gelassen weil die IP-Adresse in einer IP-Zulassungsliste im Verbindungsfilter angegeben wurde.	
H=[helostring]	Die HELO- oder EHLO-Zeichenfolge des verbundenen E-Mail-Servers.	
PTR = [ReverseDNS]	Der PTR-Eintrag der IP-Adresse des Absenders, auch bekannt als Reverse-DNS-Adresse.	

Wenn eine Nachricht als Spam ausgefiltert wird, könnte ein Beispieleintrag für custom\_data etwa wie folgt aussehen:

```
S:SFA=SUM|SFV=SPM|IPV=CAL|SRV=BULK|SFS=470454002|SFS=349001|SCL=9|SCORE=-1|LIST=0|DI=SN|RD=ftmail.inc.com|H=ftmail.inc.com|CIP=98.129.140.74|SFP=1501|ASF=1|CTRY=US|CLTCTRY=|LANG=en|LAT=287|LAT=260|LAT=18;
```

## Malware Filter Agent (S:AMA)

Eine Zeichenfolge, die mit S:AMA beginnt, ist ein Eintrag vom Antischadsoftware-Agent, der die folgenden wichtigen Details bereitstellt:

PROTOKOLLINFORMATIONEN	BESCHREIBUNG
AMA = Summe V = 1 oder AMA = EV V = 1\	Die Nachricht enthält Schadsoftware. SUM zeigt an, dass die Schadsoftware von beliebigen anderen Modulen hätte erkannt werden können. EV zeigt an, dass die Schadsoftware von einem bestimmten Modul erkannt wurde. Wenn von einem Modul Schadsoftware erkannt wird, werden dadurch die nachfolgenden Aktionen ausgelöst.
Action=r	Die Nachricht wurde ersetzt.
Action=p	Die Nachricht wurde umgangen.
Action=d	Die Nachricht wurde zurückgestellt.

PROTOKOLLINFORMATIONEN	BESCHREIBUNG
Action=s	Die Nachricht wurde gelöscht.
Action=st	Die Nachricht wurde umgangen.
Action=sy	Die Nachricht wurde umgangen.
Action=ni	Die Nachricht wurde abgelehnt.
Action=ne	Die Nachricht wurde abgelehnt.
Action=b	Die Nachricht wurde blockiert.
Name = <Schadsoftware>	Der Name der Schadsoftware, die gefunden wurde.
Datei = <Dateiname>	Der Name der Datei, welche die Schadsoftware enthielt.

Wenn eine Nachricht Schadsoftware enthält, könnte ein Beispieleintrag für custom\_data etwa wie folgt aussehen:

```
S:AMA=SUM|v=1|action=b|error=|atch=1;S:AMA=EV|engine=M|v=1|sig=1.155.974.0|name=DOS/Test_File|file=filename;S:AMA=EV|engine=A|v=1|sig=201307282038|name=Test_File|file=filename
```

#### Transport Rule Agent (S:TRA)

Eine Zeichenfolge, die mit S:TRA beginnt, ist ein Eintrag vom Transportregel-Agent, der die folgenden wichtigen Details bereitstellt:

PROTOKOLLINFORMATIONEN	BESCHREIBUNG
ETR RuleId = [Guid]	Die ID der Regel, die abgeglichen wurde.
St=[datetime]	Datum und Uhrzeit (in UTC), als die Regelzuordnung stattfand.
Aktion = ["actiondefinition"]	Die Aktion, die angewendet wurde. Eine Liste der verfügbaren Aktionen finden Sie unter <a href="#">E-Mail-Fluss Regelaktionen in Exchange Online</a> .
Mode=Enforce	Der Modus der Regel. Die folgenden Werte sind möglich: <ul style="list-style-type: none"> <li>• <b>Erzwingen:</b> alle Aktionen für die Regel werden erzwungen.</li> <li>• <b>Test mit Richtlinientipps:</b> alle Richtlinientippaktionen werden gesendet, aber andere zu erzwingende Aktionen werden nicht ausgeführt.</li> <li>• <b>Test ohne Richtlinientipps:</b> Aktionen werden in einer Protokolldatei aufgelistet, aber Absender werden keinerlei Benachrichtigung und erzwingende Aktionen werden nicht ausgeführt.</li> </ul>

Wenn eine Nachricht eine e-Mail-Flussregel entspricht, könnte ein Beispieleintrag für custom\_data etwa wie folgt aussehen:

```
S:TRA=ETR|ruleId=19a25eb2-3e43-4896-ad9e-47b6c359779d|st=7/17/2013 12:31:25 AM|action=ApplyHtmlDisclaimer|sev=1|mode=Enforce
```

## Weitere Informationen

[Häufig gestellte Fragen zur Nachrichtenablaufverfolgung](#) Fragen zu Nachrichten, die Benutzer möglicherweise stellen, zusammen mit möglichen Antworten. Zudem wird erläutert, wie diese Antworten mit dem Tool für die Nachrichtenablaufverfolgung abgerufen und bestimmte Probleme bei der E-Mail-Zustellung behoben werden können.

[Kann ich eine nachrichtenablaufverfolgung über Exchange Online PowerShell oder Exchange Online Protection PowerShell ausführen? Was sind die Cmdlets verwenden?](#) Liefert Informationen zu den PowerShell-Cmdlets, mit denen Sie eine nachrichtenablaufverfolgung ausführen.

# Häufig gestellte Fragen zur Nachrichtenablaufverfolgung

18.12.2018 • 23 minutes to read

Dieses Thema bietet eventuelle Messaging-bezogene Fragen von Benutzern sowie mögliche Antworten. Zudem wird die Verwendung des Tools für die Nachrichtenablaufverfolgung beschrieben, um die entsprechenden Antworten abzurufen und bestimmte Probleme bei der E-Mail-Übermittlung zu behandeln.

## Wie lange dauert es, bis die Ergebnisse einer Nachrichtenablaufverfolgung angezeigt werden?

- In der Exchange-Verwaltungskonsole (EAC) werden die Suchergebnisse für Nachrichten, die weniger als 7 Tage alt sind sofort angezeigt.
- Die Suchergebnisse in die Office 365-Sicherheit und Compliance Center für Nachrichten, die weniger als 10 Tage alt sind sofort angezeigt.

Wenn Sie eine nachrichtenablaufverfolgung für ältere Nachrichten ausführen, werden die Ergebnisse innerhalb von ein paar Stunden als herunterladbaren CSV-Datei zurückgegeben.

## Wie lange dauert es für eine gesendete Nachricht in einer nachrichtenablaufverfolgung angezeigt werden, bis?

Wenn eine Nachricht gesendet wird, dauert es zwischen 5 bis 10 Minuten für die Nachricht in den Daten der nachrichtenablaufverfolgung angezeigt wird.

## Kann ich eine nachrichtenablaufverfolgung über Exchange Online PowerShell oder Exchange Online Protection PowerShell werden ausgeführt? Was sind die Cmdlets verwenden?

Die folgenden Cmdlets in Exchange Online PowerShell oder Exchange Online Protection PowerShell können Sie eine nachrichtenablaufverfolgung ausführen:

[Get-MessageTrace](#): Verfolgen von Nachrichten, die weniger als 10 Tage alt sind.

[Get-MessageTraceDetail](#): Ereignisdetails der nachrichtenablaufverfolgung für eine bestimmte Nachricht anzeigen.

[Get-HistoricalSearch](#): Verwenden Sie dieses Cmdlet, um Informationen über historische Suchläufe anzuzeigen, die innerhalb der letzten 10 Tage durchgeführt wurden.

[Start-HistoricalSearch](#): Starten Sie eine neue verlaufsüche für Nachrichten, die weniger als 90 Tage alt sind.

[Stop-HistoricalSearch](#): Beenden in der Warteschlange historischen Suchläufe, die noch nicht begonnen haben (der Statuswert ist `NotStarted`).

Zum Verbinden mit Exchange Online PowerShell finden Sie unter [Connect to Exchange Online Using Remote PowerShell](#).

Zum Verbinden mit Exchange Online Protection PowerShell finden Sie unter [Connect to Exchange Online Protection Using Remote PowerShell](#).

# Warum erhalte ich beim Ausführen einer Nachrichtenablaufverfolgung an der Benutzeroberfläche einen Timeoutfehler?

Die Ursache für ein Timeoutfehler wahrscheinlich ist, dass die Abfrage zu lange dauert. Vereinfachen Sie Ihre Suchkriterien. Sie sollten erwogen werden, das **Get-MessageTrace** -Cmdlet, das liberaler Timeout hat.

# Warum habe ich eine erwartete E-Mail nicht erhalten?

Freigeben sind einige Gründe:

- Die Nachricht wurde als Spam erkannt.
- Die Nachricht entsprach einer Regel, aufgrund derer sie in die Quarantäne verschoben wurde.
- Die Nachricht wurde abgelehnt
  - Durch den Schadsoftwarefilter
  - Da eine an die Nachricht angefügte Datei Schadsoftware enthielt
  - Da der Nachrichtentext Schadsoftware enthielt
  - Durch eine Regel
  - Da die Aktion "Ablehnen" lautete
  - Da die Aktion "TLS erzwingen" lautete und TLS nicht eingerichtet werden konnte
  - Durch einen Connector, da TLS erforderlich war, aber nicht eingerichtet werden konnte
- Die Nachricht wurde zur Moderation gesendet und wartet auf Genehmigung oder wurde vom Moderator abgelehnt,
- Die Nachricht wurde nicht gesendet.
- Die Nachricht wird noch verarbeitet, da zuvor ein Fehler aufgetreten ist und der Dienst sie erneut zustellt.
- Die Nachricht konnte nicht an Ihre Postfächer übermittelt werden
  - Da das Ziel nicht erreichbar ist
  - Da das Ziel die Nachricht zurückgewiesen hat
  - Da für die Nachricht während des Zustellversuchs die Zeitdauer überschritten wurde

Um herauszufinden, was passiert ist:

[Ausführen einer nachrichtenablaufverfolgung](#). Verwenden Sie zum Einschränken der Ergebnisse beliebig viele Suchkriterien wie möglich. Wissen Sie beispielsweise, den Absender und Empfänger oder Empfänger der Nachricht sowie die allgemeinen Zeitraum, wenn die Nachricht gesendet wurde.

Anzeigen der Ergebnisse, suchen Sie die Nachricht, und zeigen Sie bestimmte Informationen über die Nachricht (siehe [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten weniger als 7 Tage](#) oder [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten mehr als 7 Tage](#)). Suchen Sie nach Delivery Status " **Fehler** " oder **ausstehende** erläutern, warum die Nachricht nicht empfangen wurde.

Vergewissern Sie sich, dass die Nachricht gesendet wurde, dass sie erfolgreich vom Dienst empfangen wurde, dass sie nicht gefiltert, umgeleitet oder zur Moderation gesendet wurde und dass bei ihrer Zustellung keine Fehler oder Verzögerungen aufgetreten sind.

# Warum habe ich eine unerwartete Nachricht erhalten?

Freigeben sind einige Gründe:

- Die Nachricht wurde aus der Quarantäne freigegeben.
- Die Nachricht wartete auf Genehmigung durch einen Moderator und wurde freigegeben.
- Die Nachricht war Spam, der nicht erkannt wurde.
- Die Nachricht entsprach einer Regel, durch die Sie ihr als Empfänger hinzugefügt wurden.
- Die Nachricht wurde an eine Verteilerliste gesendet, der Sie angehören.

Um herauszufinden, was passiert ist:

[Ausführen einer nachrichtenablaufverfolgung](#). Verwenden Sie zum Einschränken der Ergebnisse beliebig viele Suchkriterien wie möglich. Beispielsweise geben Sie den Empfänger, der die Nachricht empfangen hat Zustellungsstatus auf **übermittelte** festgelegt, und legen Sie den Zeitraum basierend auf, wenn die Nachricht empfangen wurde.

Anzeigen der Ergebnisse, suchen Sie die Nachricht, und zeigen Sie bestimmte Informationen über die Nachricht (siehe [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten weniger als 7 Tage](#) oder [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten mehr als 7 Tage](#)).

**Warum haben eine Person nicht meine Nachricht erhalten, oder Warum erhalte ich diese Unzustellbarkeitsbericht (auch bekannt als ein Unzustellbarkeitsbericht oder Springeffekt Nachricht)?**

Mögliche Gründe sind:

- Die Nachricht wurde als Spam erkannt.
- Die Nachricht entsprach einer Regel, aufgrund derer sie in die Quarantäne verschoben wurde.
- Die Nachricht wurde umgeleitet, da ein Connector sie an ein anderes Ziel gesendet hat.
- Die Nachricht wurde abgelehnt
  - Durch den Schadsoftwarefilter
  - Da eine an die Nachricht angefügte Datei Schadsoftware enthielt
  - Da der Nachrichtentext Schadsoftware enthielt
  - Durch eine Regel
  - Da die Aktion "Ablehnen" lautete
  - Da die Aktion "TLS erzwingen" lautete und TLS nicht eingerichtet werden konnte
  - Durch einen Connector, da TLS erforderlich war, aber nicht eingerichtet werden konnte
- Die Nachricht wurde zur Moderation gesendet und wartet auf Genehmigung oder wurde vom Moderator abgelehnt,
- Die Nachricht wurde nicht gesendet.
- Die Nachricht wird noch verarbeitet, da zuvor ein Fehler aufgetreten ist und der Dienst sie erneut zustellt.
- Die Nachricht konnte nicht an das Ziel übermittelt werden
  - Da das Ziel nicht erreichbar ist

- Da das Ziel die Nachricht zurückgewiesen hat
- Da für die Nachricht während des Zustellversuchs die Zeitdauer überschritten wurde
- Die Nachricht wurde dem Ziel zugestellt, wurde jedoch gelöscht, bevor auf sie zugegriffen werden konnte (möglicherweise, weil sie einer Regel entsprach).

Um herauszufinden, was passiert ist:

[Ausführen einer nachrichtenablaufverfolgung](#). Verwenden Sie zum Einschränken der Ergebnisse beliebig viele Suchkriterien wie möglich. Wissen Sie beispielsweise, den Absender und Empfänger oder Empfänger der Nachricht sowie die allgemeinen Zeitraum, wenn die Nachricht gesendet wurde.

Anzeigen der Ergebnisse, suchen Sie die Nachricht, und zeigen Sie bestimmte Informationen über die Nachricht (siehe [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten weniger als 7 Tage](#) oder [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten mehr als 7 Tage](#)).

Suchen Sie nach Delivery Status "**Fehler**" oder **ausstehende** erläutern, warum die Nachricht nicht übermittelt wurde. Vergewissern Sie sich, dass die Nachricht gesendet wurde, dass sie erfolgreich vom Dienst empfangen wurde, die nicht gefiltert, umgeleitet, oder für die Moderation gesendet und keine Übermittlungsfehler oder Verzögerungen Erfahrung. Wenn das Ziel nicht erreichbar ist, können Sie den **Um-IP**, zur Problembehandlung für Verbindungsprobleme.

## Warum dauert es so lange, bis meine Nachricht ihr Ziel erreicht? An welchem Punkt der Pipeline befindet sie sich?

Mögliche Gründe sind:

- Die Zieladresse antwortet nicht. Dies ist das häufigste Szenario.
- Möglicherweise handelt es sich um eine umfangreiche Nachricht, deren Verarbeitung lange dauert
- Wartezeiten beim Dienst verursachen möglicherweise Verzögerungen
- Möglicherweise wurde die Nachricht blockiert; in diesem Fall lesen Sie [Warum hat ein Benutzer meine Nachricht nicht erhalten, oder warum habe ich einen Unzustellbarkeitsbericht bekommen?](#)

Um herauszufinden, was passiert ist:

[Ausführen einer nachrichtenablaufverfolgung](#). Verwenden Sie zum Einschränken der Ergebnisse beliebig viele Suchkriterien wie möglich. Wissen Sie beispielsweise, den Absender und Empfänger oder Empfänger der Nachricht sowie die allgemeinen Zeitraum, wenn die Nachricht gesendet wurde.

Anzeigen der Ergebnisse, suchen Sie die Nachricht, und zeigen Sie bestimmte Informationen über die Nachricht (siehe [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten weniger als 7 Tage](#) oder [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten mehr als 7 Tage](#)).

Abschnitt "Events" sagen Ihnen, warum die Nachricht noch nicht übermittelt wurde. Bei der Anzeige der Ereignisse können die Timestampinformationen Sie die führen Sie die Nachricht in der messagingpipeline, und erfahren Sie, wie lange dauert auf der Dienst, um jedes Ereignis zu verarbeiten. Die Ereignisdetails werden auch darüber informiert, wenn die Nachricht wird zugestellt sehr groß ist oder wenn das Ziel nicht erreichbar ist.

## Wurde eine Nachricht als Spam gekennzeichnet?

Nachrichten können aus mehreren Gründen als Spam gekennzeichnet werden. Beispielsweise kann sich die IP-Adresse des Absenders in einer der IP-Sperrlisten des Diensts befinden. Eine Nachricht kann aufgrund ihres tatsächlichen Inhalts als Spam gekennzeichnet werden, wenn sie beispielsweise einer Regel im Spaminhaltsfilter entspricht. Das Tool für die Nachrichtenablaufverfolgung verfolgt nur Ereignisse des Spaminhaltsfilters; Ereignisse

des Verbindungsfilters (z. B. gesperrte IP-Adressen) sind nicht verfolgbar. Weitere Informationen zur Spamfilterung, einschließlich der Spaminhaltsfilterung, finden Sie unter [Antispamschutz für Office 365-E-Mails](#).

Um herauszufinden, warum eine Nachricht als Spam gekennzeichnet wurde:

[Ausführen einer nachrichtenablaufverfolgung](#), suchen Sie die Nachricht in den Ergebnissen, und zeigen Sie bestimmte Informationen über die Nachricht (siehe [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten weniger als 7 Tage](#) oder [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten mehr als 7 Tage](#)).

Wenn der Inhaltsfilter eine Nachricht als Spam markiert, wenn sie in den Junk-e-Mail-Ordner oder die Quarantäne gesendet wird, wird es **übermittelte** Status aufweisen. Sie können die Ereignisdetails anzeigen, um zu sehen wie die Nachricht ihr Ziel erreicht. Beispielsweise kann es Sie darüber informieren, dass die Nachricht zu einer hohen Spam Confidence Level haben festgestellt wurde oder eine erweiterte spamfilterungsoption Übereinstimmung gefunden wurde. Sie werden auch der Aktion informiert werden, die als Ergebnis der Nachricht als Spam gekennzeichnet werden, für Beispiel, wenn es in Quarantäne gesendet wurde mit einem X-Header versehen, oder wenn sie über den Pool für hoch riskante Übermittlung gesendet wurde aufgetreten sind.

## Wurde erkannt, dass eine Nachricht Schadsoftware enthielt?

Nachrichten werden als Schadsoftware erkannt, wenn seine Eigenschaften, die im Textkörper Nachricht oder in einer Anlage eine Definition Schadsoftware in eines der antischadsoftwaremodulen übereinstimmen.

Ausführlichere Informationen zum Filtern von Schadsoftware finden Sie unter [Anti-Malware Protection](#).

Um herauszufinden, warum eine Nachricht Schadsoftware, [Ausführen einer nachrichtenablaufverfolgung](#) enthält erkannt wurde. Verwenden Sie zum Einschränken der Ergebnisse beliebig viele Suchkriterien wie möglich. Legen Sie den Delivery-Status auf **Fehler**.

Anzeigen der Ergebnisse, suchen Sie die Nachricht, und zeigen Sie bestimmte Informationen über die Nachricht (siehe [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten weniger als 7 Tage](#) oder [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten mehr als 7 Tage](#)).

Wenn die Nachricht nicht übermittelt wurde, da es Schadsoftware erkannt wurde, werden diese Informationen im Ereignisabschnitt bereitgestellt werden. Beispielsweise ist ein Beispiel für **Detail**: Malware: "ZipBomb" in Anlagen Dateigefunden wurde. Zip. Sie werden auch darüber informiert, die Aktion, die als Ergebnis einer Nachricht Schadsoftware, beispielsweise mit aufgetreten sind, wenn die gesamte Nachricht gesperrt wurde oder wenn alle Anlagen gelöscht und durch eine Datei Warntext ersetzt wurden.

## Welche e-Mail-Flussregel (auch bekannt als eine Transportregel) oder DLP-Richtlinie wurde auf eine Nachricht angewendet?

Um herauszufinden, welche Mail Flow Regel (benutzerdefinierte Richtlinienregel) oder Data Loss Prevention (DLP) Richtlinie (nur Exchange Online-Kunden) wurde auf eine Nachricht, [Ausführen einer nachrichtenablaufverfolgung](#) angewendet. Verwenden Sie zum Einschränken der Ergebnisse beliebig viele Suchkriterien wie möglich. Legen Sie den Delivery-Status auf **Fehler**.

Anzeigen der Ergebnisse, suchen Sie die Nachricht, und zeigen Sie bestimmte Informationen über die Nachricht (siehe [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten weniger als 7 Tage](#) oder [Anzeigen der Ergebnisse der nachrichtenablaufverfolgung für Nachrichten mehr als 7 Tage](#)).

Wenn die Nachricht nicht übermittelt wurde, da der Inhalt einer Regel entsprach, wird der Abschnitt "Events" können Sie den Namen der Regel Mail Flow kennen, die abgeglichen wurde. Sie werden außerdem benachrichtigt werden, der die Aktion, die als Ergebnis der e-Mail-Fluss Abgleich, beispielsweise auftritt, wenn die Nachricht abgelehnt isoliert wurde, umgeleitet, für die Moderation, entschlüsselt, gesendet, oder eine beliebige Anzahl von anderen möglichen Optionen. Informationen zur Exchange-Mail Flow Regeln erstellen, und legen Sie für diese Aktionen finden Sie in der [E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#).

## Wenn ich eine Nachrichtenablaufverfolgung ausführe, gibt sie Regel-ID-1 zurück. Was bedeutet das?

Regel-ID-1 wird zurückgegeben, wenn die nachrichtenablaufverfolgung eine e-Mail erkennt Flow-Regel, die nicht mehr vorhanden ist. (Die Regel der e-Mail-Fluss konnte geändert oder gelöscht wurden, nachdem die ursprüngliche Nachricht gesendet wurde.)

## Gibt es bekannte Einschränkungen oder Erläuterungen zum Verhalten, die ich kennen sollte, wenn ich das Tool für die Nachrichtenablaufverfolgung verwende?

Beim Verwenden des Tools für die Nachrichtenablaufverfolgung sollten Sie Folgendes beachten:

- **IP-blockierte Nachrichten:** Nachrichten von IP-Reputation-Sperrlisten blockiert werden in den Spam-Daten für Echtzeitberichte enthalten sein, aber Sie können nicht auf diese Nachrichten keine nachrichtenablaufverfolgung durchführen.
- **Nachrichten umgeleitet:** Wenn ein Empfänger durch eine e-Mail-Flussregel umgeschrieben wird oder, da die Spam-Aktion für die Domäne auf **Umleiten an e-Mail-Adresse** festgelegt ist, die Nachricht nicht nachverfolgbare in einem einzelnen Suchvorgang wird. Die ursprüngliche Nachricht kann bis zu dem Punkt zurückverfolgt werden, wenn der Empfänger geändert wird. Danach wird die Meldung nicht nachverfolgbare unter den ursprünglichen Empfänger. Sie können die Nachricht erneut mit den neuen Empfänger verfolgen.
- **MAIL FROM:** das Tool für die nachrichtenablaufverfolgung verwendet den Wert MAIL FROM präsentiert an die Einleitung der SMTP-Unterhaltung als Absender in einer Suche, unabhängig davon, welche Datenabschnitt der Nachricht angezeigt. Die Nachricht eine Antwort-an-Adresse anzeigen kann oder unterscheidet: oder Absender Werte. Wenn die e-Mail-Nachricht von einem Prozess und nicht durch ein e-Mail-Client gesendet wurde, wird sehr wahrscheinlich, dass der Absender in der MAIL FROM den Absender in der aktuellen Nachricht nicht übereinstimmt.
- **Mail Flow Regel Updates:** Wenn eine Nachricht eine e-Mail-Flussregel entspricht, wird die Regel-ID in der Nachricht Trace und Echtzeit reporting Datenbanken gespeichert. Wenn Sie eine dieser Nachrichten verfolgen oder einen für Regeldetails in einem Bericht Drilldown, ziehen Sie die nachrichtenablaufverfolgung und Benutzeroberflächen dynamisch reporting Echtzeit die aktuelle Regelinformationen vom Netzwerk gehostete Dienste basierend auf die Regel-ID in der Berichtsdatenbank. Wenn Sie die Attribute dieser bestimmten Regel geändert haben, da die Nachricht verarbeitet wurde (es von geändert ablehnen auf zulassen, beispielsweise), die Regel-ID bleibt in der Nachricht Trace und Echtzeit reporting Ergebnisse zurückgegeben, aber die Exchange-Verwaltungskonsole wird angezeigt. die e-Mail-Flusseigenschaften für neue Regel. Sie können das Überwachungsfeature-Berichte, um zu bestimmen, wann die Regel geändert wurde und die Eigenschaften, die geändert wurden.
- **Spamgefilterte Nachrichten:** Wenn der Inhaltsfilter eine Nachricht als Spam markiert und die Nachricht in den Ordner "Junk-E-Mail" verschoben oder isoliert wird, weist sie den Status **Zugestellt** auf. Führen Sie einen Drilldown in den Ereignisdetails aus, um festzustellen, wie die Nachricht ihr Ziel erreicht hat.

## Weitere Informationen

[Verfolgen einer E-Mail](#)

[Help and Support for EOP](#)

# Sichern von E-Mails in Exchange Online

18.12.2018 • 7 minutes to read

Eine der Fragen, die uns häufig gestellt wird, lautet: "Wie sichert Exchange Online meine Daten?" Sie stellen diese Frage möglicherweise, weil Sie sich Sorgen darüber machen, wie Ihre Daten bei Auftreten eines Fehlers gesichert werden. Oder Sie überlegen, wie Ihre Daten wiederhergestellt werden können, wenn sie versehentlich gelöscht wurden. Im folgenden Thema werden diese Fragen beantwortet.

## Sichern von Daten in Exchange Online

Vieles können Verfügbarkeit, wie Hardwarefehler, Naturkatastrophen oder Benutzerfehler unterbrochen werden. Um sicherzustellen, dass Ihre Daten stets zur Verfügung steht und Dienste fortgesetzt, auch wenn unerwartete Ereignisse auftreten, verwendet Exchange Online die gleiche Technologie im Exchange-Server gefunden. Exchange Online verwendet beispielsweise die Exchange Server-Funktion bekannt als Database Availability Groups zum Replizieren von Exchange Online-Postfächer auf mehrere Datenbanken in separaten Microsoft-Rechenzentren. Daher können Sie jederzeit auf dem neuesten Stand Postfachdaten im Fall eines Ausfalls zugreifen, die eine der Datenbankkopien wirkt sich auf. Zusätzlich zu mehreren Exemplaren eines einzelnen Postfachdatenbank, Sichern der verschiedenen Datencentern Daten für voneinander. Bei Ausfall eines werden die betroffenen Daten in einer anderen Datacenter mit eingeschränkter Dienst Unterbrechung übertragen und Benutzer nahtlose Konnektivität bemerken.

### NOTE

Sie können die aktuellen Informationen zu einem Ereignis, das eine Dienstunterbrechung verursacht, abrufen, indem Sie sich am Service Health Dashboard anmelden. Weitere Informationen finden Sie unter [Anzeigen des Status Ihrer Dienste](#).

### Was geschieht, wenn Benutzer versehentlich Daten aus ihren Postfächern löschen?

Der Exchange Online-Dienst bietet mehrere Optionen zur Wiederherstellung gelöschter Elemente. Dazu zählen beispielsweise die Wiederherstellung aus gelöschten Elementen, die Wiederherstellung aus wiederherstellbaren Elementen, die Wiederherstellung einzelner Elemente sowie Aufbewahrungsrichtlinien und -tags. Archivierung und Beweissicherungsverfahren stehen auch innerhalb der entsprechenden Lizzenen zur Verfügung und ergänzen die Anforderungen der Aufbewahrung von Daten.

- **Aufbewahrungszeit für gelöschte:** Benutzer können wiederherstellen, e-Mail-Elemente, die in einem beliebigen e-Mail-Ordner gelöscht wurden. Wenn ein Benutzer ein Element löscht, wird es in den Löschgänge Unterordner des Ordners "wiederherstellbare Elemente" gespeichert. Elemente bleiben in diesem Ordner, bis der Benutzer manuell entfernt, oder sie automatisch von Aufbewahrungsrichtlinien entfernt werden. Weitere Informationen zu wiederherstellbaren Elementen finden Sie unter [Ordner "wiederherstellbare Elemente"](#)
- **Wiederherstellung einzelner Elemente:** e-Mail-Wiederherstellung bietet verbesserte in Exchange Online, dass Benutzer einzelne Elemente wiederherstellen, ohne Postfachdatenbanken wiederherstellen können. Beim Assistenten für verwaltete Ordner "wiederherstellbare Elemente" für ein Postfach, die Wiederherstellung einzelner Elemente aktiviert hat verarbeitet, wird keines Element im Unterordner "bereinigt" die Aufbewahrungszeit für gelöschte Elemente für dieses Element nach Ablauf der noch nicht gelöscht.
- **Aufbewahrungstags und Aufbewahrungsrichtlinien:** Diese Einstellungen angeben, wie lange eine Nachricht verbleibt in einem Postfach und die Aktion, die ausgeführt werden soll, wenn die Meldung die angegebenen Aufbewahrungszeitraum erreicht. Wenn eine Nachricht den Aufbewahrungszeitraum erreicht,

hat des Benutzers Compliance-Archiv verschoben oder gelöscht. Weitere Informationen zu aufbewahrungstags und Richtlinien finden Sie unter [aufbewahrungstags und Aufbewahrungsrichtlinien](#).

#### **IMPORTANT**

Alle zuvor erwähnten Optionen für die Wiederherstellung für gelöschte Elemente ist Notiz, die Zeit Wiederherstellung der Postfachelemente verweisen außerhalb des Bereichs der Exchange-Dienst. Allerdings bietet Exchange Online umfassende Aufbewahrung und Wiederherstellung für die e-Mail-Infrastruktur einer Organisation unterstützen und Ihrer Postfachdaten ist verfügbar, wenn Sie wird, benötigt unabhängig davon, was geschieht.

In den folgenden Themen finden Sie weitere Details zu weiteren Optionen.

- [Hohe Verfügbarkeit und Geschäftskontinuität](#)
- [Exchange Online-Dienstbeschreibung](#)
- [Erstellen oder Entfernen eines Compliance-Archivs](#)
- [Aktivieren des Beweissicherungsverfahrens für ein Postfach](#)
- [Verwalten Sie inaktiver Postfächer in Exchange Online](#)

## Wie sichern Benutzer Outlook-Daten?

Benutzer können ihre Outlook-Daten in Outlook auf einen anderen Computer exportieren oder ein Backup dieser Daten erstellen, indem Sie die Schritte im Thema [Exportieren oder Sichern von E-Mails, Kontakten und Kalenderelementen in eine Outlook-PST-Datei](#) ausführen. Leider können Benutzer von Outlook Web App das Backup ihrer Daten nicht selbst durchführen.

Informationen zum Wiederherstellen von gelöschten Elementen in Outlook finden Sie unter [Wiederherstellen gelöschter Elemente in Outlook](#).

Informationen zum Wiederherstellen von gelöschten Elementen in finden Sie unter [Wiederherstellen gelöschter Elemente oder E-Mails in Outlook Web App](#).

## Sichern von Exchange Server

Lesen Sie weitere Informationen zum Sichern von Exchange Server 2016 und Exchange Server 2019 [Mithilfe von Windows Server-Sicherung zum Sichern und Wiederherstellen von Exchange-Daten](#) .

## Offboarding von Benutzern aus Office 365

Weitere Informationen zu den erforderlichen Schritten, wenn Benutzer Ihre Organisation verlassen, finden Sie unter [Offboarding von Benutzern aus Office 365](#). Dieses Thema enthält Informationen zu Schritten, die Sie ausführen sollten, wenn Mitarbeiter Ihre Organisation verlassen, und zum Schutz von Daten.

# Outlook reparieren - Was tun, wenn Office nicht mehr funktioniert

18.12.2018 • 3 minutes to read

Wenn Sie Outlook für den Zugriff auf Ihr Office 365-E-Mail-Konto oder ein anderes Exchange-basiertes E-Mail-Konto verwenden und Probleme auftreten, möchten wir, dass Sie so schnell wie möglich wieder E-Mails senden und empfangen können.

## NOTE

Wenn Sie Hilfe zu Outlook.com benötigen, sehen Sie in der [Hilfe zu Outlook.com](#) nach. > Wenn Sie Hilfe zu Outlook für Mac benötigen, lesen Sie [Hilfe zu Outlook 2016 für Mac](#).

## Lassen Sie uns Ihre Outlook-Verbindungsprobleme für Sie beheben

Wir können verschiedene allgemeine Outlook-Verbindungsprobleme für Sie diagnostizieren und beheben. Wenn das Problem mithilfe unseres automatisierten Tools nicht behoben werden kann oder Sie selber das Problem beheben möchten, finden Sie Informationen dazu im nächsten Abschnitt.

<input type="text"/>	<b>Lassen Sie uns Ihr Problem beheben</b> Herunterladen des Support- und Wiederherstellungs-Assistenten für Office 365	<input type="text"/>	<b>Benötigen Sie weitere Hilfe?</b> Kontakt-Unterstützung für Business-Produkte - Admin-Hilfe.
----------------------	--	----------------------	--

## Beheben von Problemen mit Softwareupdates und Profilen

Veraltete Software und beschädigte Outlook-Profile sind zwei der am häufigsten auftretenden Probleme, die Sie am Senden und Empfangen von E-Mails hindern können. Wenn Sie ein Administrator sind und mehrere Benutzer Probleme melden, sollten Sie auch auf Dienstprobleme mit Office 365 prüfen.

\*\*\*\*GÄNGIGE OUTLOOKFEHLERBEHEBUNGEN\*\*\*\*

\*\*\*\*GÄNGIGE  
OUTLOOKFEHLERBEHEBUNGEN\*\*\*\*

**Ausführen von Windows Update**

Wenn Ihre Outlook-Clientsoftware oder Windows-Betriebssystemsoftware veraltet ist, können Probleme beim Senden und Empfangen von E-Mails auftreten. Gehen Sie unter Windows 8 folgendermaßen vor, um Windows Update auszuführen. Anweisungen für Windows 7 finden Sie unter [Wie kann ich feststellen, ob der Computer auf dem neuesten Stand ist?](#)

Wischen Sie auf dem Bildschirm von rechts nach links, und wählen Sie **Suchen** aus.

Geben Sie **Windows Update** in das Suchfeld ein.

Tippen oder klicken Sie auf **Einstellungen**, und tippen oder klicken Sie dann auf **Optionale Updates installieren**. Möglicherweise müssen Sie Ihren Computer neu starten.

**Reparieren Ihres Outlook-Profil**

Bei einem Outlook-Profil handelt es sich um eine Reihe von Konfigurationsinformationen, die Ihren Benutzernamen, das Kennwort und den Speicherort von Dateien umfassen.

Reparieren Sie Ihr Outlook-Profil anhand der folgenden Schritte.

Wählen Sie **Datei** aus.

Wählen Sie den Abwärtspfeil für **Kontoeinstellungen** und dann **Kontoeinstellungen** aus.

Wählen Sie auf der Registerkarte **E-Mail** Ihr Konto (Profil) und dann **Reparieren** aus.

Befolgen Sie die Aufforderungen im Assistenten. Wenn Sie damit fertig sind, starten Sie Outlook erneut.

**Prüfen auf Dienstprobleme**

**Nur Administratoren:** Wenn mehr als eine Person in Ihrer Organisation Probleme mit E-Mails in Office 365 hat, könnte ein Problem mit dem Dienst aufgetreten sein. Wechseln Sie zur [Office 365-Dashboardseite](#) "Dienststatus" (Anmeldung mit Administratorrechten erforderlich), und prüfen Sie den Status der Dienste unter [Exchange Online](#).

# Beheben von Outlook und Office 365-Problemen mit Unterstützung und Recovery-Assistenten für Office 365

18.12.2018 • 3 minutes to read

*Letzte aktualisierte 1-August, 2017*

Die Unterstützung und Recovery-Assistenten-app kann Ihnen identifizieren und korrigieren mehrere Aspekte für die folgenden apps und Dienste.

- Office-setup
- Outlook
- Outlook für Mac 2016 oder Outlook für Mac 2011
- Mobile Geräte
- Outlook im Web für Unternehmen
- Microsoft Dynamics CRM Online
- Exchange Online
- OneDrive for Business

Das folgende Video veranschaulicht, wie zum Ausführen von Diagnosetests Support- und Recovery-Assistenten verwenden.

## Erstellen eines Outlook-Profils

Erstellen oder Ihr Outlook-Profil neu erstellen, installieren und Ausführen der [\\*\\* Office 365-Support und Recovery-Assistenten.\\*\\*](#)

1. Melden Sie sich mit Ihren Office 365-Anmeldeinformationen.
2. Öffnen Sie **Outlook**.
3. Wählen Sie **ich meine Office 365 e-Mail in Outlook einrichten Hilfe benötigen**.

Die Unterstützung und Recovery-Assistenten werden einige Tests ausgeführt und nun können Sie die e-Mail-Adresse ein Outlook-Profil erstellen.

## Herunterzuladen und Support und Recovery-Assistenten zu starten

1. Wechseln Sie zu der [Support- und Recovery-Assistenten für Office 365-Downloadseite](#).
2. Klicken Sie auf **jetzt herunterladen**.
3. Führen Sie das Installationsprogramm.
4. Support und Recovery-Assistent wird nach der Installation automatisch gestartet.

## Unterstützung für die Verwendung und Recovery-Assistent

1. Wählen Sie **ich stimme zu**, den Lizenzvertrag zu akzeptieren.
2. Wählen Sie die app aus, den, die Sie verwenden möchten, hier erhalten Sie Hilfe, und klicken auf **Weiter**.
3. Wählen Sie im Supportthema, das am ehesten Ihres Problems ein, und wählen Sie dann auf **Weiter**.
4. Melden Sie sich mit Ihrem Office 365-Geschäfts-, Schul- oder Unikonto an.
5. Warten Sie, bis die Reihe der Tests abgeschlossen ist.
6. Prüfen Sie die Testergebnisse, und gehen Sie anschließend wie folgt vor:
  - Wenn die Anwendung Ihr Problem beheben konnte, folgen Sie den Eingabeaufforderungen, und schließen Sie das Tool.
  - Wenn die Tests fehlgeschlagen sind, gibt die Anwendung den Grund hierfür an und schlägt weitere Lösungen vor.
7. Nach Abschluss die app abgeben Sie, und schließen Sie die app.

## Und was ist, wenn weiterhin Probleme auftreten?

Wenn Support- und Wiederherstellungs-Assistent für Office 365 das Problem nicht automatisch beheben kann, bieten wir Ihnen Vorschläge für die nächsten Schritte und helfen Ihnen, mit dem Office 365-Support in Verbindung zu treten.

## Wie verwende ich Support- und Recovery-Assistent mit meinem mobilen Gerät, und Outlook für Mac 2016 oder Outlook für Mac 2011?

Support und Recovery-Assistenten können ausführen Diagnose und Beheben von Problemen mit Office 365-Konten, die den Dienst über ein mobiles Gerät oder einem Mac zugreifen Die app zur Ausführung der Diagnose verwenden, müssen Sie jedoch herunter und führen es auf einem PC.

# Deaktivieren der Diagnoseprotokollierung im Support- und Wiederherstellungs-Assistenten für Office 365

18.12.2018 • 4 minutes to read

[] Der [Support- und Wiederherstellungs-Assistent für Office 365](#) sammelt standardmäßig Diagnoseprotokolle, um Probleme in den folgenden Szenarien behandeln zu können.

- Manchmal sammelt der Support- und Wiederherstellungs-Assistent Diagnoseprotokolle, wenn ein Problem eines Benutzers nicht mithilfe des Tools behoben werden konnte.
- Der Support- und Wiederherstellungs-Assistent sammelt Diagnoseprotokolle, wenn ein Benutzer die erweiterte Diagnose ausführt. Dies geschieht in der Regel auf Anforderung eines Administrators oder Microsoft-Supporttechnikers.

In Office 365 werden Diagnoseprotokolle zur Verbesserung des Tools verwendet, um künftig eine bessere Problembehandlung bieten zu können. Microsoft-Supporttechniker können diese Protokolle auch verwenden, um das spezifische Problem des Benutzers genauer zu analysieren. Als Administrator können Sie die Registrierung bearbeiten, um zu verhindern, dass Benutzer Diagnoseprotokolle sammeln, wenn Ihre Organisation die Datenfreigabe einschränken möchte.

#### Caution

Der Registrierungs-Editor ist ein Tool für fortgeschrittene Benutzer. Führen Sie die in diesem Artikel aufgeführten Schritte sorgfältig aus, um sicherzustellen, dass Sie nur Änderungen an der Datensammlung für den Support- und Wiederherstellungs-Assistenten vornehmen. Erstellen Sie eine Sicherungskopie (für den Fall, dass Probleme auftreten), bevor Sie Änderungen an der Registrierung vornehmen. Weitere Informationen zum Erstellen einer Sicherungskopie finden Sie unter [Sichern und Wiederherstellen der Registrierung in Windows](#).

## Option 1: Erstellen eines neuen Registrierungseintrags

Zum Deaktivieren der Datensammlung im Support- und Wiederherstellungs-Assistenten müssen Sie den folgenden Registrierungseintrag erstellen.

Unterschlüssel: HKEY\_LOCAL\_MACHINE\Software\Microsoft\Support- und Wiederherstellungs-Assistent

DWORD-Wert: UploadDiagnosticLogsDisabled

Wert: 1

Ausführliche Informationen zum Erstellen von Registrierungswerten finden Sie unter [Hinzufügen, Ändern oder Löschen von Registrierungsunterschlüsseln und -werten mit einer REG-Datei](#).

Mit der Registrierungseintrag vorhanden können keine Support- und Recovery-Assistenten von Diagnoseprotokollen sammeln. Wenn Sie die Log-Auflistung später wieder aktivieren möchten, können Sie ändern Sie den Wert auf 0 oder den Registrierungseintrag löschen.

## Option 2: Bearbeiten eines vorhandenen Registrierungsunterschlüssels

Wenn Sie zuvor einen Registrierungseintrag für den Support- und Wiederherstellungs-Assistenten erstellt haben, können Sie den Eintrag so bearbeiten, dass die Datensammlung deaktiviert wird. Führen Sie die folgenden Schritte

aus, um einen vorhandenen Registrierungsunterschlüssel zwecks Deaktivierung der Datensammlung zu bearbeiten.

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zum folgenden Registrierungsunterschlüsselpfad:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Support- und Wiederherstellungs-Assistent

3. Doppelklicken Sie auf den **Reg\_DWORD**-Wert mit dem Namen **UploadDiagnosticLogsDisabled**. (Wenn **UploadDiagnosticLogsDisabled** nicht angezeigt wird, müssen Sie diesen Wert gemäß den Anweisungen unter "Option 1: Erstellen eines neuen Registrierungseintrags" hinzufügen.)
4. Geben Sie im Feld **Wertdaten** den Wert 1 ein, und wählen Sie **OK** aus.
5. Schließen Sie den Registrierungs-Editor.

Nachdem Sie diesen Registrierungseintrag bearbeitet haben, können die Benutzer keine Diagnoseprotokolle mehr sammeln.

## Festlegen, ob der Support- und Wiederherstellungs-Assistent Daten sammeln soll

Der Support- und Wiederherstellungs-Assistent sammelt Protokolldaten, wenn eine der folgenden Einstellungen vorhanden ist.

- Der DWORD-Wert **UploadDiagnosticLogsDisabled** ist auf einen anderen Wert als 1 festgelegt.
- Der Unterschlüssel `HKEY_LOCAL_MACHINE\Software\Microsoft\Support and Recovery Assistant` ist nicht vorhanden.

## Verwandte Artikel

- [Beheben von Outlook- und Office 365-Problemen mit dem Support- und Wiederherstellungs-Assistenten von Microsoft für Office 365](#)
- [Herunterladen des Support- und Wiederherstellungs-Assistenten von Microsoft](#)

# Suchen und Beheben von Problemen mit der E-Mail-Zustellung als Office 365 Business-Administrator

18.12.2018 • 14 minutes to read

Wenn Benutzer melden, dass sie keine E-Mails empfangen, kann sich die Suche nach der Lösung schwierig gestalten. Möglicherweise spielen Sie im Kopf eine Reihe von Problembehandlungsszenarien durch. Ist etwas mit Outlook nicht in Ordnung? Ist der Office 365-Dienst ausgefallen? Gibt es ein Problem beim Nachrichtenfluss oder den Einstellungen für die Spamfilterung? Oder liegt das Problem an einer Stelle, die sich Ihrer Kontrolle entzieht, wie etwa einem Absender, der in einer globalen Liste mit blockierten Absendern geführt wird? Glücklicherweise bietet Office 365 leistungsstarke automatische Tools, die Sie beim Suchen und Beheben einer Vielzahl von Problemen unterstützen können.

## Das Wichtigste zuerst: Überprüfen Sie, ob ein Problem mit Outlook oder einer anderen E-Mail-App vorliegt.

Wenn nur ein Benutzer Probleme beim Empfang von E-Mails meldet, liegt möglicherweise ein Problem bei seinem E-Mail-Konto oder seiner E-Mail-App vor. Lassen Sie den betroffenen Benutzer die folgenden Lösungen ausprobieren, bevor Sie zu administratorspezifischen Aufgaben übergehen.

### Verwenden von Outlook im Web zur Suche nach fehlenden Nachrichten - 5 Minuten

Wenn ein Benutzer E-Mails in seinem Outlook im Web-Posteingang empfängt, doch nicht in der auf seinem Computer installierten E-Mail-App, könnte dies darauf hindeuten, dass ein Problem mit dem Computer des Benutzers oder einer E-Mail-App vorliegt. Bitten Sie diesen Benutzer, sich bei Outlook im Web anzumelden, um zu überprüfen, ob sein Office 365-E-Mail-Konto ordnungsgemäß funktioniert.

**Anweisungen:** [Melden Sie sich bei Outlook im Web für Unternehmen](#)

### Ausführen des Support- und Wiederherstellungs-Assistenten für Office 365 zur Behebung von Problemen mit Outlook oder dem Konto - 10 Minuten

Wenn ein einzelner Benutzer in Ihrer Organisation Probleme beim E-Mail-Empfang hat, kann dies an einem Lizenzproblem, einem Profilproblem, einer falschen Outlook-Version oder einer Kombination anderer Probleme liegen. Glücklicherweise findet der Support- und Wiederherstellungs-Assistent die meisten Probleme mit Outlook oder Office 365 und hilft Ihnen bei deren Behebung. Als ersten Schritt bei der Behandlung von Problemen mit der E-Mail-Zustellung für Office 365 Business empfehlen wir Ihnen, den Support- und Wiederherstellungs-Assistenten herunterzuladen und auf dem betroffenen Computer auszuführen. Wenn Probleme mit Outlook für Mac oder beim mobilen Zugriff auftreten, können Sie Ihre Kontoeinstellungen mithilfe der App überprüfen, müssen diese aber auf einem PC installieren. Nachdem Sie sich mit dem betroffenen Konto angemeldet haben, überprüft die App auf Probleme. Benutzer können den Support- und Wiederherstellungs-Assistenten in der Regel herunterladen und ausführen, ohne ihren Office 365-Administrator um Hilfe bitten zu müssen.

[Lassen Sie uns Ihr Problem beheben](#) [Laden Sie Support- und Recovery-Assistent für Office 365](#)

Schauen Sie sich das folgende Video mit weiteren Informationen dazu an, wie Sie die App Support- und Wiederherstellungs-Assistent verwenden können.

# Wenn die App Support- und Wiederherstellungs-Assistent das Problem mit der Zustellung von E-Mails nicht beheben kann, probieren Sie diese Administrator tools aus

Als Office 365 Business-Administrator haben Sie Zugriff auf mehrere Tools, mit denen Sie ermitteln können, warum die Benutzer keine E-Mails erhalten haben. Das folgende Video gibt einen kurzen Überblick über die für Sie verfügbaren Tools.

Die nachstehenden Tools werden von der schnellsten zur tiefgreifendsten Option aufgeführt.

## Überprüfen des Office 365-Dienststatus auf Exchange Online-Probleme - 5 Minuten

Auf der Seite für den Dienststatus wird der Status von Office 365-Diensten aufgelistet und angegeben, ob es kürzlich zu Dienstvorfällen gekommen ist. Führen Sie die nachstehenden Schritte aus, um den Dienststatus zu überprüfen.

1. [Where to sign in to Office 365 for business](#) mit Ihrem Firmen- oder Schulkonto an.
2. Wählen Sie das Symbol für das App-Startfeld in der oberen linken Ecke und dann **Administrator** aus.

### TIP

**Administrator** wird nur Office 365-Administratoren angezeigt.

Sie können die gesuchte App nicht finden? Wählen Sie im Startprogramm auf **Alle Apps** aus, um eine alphabetische Liste der verfügbaren Office 365-Apps anzuzeigen. Hier können Sie nach einer bestimmten App suchen.

3. Wechseln Sie unter **Dienststatus** zu **Dienststatus anzeigen**.

Wenn es ein Hinweis darauf ist verschlechtert sich die ExchangeOnline Service für Ihre Organisation möglicherweise e-Mail-Übermittlung verzögert werden und CompanyName Service Ingenieure funktionieren bereits Wiederherstellen des Diensts. Überprüfen der Integrität Seite für Aktualisierungen des Aufgabenstatus. In diesem Fall müssen Sie keine Serviceanfrage geöffnet werden, da bereits CompanyName funktionsfähig ist, um das Problem zu beheben.

## Verwenden der Nachrichtenablaufverfolgung für tiefgreifende Problembehandlung bei der Nachrichtenübermittlung - 15 Minuten

Es kann vorkommen, dass eine E-Mail bei der Übermittlung verloren geht oder dass die Übermittlung länger als erwartet dauert und Ihre Empfänger sich wundern, was passiert ist. Mit der Funktion für die Nachrichtenablaufverfolgung können Sie die Nachrichtenübermittlung durch den Exchange Online-Dienst verfolgen. Mit dem Erhalt detaillierter Informationen zu einer bestimmten Nachricht können Sie die Fragen Ihrer Benutzer effizient beantworten, Probleme mit dem Nachrichtenfluss behandeln und Richtlinienänderungen überprüfen. Außerdem verringert sich damit die Notwendigkeit, den technischen Support um Mithilfe bitten zu müssen.

### Öffnen des Tools für die Nachrichtenablaufverfolgung

Wenn Sie ein Office 365 Midsize Business-, Office 365 Business- oder Office 365 Enterprise-Administrator sind, greifen Sie über das Exchange Admin Center auf das Tool für die Nachrichtenablaufverfolgung zu und führen es von dort aus. Führen Sie dazu die folgenden Schritte aus:

1. [Where to sign in to Office 365 for business](#) mit Ihrem Firmen- oder Schulkonto an.

2. Wählen Sie das Symbol für das App-Startfeld in der oberen linken Ecke und dann **Administrator** aus.

**TIP**

**Administrator** wird nur Office 365-Administratoren angezeigt.

Sie können die gesuchte App nicht finden? Wählen Sie im Startprogramm auf **Alle Apps** aus, um eine alphabetische Liste der verfügbaren Office 365-Apps anzuzeigen. Hier können Sie nach einer bestimmten App suchen.

3. Wechseln Sie zu **Exchange**.



4. Wechseln Sie unter **Nachrichtenfluss** zu **Nachrichtenablaufverfolgung**.

Wenn Sie ein Office 365 Small Business-Administrator sind, führen Sie die folgenden Schritte aus, um die Nachrichtenablaufverfolgung zu finden.

1. Wechseln Sie zu **Administrator** > **Diensteinstellungen** > **E-Mail, Kalender und Kontakte**.

2. Klicken Sie unter **Behandlung von E-Mail-Problemen** auf **Probleme mit der Nachrichtenübermittlung behandeln**.

**Ausführen der Nachrichtenablaufverfolgung und Anzeigen der Zustelldetails von Nachrichten, die in der letzten Woche gesendet wurden**

Die Nachrichtenablaufverfolgung wird standardmäßig auf eine Suche nach allen Nachrichten festgelegt, die innerhalb der letzten 48 Stunden von Ihrer Organisation gesendet oder empfangen wurden. Sie können am Ende der Seite **Suchen** auswählen, um diesen Bericht zu generieren. Er kann Ihnen eine allgemeine Vorstellung davon vermitteln, was mit dem Nachrichtenfluss in Ihrer Organisation geschieht. Um jedoch das Problem mit der Zustellung von E-Mails bei einem bestimmten Benutzer zu beheben, können Sie die Ergebnisse der Nachrichtenablaufverfolgung auf dessen Postfach und den Zeitrahmen begrenzen, innerhalb dessen der Nachrichtenempfang erwartet wurde.



1. Wählen Sie aus dem Menü **Datumsbereich** den Datumsbereich aus, der dem Zeitpunkt am nächsten kommt, zu dem die fehlende Nachricht gesendet wurde.
2. Verwenden Sie **Absender hinzufügen** und **Empfänger hinzufügen**, um einen oder mehrere Absender bzw. Empfänger hinzuzufügen.
3. Klicken Sie auf **Suchen**, um die Nachrichtenablaufverfolgung durchzuführen.
4. Auf der Seite **Ergebnisse der Nachrichtenablaufverfolgung** werden alle Nachrichten angezeigt, die mit den ausgewählten Kriterien übereinstimmen. Typische Nachrichten sind unter der Statusspalte mit **Zugestellt** gekennzeichnet.



5. Wenn Sie Details zu einer Nachricht anzeigen möchten, wählen Sie die Nachricht und dann  ( **Details** ) aus.
6. In den daraufhin angezeigten Details wird erläutert, was mit der Nachricht geschehen ist. Folgen Sie den Anweisungen im Abschnitt **So beheben Sie das Problem**, um das Problem zu beheben.



Wenn Sie nach einer anderen Nachricht suchen möchten, können Sie auf der Seite

**Nachrichtenablaufverfolgung** auf die Schaltfläche **Löschen** klicken und dann neue Suchkriterien eingeben.

#### Anzeigen der Ergebnisse einer Nachrichtenablaufverfolgung für mehr als sieben Tage

Nachrichtenablaufverfolgungen für Elemente, die älter als sieben Tage sind, stehen nur als herunterladbare CSV-Datei zur Verfügung. Weil Daten zu älteren Nachrichten in einer anderen Datenbank gespeichert sind, können Nachrichtenablaufverfolgungen für ältere Nachrichten bis zu einer Stunde dauern. Führen Sie eine der folgenden Aktionen aus, um die CSV-Datei herunterzuladen:

- Klicken Sie auf den Link in der E-Mail-Benachrichtigung, die nach Abschluss der Nachrichtenablaufverfolgung gesendet wird.
- Wenn Sie eine Liste der Ablaufverfolgungen für Elemente, die älter als sieben Tage sind, anzeigen möchten, klicken Sie im Tool für die Nachrichtenablaufverfolgung auf **Ausstehende oder abgeschlossene Nachrichtenablaufverfolgungen anzeigen**.



In der daraufhin angezeigten Benutzeroberfläche ist die Liste der Ablaufverfolgungen basierend auf dem Datum und der Uhrzeit sortiert, an dem bzw. zu der sie gesendet wurden. Dabei stehen die letzten Übermittlungen an erster Stelle.

Wenn Sie eine bestimmte Nachrichtenablaufverfolgung auswählen, werden im rechten Bereich zusätzliche Informationen angezeigt. Je nach den angegebenen Suchkriterien sind hierin Details wie der Datumsbereich aufgeführt, für den die Ablaufverfolgung ausgeführt wurde, sowie der Absender und die gewünschten Empfänger der Nachricht.

#### NOTE

Nachrichtenablaufverfolgungen, die Daten enthalten, die älter als sieben Tage sind, werden automatisch gelöscht. Sie können nicht manuell gelöscht werden.

#### Häufig gestellte Fragen zur Nachrichtenablaufverfolgung

##### Wie lange dauert es nach dem Senden einer Nachricht, bis sie von der Nachrichtenablaufverfolgung gefunden wird?

Nachrichtenablaufverfolgungs-Daten können schon 10 Minuten nach dem Versand einer Nachricht angezeigt werden, es kann aber auch bis zu einer Stunde dauern.

##### Warum erhalte ich beim Ausführen der Nachrichtenablaufverfolgung einen Timeoutfehler?

Wahrscheinlich dauert die Suche zu lange. Versuchen Sie, die Suchkriterien zu vereinfachen.

##### Warum dauert es so lange, bis meine Nachricht den Zielort erreicht?

Zu den möglichen Ursachen gehören folgende:

- Der gewünschte Zielserver reagiert nicht. Dies ist die häufigste Ursache.
- Eine umfangreiche Nachricht erfordert eine lange Verarbeitungszeit.
- Die Verzögerungen werden von der Wartezeit des Diensts verursacht.
- Die Nachricht wurde vom Filterdienst blockiert.

# Dienstupgrade von Exchange Online und Exchange Online Protection [wave15]

18.12.2018 • 2 minutes to read

Microsoft aktualisiert alle Office 365-Kunden, einschließlich Exchange Online-Kunden, auf die neue Version von Office 365. Der E-Mail-Schutz von Exchange Online-Kunden wird auf Exchange Online Protection (EOP) aktualisiert. Auf der Wiki-Webseite der Office 365-Community finden Sie einige Themen mit hilfreichen Informationen für Exchange Online-Upgradekunden. Hierzu gehören die Folgenden:

Unter [Dienstupgrade für Exchange Online und Exchange Online Protection - Zugriff auf die FOPE-Verwaltungskonsole](#) werden Zugriffsänderungen in der FOPE-Verwaltungskonsole erläutert.

Unter [Funktionsunterschiede zwischen FOPE und EOP](#) werden Verhaltens- und Funktionsunterschiede zwischen FOPE und EOP beschrieben.

Unter [Dienstupgradebedingte Änderungen an Richtlinienregeln](#) werden Unterschiede zwischen FOPE-Richtlinienregeln in der aktuellen Version von Office 365 und Exchange-Transportregeln in der neuen Version erläutert.

Unter [Melden Sie sich bei FOPE Administration Center nach dem Dienst zu aktualisieren](#), die sich bei der FOPE-Verwaltungskonsole nach dem dienstupgrade anmelden erläutert, wenn Sie Ihre Einstellungen verweisen möchten.

## TIP

Wenn Sie weitere Informationen zu Dienstupgrades benötigen, ist [Office 365-Dienstupdates](#) die beste übergeordnete Informationsquelle.

# Informationen zur Exchange-Dokumentation

18.12.2018 • 3 minutes to read

Sie lesen eine Zusammenstellung von konzeptuellen Themen und Vorgehensweisen, die nach Thema oder von Microsoft Exchange verwendeten Technologien organisiert sind. Sie können jedes Thema im Inhaltsverzeichnis im linken Fensterbereich, über einen Link in einem anderen Hilfethema, in den Ergebnissen eines Suchvorgangs oder in Ihrer benutzerdefinierten Favoritenliste direkt aufrufen.

Weitere Informationen im Zusammenhang mit der Exchange-Dokumentation ist in der [Drittanbieter-Copyright-Hinweise](#).

## Abrufen der Exchange-Dokumentation

Das TechCenter [Exchange für IT-Experten](#) ist die primäre Anlaufstelle für ausführliche technische Informationen zu Microsoft Exchange. Über das TechCenter auf der Microsoft TechNet-Website können Sie auf die Exchange-Bibliothek und den Blog des Exchange-Teams zugreifen.

Wenn Sie Administrator einer hybriden Exchange-Bereitstellung oder einer Exchange Online-Bereitstellung sind, kann auch das TechCenter [Office 365 für IT-Experten](#) für Sie von Interesse sein.

Die [Exchange-Bibliothek](#) enthält die aktuelle Hilfedokumentation. Diese Dokumentation wird vom Exchange-Produktteam geprüft und genehmigt. Sobald neue Informationen, Probleme und Tipps zur Problembehandlung zur Verfügung stehen, wird die Dokumentation entsprechend aktualisiert.

Der [Blog des Exchange-Teams](#) enthält technische Artikel des Exchange-Teams sowie Produktankündigungen und -updates. Der Blog ist eine hervorragende Möglichkeit zur Interaktion mit dem Exchange-Team. Wir lesen Ihr Feedback und Ihre Kommentare, und reagieren darauf.

## Weitere Ressourcen

Suchen Sie zusätzlich zur Dokumentation nach weiteren Informationen? Dann sind diese Exchange-Ressourcen für Sie interessant:

- [Exchange Server-Downloads](#): Über diese Seite können Sie Service Packs, Add-Ins, Tools und Testsoftware herunterladen, mit denen sich Ihre Exchange-Organisation optimieren lässt.
- [Exchange Server-Foren](#) : Im Forum können Sie mit Benutzern und Mitgliedern des Exchange-Teams über Exchange diskutieren.
- [Exchange Server für Entwickler](#) : Hier finden Sie die Exchange-Entwicklerdokumentation.
- [Support für Microsoft Exchange Server](#): Auf dieser Seite finden Sie Supportressourcen für mehreren Versionen von Exchange.
- [Eingabehilfen für Personen mit Disabilities\\_E15](#) Dieses Thema enthält wichtige Informationen zu Features, Produkten und Diensten, mit denen Microsoft Exchange für Menschen mit Behinderung mehr zugegriffen werden kann.

# Barrierefreiheit in Exchange Online

18.12.2018 • 5 minutes to read

Microsoft möchte die bestmögliche Erfahrung für alle Kunden bereitstellen, auch für Kunden mit Behinderungen. Dieser Artikel enthält Links zu Artikeln, die für Personen geschrieben wurden, die die Sprachausgabe JAWS von Freedom Scientific oder Narrator verwenden, die in Windows 10 integrierte Sprachausgabe.

Die folgenden Artikel bieten Hilfestellung, die nur von bestimmten Tastenkombinationen und einer Sprachausgabe abhängig ist.

## Technischer Support für Personen mit Behinderungen

Microsoft bietet an vielen Orten auf der ganzen Welt kostenlose technischen Support für Personen mit Behinderungen. Wenn Sie eine Behinderung oder Fragen zur Barrierefreiheit haben, wenden Sie sich bitte an den [Microsoft Disability Answer Desk](#), um technische Unterstützung zu erhalten.

Das Supportteam am Disability Answer Desk ist in vielen gängigen Hilfstechnologien geschult und kann Unterstützung in englischer, spanischer, französischer und amerikanischer Gebärdensprache bieten. Besuchen Sie die Microsoft Disability Answer Desk-Website, um die Kontaktinformationen für Ihre Region zu finden.

## Hilfeinhalte für Barrierefreiheit für das Exchange Admin Center in Exchange Online

### Durchführen grundlegender Aufgaben

- [Eingabehilfen in der Exchange Admin center in Exchange Online](#)
- [Erste Schritte mit der Bildschirmsprachausgabe in der Exchange-Verwaltungskonsole in Exchange Online](#)
- [Tastenkombinationen Sie für die Exchange-Verwaltungskonsole in Exchange Online](#)
- [Verwenden Sie eine Bildschirmsprachausgabe So öffnen Sie die Exchange-Verwaltungskonsole in Exchange Online](#)
- [Verwenden Sie eine Bildschirmsprachausgabe zur Identifizierung der Administratorrolle in der Exchange-Verwaltungskonsole in Exchange Online](#)

### Arbeiten mit Postfächern

- [Verwenden Sie eine Bildschirmsprachausgabe zum Hinzufügen einer neuen gerätepostfach in der Exchange-Verwaltungskonsole in Exchange Online](#)
- [Verwenden Sie eine Bildschirmsprachausgabe zum Hinzufügen eines neuen raumpostfachs in der Exchange-Verwaltungskonsole in Exchange Online](#)
- [Verwenden Sie eine Bildschirmsprachausgabe, um ein neues freigegebenes Postfach in der Exchange-Verwaltungskonsole in Exchange Online hinzuzufügen](#)
- [Verwenden Sie eine Bildschirmsprachausgabe so bearbeiten Sie den Anzeigenamen des Postfachs in der Exchange-Verwaltungskonsole in Exchange Online](#)
- [Verwenden Sie eine Bildschirmsprachausgabe zum Archivieren von Postfachelemente in der Exchange-Verwaltungskonsole in Exchange Online](#)

### Arbeiten mit Verteilergruppen

- Verwenden Sie eine Bildschirmsprachausgabe zum Erstellen einer neuen Verteilergruppe in der Exchange-Verwaltungskonsole in Exchange Online
- Verwenden Sie eine Bildschirmsprachausgabe eine Verteilergruppe in der Exchange-Verwaltungskonsole in Exchange Online Mitglieder hinzufügen

### **Schutz vor Spam und Schadsoftware**

- Verwenden Sie eine Bildschirmsprachausgabe zum Verwalten von Anti-Malware Protection in der Exchange-Verwaltungskonsole in Exchange Online
- Verwenden einer Sprachausgabe zum Verwalten des Antispamschutzes in Exchange Online

### **Konfigurieren von Features**

- Verwenden Sie eine Bildschirmsprachausgabe zum Hinzufügen eines neuen e-Mail-Kontakts in der Exchange-Verwaltungskonsole in Exchange Online
- Verwenden Sie eine Bildschirmsprachausgabe mobilen Clients in der Exchange-Verwaltungskonsole in Exchange Online entwickelt
- Verwenden Sie eine Bildschirmsprachausgabe so konfigurieren Sie für die Zusammenarbeit in der Exchange-Verwaltungskonsole in Exchange Online
- Verwenden Sie eine Bildschirmsprachausgabe Definieren von Regeln, die Ver- oder Entschlüsse von e-Mail-Nachrichten in der Exchange-Verwaltungskonsole in Exchange Online
- Verwenden Sie eine Bildschirmsprachausgabe zum Konfigurieren von e-Mail-Fluss Regel Regeln in der Exchange-Verwaltungskonsole in Exchange Online

### **Nachverfolgen von Inhalten mit Überwachung und Ablaufverfolgung**

- Verwenden Sie eine Bildschirmsprachausgabe zur Ausführung der eines Überwachungsberichts in der Exchange-Verwaltungskonsole in Exchange Online
- So exportieren Sie eine Bildschirmsprachausgabe verwenden, und Überprüfen von Überwachungsprotokollen in der Exchange-Verwaltungskonsole in Exchange Online
- Verwenden Sie eine Bildschirmsprachausgabe verfolgen eine e-Mail-Nachricht in der Exchange-Verwaltungskonsole in Exchange Online

# Eingabehilfen in der Exchange Admin center in Exchange Online

18.12.2018 • 9 minutes to read

Die Exchange-Verwaltungskonsole (EAC) in Exchange Online umfasst Funktionen für Bedienungshilfen, die das Arbeiten mit Dateien für Personen mit eingeschränkter Beweglichkeit, einer Sehbehinderung oder anderen Einschränkungen erleichtern. Dies bedeutet, dass Sie Tastenkombinationen, eine Sprachausgabe oder eine Spracherkennung in der EAC verwenden können.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie die entsprechende Office 365-Abonnement und Admin Rolle in der Exchange-Verwaltungskonsole ausgeführt haben. Klicken Sie dann die Exchange-Verwaltungskonsole öffnen und die ersten Schritte. Weitere Informationen zu der Exchange-Verwaltungskonsole finden Sie unter [Exchange Admin center in Exchange Online](#).

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden.

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Pop-up-Fenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### **Bestätigen Ihres Office 365-Abonnementplans**

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung..](#)

### **Öffnen der EAC und Bestätigen Ihrer Administratorrolle**

[Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#) [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen eine Administratorrollengruppe, z. B. „Organisationsverwaltung“ zugewiesen hat. Sie können erkennen, dass Ihnen mindestens eine Administratorrollengruppe zugewiesen wurde, wenn Sie die Exchange-Verwaltungskonsole öffnen können. Erfahren Sie mehr über das [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Vertrautmachen mit der Benutzeroberfläche der Exchange-Verwaltungskonsole

Die Benutzeroberfläche der Exchange-Verwaltungskonsole ist in Ihrem Webbrowser als Teil von Exchange Online enthalten. In diesem Fenster wird „Office 365 Admin“ in der Titelleiste angezeigt. Am linken Rand der

Titelleiste befindet sich das Office 365 App-Startfeld, das die Liste von Microsoft-Diensten und Office Online-Anwendungen enthält, einschließlich E-Mail (Outlook.com), Excel Online, OneNote und vieles mehr. Auf der rechten Seite der Titelleiste befinden sich Befehle zum Abrufen von Benachrichtigungen, zum Verwalten der Optionen, für Hilfe und zum Abmelden.

Unter dem Titel wird häufig verwendete Hyperlinks, den Namen, die "Exchange-Verwaltungskonsole". Im linken Bereich enthält Informationen über zwölf Exchange administrative Kategorien, beispielsweise **Dashboard**, **Berechtigungen** und **e-Mail-Fluss**. Dashboard wird standardmäßig den Fokus besitzt.

Die im linken Bereich ausgewählte Verwaltungskategorie hat Auswirkungen auf den Inhalt des Hauptfensters rechts davon. Wenn Sie z. B. **Dashboard** im linken Bereich auswählen, werden alle Verwaltungskategorien in der Listenansicht im Hauptfenster zusammen mit ihren Unterkategorien angezeigt. Wenn Sie **Empfänger** im linken Bereich auswählen, wird eine Liste aller Benutzerpostfachnamen und -adressen in der Listenansicht im Hauptfenster angezeigt.

Wenn Sie ein Element in der Listenansicht im Hauptfenster auswählen, wird häufig eine Detailansicht zu diesem Element im rechten Bereich angezeigt. Wenn Sie beispielsweise die Verwaltungskategorie **Berechtigungen** im linken Bereich auswählen, wird in der Listenansicht im Hauptfenster eine Liste von Administratorrollen angezeigt, und der Fokus liegt auf der ersten Administratorrolle. **Complianceverwaltung**. Informationen zur Complianceverwaltung werden in der rechten Detailansicht angezeigt.

Am oberen Rand der Listenansicht des Hauptfensters wird eine Reihe von Menüregisterkarten angezeigt, in denen Unterkategorien für die Verwaltungskategorie mit dem Fokus aufgeführt sind. Wenn Sie beispielsweise **Schutz** im linken Bereich auswählen, werden Menüregisterkarten wie **Schadsoftwarefilter** und **Spamfilter** am oberen Rand im Hauptfenster angezeigt. Außerdem wird manchmal eine Symbolleiste angezeigt, die Befehle wie **Neu**, **Bearbeiten**, **Löschen** und **Aktualisieren** enthält.

Unten im Hauptfenster befindet sich eine Statusleiste, die angibt, wie viele Datensätze ausgewählt sind.

## Verwenden von Sprachausgabe und Tastenkombinationen

Die Exchange-Verwaltungskonsole enthält Namen, die von einer Sprachausgabe gelesen werden können, während Sie in der Anwendung arbeiten. Sie können Sprachausgabe, die integrierte Sprachausgabe in Windows, oder eine Sprachausgabe von einem Drittanbieter verwenden, z. B. [JAWS](#). Weitere Informationen finden Sie unter [Erste Schritte bei der Verwendung einer Sprachausgabe im Exchange Admin Center](#). Sie können auch die [Windows-Spracherkennung](#) oder ein Spracherkennungstool von einem Drittanbieter verwenden, um der Exchange-Verwaltungskonsole Sprachbefehle zu erteilen.

Um in der Exchange-Verwaltungskonsole zu navigieren und die Gruppen von Bildschirmelementen zu durchlaufen, drücken Sie STRG+F6 (vorwärts) oder STRG+UMSCHALT+F6 (rückwärts). Um Bildschirmelemente, einschließlich Elementlisten, zu durchlaufen, drücken Sie die TAB-TASTE (vorwärts) oder UMSCHALT+TAB (rückwärts). Um ein Element auszuwählen, drücken Sie die EINGABETASTE. Zum Navigieren in Menüs oder Listen, drücken Sie die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE und dann die EINGABETASTE, um eine Auswahl vorzunehmen. Um ein Menü oder einen Modus zu beenden, drücken Sie ESC. Weitere Informationen finden Sie unter [Tastenkombinationen in der Exchange-Verwaltungskonsole](#).

Während Sie die Bereiche der Exchange-Verwaltungskonsole durchlaufen, stellt die Sprachausgabe Informationen zu dem Bereich bereit, der den Fokus hat, z. B. der linke Funktionsbereich (Sie hören „Primäre Navigation, Link“), Menüregisterkarten, die Symbolleiste, die Listenansicht im Hauptfenster (Sie hören „Sekundäre Navigation“) oder die Detailansicht im rechten Bereich (in Sprachausgabe hören Sie den Inhalt des Bereichs).

## Technischer Support für Kunden mit Behinderungen

Microsoft möchte die bestmögliche Erfahrung für alle Kunden bereitstellen. Wenn Sie eine Behinderung oder Fragen zur Barrierefreiheit haben, wenden Sie sich bitte an den [Microsoft Disability Answer Desk](#), um technische Unterstützung zu erhalten.

Das Supportteam am Disability Answer Desk ist in vielen gängigen Hilfstechnologien geschult und kann Unterstützung in englischer, spanischer, französischer und amerikanischer Gebärdensprache bieten. Besuchen Sie die [Microsoft Disability Answer Desk](#)-Website, um die Kontaktinformationen für Ihre Region zu finden.

# Erste Schritte mit der Bildschirmsprachausgabe in der Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 9 minutes to read

Sie können eine Sprachausgabe mit der Exchange-Verwaltungskonsole (EAC) in Exchange Online verwenden, um Verwaltungsaufgaben auszuführen. Die Exchange-Verwaltungskonsole arbeitet mit Sprachausgabe, der integrierten Sprachausgabe in Windows, oder JAWS, einer Sprachausgabe eines Drittanbieters. Diese Sprachausgaben konvertieren Text in Sprache, um den Inhalt des Fensters der Exchange-Verwaltungskonsole zu lesen.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie die entsprechende Office 365-Abonnement und Admin Rolle in der Exchange-Verwaltungskonsole ausgeführt haben. Klicken Sie dann die Exchange-Verwaltungskonsole öffnen und die ersten Schritte. Weitere Informationen zu der Exchange-Verwaltungskonsole finden Sie unter [Exchange Admin center in Exchange Online](#).

### Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Pop-up-Fenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### Bestätigen Ihres Office 365-Abonnementplans

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### Öffnen der EAC und Bestätigen Ihrer Administratorrolle

[Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#) [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen eine Administratorrollengruppen, z. B. „Organisationsverwaltung“ zugewiesen hat. Sie können erkennen, dass Ihnen mindestens eine Administratorrollengruppe zugewiesen wurde, wenn Sie die Exchange-Verwaltungskonsole öffnen können. Erfahren Sie mehr über das [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Arbeiten mit einer Sprachausgabe

Die Exchange-Verwaltungskonsole arbeitet u. a. mit Sprachausgabe- und JAWS-Sprachausgaben. Diese Sprachausgaben konvertieren Text in Sprache und lesen Ihnen Befehle, Speicherorte, Alternativtext bei Bildern sowie die Inhalte der EAC-Bildschirme und Pop-up-Fenster vor.

- Um Sprachausgabe auf einem PC zu aktivieren oder zu deaktivieren, drücken Sie in Windows die Windows-Logotaste und die EINGABETASTE.
- Um Sprachausgabe auf einem Tablet zu aktivieren oder zu deaktivieren, drücken Sie die Windows-Logotaste + Lautstärke höher.
- Wenn Sprachausgabe ein neu geöffnetes Fenster nicht öffnet, drücken Sie F5. Durch Aktualisieren des Browserfensters wird der Fokus zurückgesetzt, und Sprachausgabe liest das Fenster.
- Wenn die Sprachausgabe mit dem Lesen fertig ist, drücken Sie ALT+TAB, um das aktuelle Fenster zu verlassen, und drücken Sie dann erneut ALT+TAB, um zu dem Fenster zurückzukehren. Dadurch wird der Fokus auf das aktuelle Fenster zurückgesetzt, damit die Sprachausgabe das Fenster korrekt liest.

Weitere Informationen zu Sprachausgabe finden Sie unter [Ausgeben von Text über die Sprachausgabe](#). Weitere Informationen zu JAWS finden Sie in der [Dokumentation zur JAWS-Sprachausgabe](#).

## Mehr Aufgaben mit der Exchange-Verwaltungskonsole und einer Sprachausgabe erledigen

Erforschen Sie bestimmte Vorgänge, die die Sprachausgabe zum Arbeiten in der EAC verwenden.

### **Erste Schritte mit der EAC**

- [Eingabehilfen in der Exchange Admin center in Exchange Online](#)
- [Tastenkombinationen in der Exchange Admin center in Exchange Online](#)
- [Verwenden Sie eine Bildschirmsprachausgabe So öffnen Sie die Exchange-Verwaltungskonsole in Exchange Online](#)

### **Arbeiten mit Postfächern und Empfängern**

- [Verwenden Sie eine Bildschirmsprachausgabe so bearbeiten Sie den Anzeigenamen des Postfachs in der Exchange-Verwaltungskonsole in Exchange Online](#)
- [Verwenden Sie eine Bildschirmsprachausgabe zum Hinzufügen eines neuen e-Mail-Kontakts in der Exchange-Verwaltungskonsole in Exchange Online](#)
- [Verwenden Sie eine Bildschirmsprachausgabe zum Hinzufügen eines neuen raumpostfachs in der Exchange-Verwaltungskonsole in Exchange Online](#)
- [Verwenden Sie eine Bildschirmsprachausgabe zum Hinzufügen einer neuen gerätepostfach in der Exchange-Verwaltungskonsole in Exchange Online](#)

### **Verwalten von Verteilergruppen Zusammenarbeit**

- [Verwenden Sie eine Bildschirmsprachausgabe zum Erstellen einer neuen Verteilergruppe in der Exchange-Verwaltungskonsole in Exchange Online](#)
- [Verwenden Sie eine Bildschirmsprachausgabe eine Verteilergruppe in der Exchange-Verwaltungskonsole in Exchange Online Mitglieder hinzu](#)
- [Verwenden einer Sprachausgabe zum Hinzufügen eines neuen freigegebenen Postfachs im Exchange Admin Center 2016](#)
- [Verwenden Sie eine Bildschirmsprachausgabe so konfigurieren Sie für die Zusammenarbeit in der Exchange-Verwaltungskonsole in Exchange Online](#)

### **Verwalten der Nachrichtenflusses und der Sicherheit**

- [Verwenden Sie eine Bildschirmsprachausgabe zum Konfigurieren von e-Mail-Flussregeln in der Exchange-Verwaltungskonsole in Exchange Online](#)

- Verwenden einer Sprachausgabe zum Definieren von Regeln, die E-Mail-Nachrichten im Exchange Admin Center 2016 verschlüsseln oder entschlüsseln
- Verwenden einer Sprachausgabe zum Verwalten des Antispamschutzes in Exchange Online
- Verwenden Sie eine Bildschirmsprachausgabe zum Verwalten von Anti-Malware Protection in der Exchange-Verwaltungskonsole in Exchange Online
- Verwenden Sie eine Bildschirmsprachausgabe mobilen Clients in der Exchange-Verwaltungskonsole in Exchange Online entwickelt

#### **Einrichten von Berechtigungen und Compliance**

- Verwenden Sie eine Bildschirmsprachausgabe zur Identifizierung der Administratorrolle in der Exchange-Verwaltungskonsole in Exchange Online
- Verwenden Sie eine Bildschirmsprachausgabe zur Ausführung der eines Überwachungsberichts in der Exchange-Verwaltungskonsole in Exchange Online
- Verwenden Sie eine Bildschirmsprachausgabe verfolgen eine e-Mail-Nachricht in der Exchange-Verwaltungskonsole in Exchange Online
- So exportieren Sie eine Bildschirmsprachausgabe verwenden, und Überprüfen von Überwachungsprotokollen in der Exchange-Verwaltungskonsole in Exchange Online

## Technischer Support für Kunden mit Behinderungen

Microsoft möchte die bestmögliche Erfahrung für alle Kunden bereitstellen. Wenn Sie eine Behinderung oder Fragen zur Barrierefreiheit haben, wenden Sie sich bitte an den [Microsoft Disability Answer Desk](#), um technische Unterstützung zu erhalten.

Das Supportteam am Disability Answer Desk ist in vielen gängigen Hilfstechnologien geschult und kann Unterstützung in englischer, spanischer, französischer und amerikanischer Gebärdensprache bieten. Besuchen Sie die [Microsoft Disability Answer Desk](#)-Website, um die Kontaktinformationen für Ihre Region zu finden.

# Tastenkombinationen Sie für die Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 5 minutes to read

Viele Benutzer feststellen, dass Tastenkombinationen für die Exchange-Verwaltungskonsole (EAC) in Exchange Online effizienter arbeiten helfen. Für Benutzer mit eingeschränkter Mobilität oder Vision sind Tastenkombinationen eine wichtige Alternative zur Verwendung der Maus.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie die entsprechende Office 365-Aboonnement und Admin Rolle in der Exchange-Verwaltungskonsole ausgeführt haben. Klicken Sie dann die Exchange-Verwaltungskonsole öffnen und die ersten Schritte. Weitere Informationen zu der Exchange-Verwaltungskonsole finden Sie unter [Exchange Admin center in Exchange Online](#).

### Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Pop-up-Fenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### Bestätigen Ihres Office 365-Aboonnementplans

Exchange Online ist in Office 365 Business- und Enterprise-Aboonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Aboonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

## Verwenden von Tastenkombinationen

### Hinweise:

- Die Tastenkombinationen in diesem Thema beziehen sich auf das amerikanische Tastaturlayout. Die Tasten anderer Tastaturlayouts stimmen möglicherweise nicht genau mit den Tasten auf einer deutschen Tastatur überein.
- Wenn für eine Tastenkombination zwei oder mehr Tasten gleichzeitig gedrückt werden müssen, werden die Tasten in diesem Thema durch ein Pluszeichen (+) getrennt. Wenn Sie eine Taste sofort nach einer anderen drücken müssen, sind die Tasten durch ein Komma (,) getrennt.
- Die Exchange-Verwaltungskonsole wird in Ihrem Webbrowser ausgeführt, es werden daher keine Zugriffstasten oder Zugriffstasteninfos verwendet. Durch Drücken von Alt verschiebt sich der Fokus beispielsweise auf die Menüleiste des Browsers, und vertraute Tastenkombinationen, wie z. B. STRG + P (Drucken) und F1 (Hilfe), führen Browserbefehle anstelle von EAC-Befehlen aus.

Um die Bereiche der Exchange-Verwaltungskonsole auf dem Bildschirm zu durchlaufen, drücken Sie STRG + F6 (vorwärts) oder STRG + UMSCHALT + F6 (rückwärts). Die Reihenfolge für den STRG + F6-Navigationszyklus ist:

- Linker Featurebereich oder primäre Navigationslinks
- Menüleiste oder sekundäre Navigationslinks
- Symbolleiste
- Listenansicht des Hauptfensters
- Detailansicht im rechten Bereich

- App-Startfeld für Office 365

## Navigieren in der Exchange-Verwaltungskonsole

ZWECK	TASTENKOMBINATION
Wechseln zwischen Bereichen	STRG + F6 oder STRG + UMSCHALT + F6
Wechseln zwischen den Bereichen oder einzelnen Steuerelementen	Nach-oben-Taste oder die nach-unten-Taste <b>Hinweis:</b> Tab und Umschalt + Tab werden nicht unterstützt, um zwischen Exchange-Verwaltungskonsole Menüelementen zu verschieben.
Wechseln zwischen Elementen in einer Liste	NACH-OBEN-TASTE oder NACH-UNTEN-TASTE, POS1-TASTE, ENDE-TASTE, BILD-AUF oder BILD-AB <b>Hinweis:</b> Sie können auch die nach-oben-Taste, die nach-unten-Taste, nach-links oder rechts-Taste verwenden, um zwischen Optionsschaltflächen oder in einer Gruppe von Kontrollkästchen zu verschieben.
Auswählen eines Elements	EINGABETASTE oder LEERTASTE
Beenden eines Menüs oder Modus	ESC

# Verwenden einer Sprachausgabe zum Hinzufügen eines neuen Gerätewechselkastens im Exchange Admin Center

18.12.2018 • 7 minutes to read

Erstellen von Postfächern in der Exchange-Verwaltungskonsole (EAC) für jeden Drucker, Projektor oder ein anderes Gerät, das mit dem Unternehmensnetzwerk mithilfe der Tastatur und alle Bildschirmsprachausgabe angefügt ist.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zur Verwendung der Exchange-Verwaltungskonsole verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Pop-up-Fenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### **Bestätigen Ihres Office 365-Abonnementplans**

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### **Öffnen der EAC und Bestätigen Ihrer Administratorrolle**

Zum Hinzufügen eines neuen Gerätewechselkastens [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Office 365-Administrator für Ihnen die Administratorrollengruppen „Organisationsverwaltung“ zugewiesen hat. Weitere Informationen zu [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#)

## Hinzufügen eines neuen Gerätewechselkastens

1. Navigieren Sie auf der EAC-Dashboardseite (Startseite) zum Textbereich, und drücken Sie STRG + F6. Sie hören „Willkommen“.
2. Drücken Sie die TAB-Taste, bis Sie „Ressourcen“, der zweite Link nach „Empfänger“.
3. Drücken Sie die EINGABETASTE, um zur Registerkarte **Ressourcen** auf der Seite **Postfächer** zu gelangen. Der Fokus befindet sich auf der Registerkarte **Ressourcen**.

4. Wenn Sie auf die Schaltfläche **neu** im Bereich **Ressourcen** erhalten möchten, drücken Sie STRG + F6. Sie hören "neue Schaltfläche..."
5. Zum Öffnen des Untermenüs **Neues Element** drücken Sie die LEERTASTE.
6. Um die Option **Equipment Mailbox** zu wechseln, drücken Sie die nach-unten-Taste. Sie hören "Gerätepostfach." (Die Sprachausgabe, die besagt, "Leerzeile".)
7. Zum Öffnen des Formulars **Neues Gerätename** in einem Popupfenster, drücken Sie die EINGABETASTE. Sie hören die URL des Popupfensters und schließlich „Gerätename“. Der Fokus befindet sich auf dem Feld **Gerätename**.

**TIP**

Es gibt nur drei Felder in diesem Formular: **Gerätename**, **E-Mail-Adresse** und **Domäne**. Alle drei sind erforderlich.

8. Geben Sie den Namen des Geräts, und drücken Sie die Tab-Taste, um in das Feld **E-Mail-Adresse** zu verschieben. Sie hören "E-Mail-Adresse..."

**TIP**

Dieser Name wird im Outlook-Adressbuch der Benutzer angezeigt. Damit Benutzer Räume leichter finden können, verwenden Sie eine konsistente Namenskonvention innerhalb Ihrer Organisation.

9. Die E-Mail-Adresse ist ebenfalls erforderlich. Geben Sie den ersten Teil der E-Mail-Adresse (vor dem @-Zeichen) ein, und drücken Sie die TAB-Taste, um zur Dropdownliste der Domäne zu gelangen. Sie hören die Option für die ausgewählte Domäne.
10. Wenn die Standardauswahl im Dropdownmenü der Domäne nicht die gewünschte Domäne ist, drücken Sie die NACH-UNTEN-TASTE, um auf andere verfügbare Domänen zuzugreifen. Während Sie sich durch die verfügbaren Optionen bewegen, hören Sie den Domänennamen und das Suffix. Wenn Sie die gewünschte Domäne gefunden haben, drücken Sie die EINGABETASTE, um sie auszuwählen.

**TIP**

Sie können keine Werte in das Domänenfeld eingeben. Es handelt sich um eine vorkonfigurierte Dropdownliste. Wenden Sie sich an Ihren Office-Administrator, um dieser Dropdownliste Domänen hinzuzufügen.

11. Gehen Sie auf die Schaltfläche **Speichern**, drücken Sie die Tab-Taste. Sie hören "speichern..."
12. Drücken Sie die EINGABETASTE. Dadurch wird das Postfach, das Sie mit den Werten zugewiesen wurde, und das Popup-Fenster wird geschlossen, erstellt Sie zur Liste **Ressourcen** auf der Registerkarte **Ressourcen** zurückgegeben gespeichert. Der Schwerpunkt liegt auf die Schaltfläche **Neues Postfach**. Sie hören 'neues Postfach...'.

**TIP**

Es kann einige Minuten dauern, bis das neue Postfach gespeichert ist und das Popupfenster geschlossen wird. Während dieser Wartezeit hören Sie kein weiteres Feedback.

Wenn Sie weitere Informationen zu Ihrem neuen Raumpostfach hinzufügen möchten, erhalten Sie unter „Verwenden einer Sprachausgabe zur Verwendung von Postfacheigenschaften und -Optionen in EAC“ auf Exchange Online Informationen zu allen verfügbaren Optionen.

## Technischer Support für Kunden mit Behinderungen

Microsoft möchte die bestmögliche Erfahrung für alle Kunden bereitstellen. Wenn Sie eine Behinderung oder Fragen zur Barrierefreiheit haben, wenden Sie sich bitte an den [Microsoft Disability Answer Desk](#), um technische Unterstützung zu erhalten.

Das Supportteam am Disability Answer Desk ist in vielen gängigen Hilfstechnologien geschult und kann Unterstützung in englischer, spanischer, französischer und amerikanischer Gebärdensprache bieten. Besuchen Sie die [Microsoft Disability Answer Desk](#)-Website, um die Kontaktinformationen für Ihre Region zu finden.

# Verwenden Sie eine Bildschirmsprachausgabe zum Hinzufügen eines neuen e-Mail-Kontakts in der Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 6 minutes to read

Eine Bildschirmsprachausgabe mit Exchange Online verwenden, können die Exchange-Verwaltungskonsole (EAC) zum Einrichten der *e-Mail-Kontakts* – ein e-Mail-aktivierte Directory Service-Objekt mit Informationen zu einer Person oder Entität, die außerhalb Ihrer Exchange Online Organisation. Jede e-Mail-Kontakt verfügt über eine externe e-Mail-Adresse. Weitere Informationen zu e-Mail-Kontakte finden Sie im TechNet-Artikel [Empfänger](#).

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zur Verwendung der Exchange-Verwaltungskonsole verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Popupfenstern, daher sollten Sie in Ihrem Browser unbedingt [Popupfenster für Office 365 aktivieren](#).

### **Bestätigen Ihres Office 365-Abonnementplans**

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten. Die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### **Öffnen von EAC und Bestätigen Ihrer Administratorrolle**

Zum Hinzufügen eines neuen E-Mail-Kontakts [use a screen reader to open the EAC](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorgruppen [Organisationsverwaltung](#) und [Empfängerverwaltung](#) zugewiesen hat. Erfahren Sie mehr über das [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Erstellen eines E-Mail-Kontakts mithilfe der Exchange-Verwaltungskonsole

1. Drücken Sie in der Exchange-Verwaltungskonsole die TAB-TASTE, bis im primären Navigationsbereich **Empfänger** angezeigt wird. Sie hören „Empfänger, primäre Navigation“. Drücken Sie die EINGABETASTE.
2. Drücken Sie STRG+F6, um den Fokus auf die Menüleiste zu verschieben. Sie hören „Postfächer, sekundäre

Navigation".

3. Drücken Sie die NACH-LINKS-TASTE, bis Sie „Kontakte, sekundäre Navigation“ hören, und drücken Sie dann die EINGABETASTE. Eine Tabelle mit E-Mail-Kontakten wird angezeigt.
4. Um den Fokus auf die Menüleiste für Kontakte zu verschieben, drücken Sie STRG+F6, bis Sie hören „Schaltflächenmenü ,Neu“.
5. Drücken Sie die LEERTASTE, und drücken Sie dann die NACH-UNTEN-TASTE, bis Sie hören „E-Mail-Kontakt“. Drücken Sie dann die EINGABETASTE. Das Fenster **Neuer E-Mail-Kontakt** wird angezeigt.

**Hinweis:** In die Sprachausgabe, wenn die Menüoptionen für die Schaltfläche **neu** nicht gelesen werden, Sie hören "Leere Zeile". **E-Mail-Kontakts** ist die erste Option. **E-Mail-Benutzer** wird die zweite Option.

Drücken Sie F5, wenn Sie **e-Mail-Kontakts**, auswählen, wenn die Sprachausgabe announce nicht den Namen des Fensters **neue e-Mail-Kontakts** oder das Feld **Vorname** zum Aktualisieren des Fensters, und stellen Sie den Fokus wieder her.

6. Wechseln Sie mit der TAB-TASTE zu den folgenden Feldern, und füllen Sie die Kontaktinformationen aus:

**Hinweis:** erforderliche Felder sind mit einem Sternchen gekennzeichnet. In der Bildschirmsprachausgabe hören Sie "Stern" oder "Stern" vor der Beschriftung. Beispielsweise hören im Feld **Anzeigename** erforderlich Sie "Stern Anzeigenamen" oder "Sternchen anzeigen..."

- **Vorname.** Geben Sie den Vornamen des Kontakts ein.
  - **Initialen.** Geben Sie die Initialen des Kontakts.
  - **Nachname:** Geben Sie den Namen des Kontakts letzten.
  - **\*Anzeigename.** Um den Standardwert zu ändern, geben Sie den Namen ein, der im Exchange Admin Center und im Adressbuch Ihrer Organisation in der Liste **Kontakte** angezeigt werden soll. Standardmäßig verwendet Exchange die Namen, die Sie in den Feldern **Vorname**, **Initialen** und **Nachname** eingegeben haben. Der Name darf nicht länger als 64 Zeichen sein.
  - **\*Alias.** Geben Sie einen eindeutigen Alias (maximal 64 Zeichen) für den Kontakt ein.
  - **\*Externe E-Mail-Adresse.** Geben Sie die E-Mail-Adresse des Kontakts außerhalb Ihrer Organisation ein. An diesen Kontakt gesendete E-Mails werden an diese E-Mail-Adresse weitergeleitet.
7. Wenn Sie fertig sind, wechseln Sie mit der TAB-TASTE zur Schaltfläche **Speichern**. Das Fenster **Neuer E-Mail-Kontakt** wird geschlossen, und der Kontakt wird der Tabelle im Fenster **Kontakte** hinzugefügt.

# Verwenden Sie eine Bildschirmsprachausgabe zum Hinzufügen eines neuen raumpostfachs in der Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 7 minutes to read

Hinzufügen eines Postfachs für Konferenzräume in der Exchange-Verwaltungskonsole (EAC) mithilfe von Tastenkombinationen und der Sprachausgabe.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zur Verwendung der Exchange-Verwaltungskonsole verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Popupfenstern, daher sollten Sie in Ihrem Browser unbedingt [Popupfenster für Office 365 aktivieren](#).

### **Bestätigen Ihres Office 365-Abonnementplans**

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### **Öffnen von EAC und Bestätigen Ihrer Administratorrolle**

Zum Hinzufügen eines neuen Raumpostfachs [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Office 365-Administrator für Ihnen die Administratorrollengruppen „Organisationsverwaltung“ zugewiesen hat. Erfahren Sie mehr über das [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Hinzufügen eines neuen Raumpostfachs

1. Navigieren Sie auf der EAC-Dashboardseite (Startseite) zum Textbereich, und drücken Sie STRG + F6. Sie hören „Willkommen“.
2. Drücken Sie die TAB-Taste, bis Sie „Ressourcen“, der zweite Link nach „Empfänger“.
3. Drücken Sie die EINGABETASTE, um zur Registerkarte **Ressourcen** auf der Seite **Postfächer** zu gelangen. Der Fokus befindet sich auf der Registerkarte **Ressourcen**.
4. Wenn Sie auf die Schaltfläche **neu** , klicken Sie im Bereich **Ressourcen** erhalten möchten, drücken Sie

STRG + F6. Sie hören "neue Schaltfläche..."

5. Zum Öffnen des Untermenüs **Neues Element** drücken Sie die LEERTASTE.
6. Um die Option **Raumpostfach** zu wechseln, drücken Sie die nach-unten-Taste. Sie hören "Raumpostfach." (Die Sprachausgabe, die besagt, "Leerzeile").
7. Zum Öffnen des Formulars **Neues Raumpostfach** in einem Popupfenster, drücken Sie die EINGABETASTE. Sie hören die URL des Popupfensters und schließlich „Raumname“. Der Fokus befindet sich auf dem Feld **Raumname**. Dies ist ein Pflichtfeld.
8. Geben Sie den Namen des Raums ein, und drücken Sie die TAB-Taste, um zum Feld **E-Mail-Adresse** zu gelangen.

**TIP**

Dieser Name wird im Outlook-Adressbuch der Benutzer angezeigt. Damit Benutzer Räume leichter finden können, verwenden Sie eine konsistente Namenskonvention innerhalb Ihrer Organisation.

9. Die E-Mail-Adresse ist ebenfalls erforderlich. Geben Sie den ersten Teil der E-Mail-Adresse (vor dem @-Zeichen) ein, und drücken Sie die TAB-Taste, um zur Dropdownliste der Domäne zu gelangen. Sie hören die Option für die ausgewählte Domäne.
10. Wenn die Standardauswahl im Dropdownmenü der Domäne nicht die gewünschte Domäne ist, drücken Sie die NACH-UNTEN-TASTE, um auf andere verfügbare Domänen zuzugreifen. Während Sie sich durch die verfügbaren Optionen bewegen, hören Sie den Domänennamen und das Suffix. Wenn Sie die gewünschte Domäne gefunden haben, drücken Sie die EINGABETASTE, um sie auszuwählen.

**TIP**

Sie können keine Werte in das Domänenfeld eingeben. Es handelt sich um eine vorkonfigurierte Dropdownliste. Wenden Sie sich an Ihren Office-Administrator, um dieser Dropdownliste Domänen hinzuzufügen.

11. Gehen Sie auf die Schaltfläche **Speichern**, drücken Sie die Tab-Taste. Sie hören "speichern..."
12. Drücken Sie die EINGABETASTE. Dadurch wird das Postfach, das Sie mit den Werten zugewiesen wurde, und das Popup-Fenster wird geschlossen, erstellt Sie zur Liste **Ressourcen** auf der Registerkarte **Ressourcen** zurückgegeben gespeichert. Der Schwerpunkt liegt auf die Schaltfläche **Neues Postfach**. Sie hören 'neues Postfach...'.

**TIP**

Es kann einige Minuten dauern, bis das neue Postfach gespeichert ist und das Popupfenster geschlossen wird. Während dieser Wartezeit hören Sie kein weiteres Feedback.

Wenn Sie weitere Informationen zu Ihrem neuen Raumpostfach hinzufügen möchten, erhalten Sie unter „Verwenden einer Sprachausgabe zur Verwendung von Postfacheigenschaften und -Optionen in EAC“ auf Exchange Online Informationen zu allen verfügbaren Optionen.

## Technischer Support für Kunden mit Behinderungen

Microsoft möchte die bestmögliche Erfahrung für alle Kunden bereitstellen. Wenn Sie eine Behinderung oder Fragen zur Barrierefreiheit haben, wenden Sie sich bitte an den [Microsoft Disability Answer Desk](#), um technische Unterstützung zu erhalten.

Das Supportteam am Disability Answer Desk ist in vielen gängigen Hilfstechnologien geschult und kann Unterstützung in englischer, spanischer, französischer und amerikanischer Gebärdensprache bieten. Besuchen Sie die [Microsoft Disability Answer Desk](#)-Website, um die Kontaktinformationen für Ihre Region zu finden.

# Verwenden Sie eine Bildschirmsprachausgabe, um ein neues freigegebenes Postfach in der Exchange-Verwaltungskonsole in Exchange Online hinzuzufügen

18.12.2018 • 7 minutes to read

Sie können die Sprachausgabe verwenden, um ein freigegebenes Postfach in der Exchange-Verwaltungskonsole (EAC) in Exchange Online zu erstellen. Freigegebene Postfächer vereinfachen einer Gruppe von Personen in Ihrer Organisation das Überwachen und Senden von E-Mails von einem gemeinsamen Konto aus, wie z. B. "info@contoso.com" oder "support@contoso.com"). Wenn eine Person in der Gruppe auf eine an das freigegebene Postfach gesendete Nachricht antwortet, hat es den Anschein, als stamme die E-Mail vom freigegebenen Postfach und nicht von dem bestimmten Benutzer. [Erfahren Sie mehr über freigegebene Postfächer.](#)

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abo und die Administratorrolle zur Verwendung der Exchange-Verwaltungskonsole verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole.](#)

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen.](#)

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Pop-up-Fenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren.](#)

### **Bestätigen Ihres Office 365-Abo**

Exchange Online ist in Office 365 Business- und Enterprise-Abo-Plänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abo finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung.](#)

### **Öffnen von EAC und Bestätigen Ihrer Administratorrolle**

Zum Hinzufügen eines neuen freigegebenen Postfachs [Use a screen reader to open the Exchange admin center](#), und überprüfen Sie, ob Ihr globaler Office 365-Administrator für Ihnen die Administratorrollengruppen „Organisationsverwaltung“ und „Empfängerverwaltung“ zugewiesen hat. Erfahren Sie mehr über das [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center.](#)

## Erstellen eines freigegebenen Postfachs

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis Sie zu **Empfänger** gelangen, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen. Sie hören „Bereich ‚Postfächer‘, sekundäre Navigation“ (In der Sprachausgabe hören Sie „Postfächer, sekundärer Navigationslink“.)
4. Drücken Sie die TAB-Taste, bis Sie zu **Freigegeben** gelangen. Sie hören „Freigegeben, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.
5. Drücken Sie STRG+F6, um zur Symbolleiste zu gelangen. Sie hören „Schaltfläche ‚Neu‘“. Drücken Sie die EINGABETASTE.
6. Im dem Dialogfeld **Freigegebenes Postfach**, das geöffnet wird, hat das Textfeld **Anzeigename** den Fokus, und Sie hören „Text eingeben“. (In der Sprachausgabe hören Sie „Anzeigename, bearbeiten“). Geben Sie den Anzeigenamen für das freigegebene Postfach ein, das Sie erstellen.
7. Drücken Sie die TAB-Taste bis zum Textfeld **E-Mail-Adresse**, und geben Sie die E-Mail-Adresse für das neue freigegebene Postfach an.
8. Um die Benutzer auszuwählen, die E-Mails von diesem neuen freigegebenen Postfach anzeigen und senden können, drücken Sie die TAB-TASTE bis zur Schaltfläche **Hinzufügen**, und wählen Sie sie aus.
9. Wenn das Dialogfeld **Freigegebenen Postfach-Benutzer auswählen** wird geöffnet, in das Feld **Suchen** den Fokus besitzt. Sie hören „Filter oder Suche bearbeiten“. Geben Sie alle oder einen Teil des Namens des ersten Benutzers, den Sie für das freigegebene Postfach hinzufügen, und drücken dann zum Suchen des Namens eingeben möchten.
10. Drücken Sie viermal die TAB-TASTE, bis Sie den Namen des Benutzers in der Liste der Suchergebnisse hören. Der Name ist ausgewählt.
11. Drücken Sie die TAB-TASTE, bis die Schaltfläche **Hinzufügen** den Fokus hat, und drücken Sie die EINGABETASTE oder die LEERTASTE. Der ausgewählte Name wird der Liste der Benutzer für das neue freigegebene Postfach hinzugefügt.
12. Um einen zweiten Benutzer hinzuzufügen, drücken Sie mehrere Mal die TAB-TASTE, bis Sie „Filter oder Suche bearbeiten“ hören. Geben Sie ganz oder teilweise den Namen des nächsten Benutzers ein, den Sie hinzufügen möchten, und drücken die EINGABETASTE. Wiederholen Sie die Schritte 10 und 11. Tun Sie dies für alle Benutzer, die Sie dem neuen freigegebenen Postfach hinzufügen möchten.
13. Wenn Sie mit dem Hinzufügen von Benutzern fertig sind, wechseln Sie mit der TAB-TASTE zur Schaltfläche **OK**, und drücken Sie die EINGABETASTE. Das Dialogfeld **Freigegebenes Postfach** hat wieder den Fokus, und die ausgewählten Benutzer werden im Feld **Benutzer von freigegebenen Postfächern** aufgeführt.
14. Drücken Sie die TAB-TASTE, bis die Schaltfläche **Speichern** den Fokus hat, und drücken Sie die EINGABETASTE. Eine Warnung sagt „Bitte warten“. Nachdem das freigegebene Postfach erstellt wurde, hören Sie eine weitere Warnung, die besagt, dass das Postfach in ca. 15 Minuten verfügbar ist.
15. Drücken Sie, während der Fokus auf der Schaltfläche **OK** liegt, die EINGABETASTE. Der Anzeigename und die E-Mail-Adresse des neuen freigegebenen Postfachs sind in der Listenansicht **Freigegeben** aufgeführt und haben den Fokus. Details zu dem neuen freigegebenen Postfachs sind im Detailbereich auf der rechten Seite aufgeführt. Um diese Details zu überprüfen, drücken Sie STRG+F6 oder die TAB-TASTE, bis der Detailbereich den Fokus hat.

# Verwenden Sie eine Bildschirmsprachausgabe eine Verteilergruppe in der Exchange-Verwaltungskonsole in Exchange Online Mitglieder hinzu

18.12.2018 • 6 minutes to read

Durch Verwenden einer Sprachausgabe mit der Exchange-Verwaltungskonsole (EAC) in Exchange Online können Sie Elemente einer Verteilergruppe hinzufügen und entfernen.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zur Verwendung der Exchange-Verwaltungskonsole verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Pop-up-Fenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### **Bestätigen Ihres Office 365-Abonnementplans**

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten. Die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### **Öffnen der EAC und Bestätigen Ihrer Administratorrolle**

Zum Ausführen der Aufgaben in diesem Thema [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorrollengruppen [Organisationsverwaltung](#) und [Datensatzverwaltung](#) zugewiesen hat. [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Verwenden der Exchange-Verwaltungskonsole zum Ändern von Verteilergruppenmitgliedschaften

1. Drücken Sie in der Exchange-Verwaltungskonsole die TAB-TASTE, bis im primären Navigationsbereich **Empfänger** angezeigt wird. Sie hören „Empfänger, primäre Navigation“. Drücken Sie die EINGABETASTE.
2. Drücken Sie STRG+F6, um den Fokus auf die Menüleiste zu verschieben. Sie hören „Postfächer, sekundäre Navigation“.
3. Drücken Sie die NACH-LINKS-TASTE, bis Sie „Gruppen, sekundäre Navigation“ hören, und drücken Sie

dann die EINGABETASTE. Die Optionen für Verteilergruppen werden angezeigt.

4. Drücken Sie die NACH-LINKS-TASTE, bis Sie „Gruppen, sekundäre Navigation“ hören, und drücken Sie dann die EINGABETASTE. Die Optionen für Verteilergruppen werden angezeigt.
5. Um die Verteilergruppe zu suchen möchten Sie bearbeiten, verwenden Sie die nach-oben- und nach-unten-Tasten aus, und drücken Sie die EINGABETASTE. Das Fenster **Verteilergruppe** für die ausgewählte Gruppe wird geöffnet. Sie hören "Registerkarte Allgemein.."
6. Drücken Sie die NACH-UNTEN-TASTE, bis Sie „Registerkarte ,Mitgliedschaft“ hören. Es wird eine Liste von Mitgliedern mit zwei Steuerelementen angezeigt. **Hinzufügen** und **Entfernen**.
7. So fügen Sie ein Mitglied hinzu:
  - a. Drücken Sie die TAB-TASTE, bis die Schaltfläche **Hinzufügen** den Fokus hat, und drücken Sie die EINGABETASTE. Das Fenster **Mitglieder auswählen** wird geöffnet und zeigt alle Benutzer in Ihrer Organisation an. Der Fokus befindet sich auf der Schaltfläche **Suchen**.
  - b. Drücken Sie die LEERTASTE, und geben Sie den Namen ganz oder teilweise ein. Benutzer mit diesem Namen werden in der Tabelle **Anzeigename** angezeigt.
  - c. Drücken Sie die TAB-TASTE, bis Sie den ersten aufgeführten Namen hören, falls vorhanden. (In JAWS hören Sie „Außerhalb der Tabelle“ sowie den Namen des ersten Benutzers, falls einer gefunden wurde. Wenn Sie in der Sprachausgabe „Schaltfläche“ ohne Bezeichnung hören, drücken Sie die LEERTASTE, um den Fokus in die Tabelle zu verschieben und die Namen zu hören.) Wählen Sie den gewünschten Benutzer aus, drücken Sie die TAB-Taste, bis Sie „Schaltfläche „Hinzufügen“ hören, und drücken Sie die LEERTASTE. Auf diese Weise können Sie weitere Namen hinzufügen.
  - d. Wenn Sie fertig sind, wechseln Sie mit der TAB-TASTE zur Schaltfläche **OK**, und drücken Sie die EINGABETASTE. Das Fenster **Mitglied auswählen** wird geschlossen.
8. Wählen Sie im Fenster **Verteilergruppe** einen Benutzer in der Tabelle **Mitglieder** aus, und drücken Sie UMSCHALT+TAB, bis Sie „Entfernen“ hören, um ein Mitglied zu entfernen. Drücken Sie die EINGABETASTE.
9. Wenn Sie fertig sind, wechseln Sie mit der TAB-TASTE zur Schaltfläche **Speichern**, und drücken Sie die EINGABETASTE.

## Technischer Support für Kunden mit Behinderungen

Microsoft möchte die bestmögliche Erfahrung für alle Kunden bereitstellen. Wenn Sie eine Behinderung oder Fragen zur Barrierefreiheit haben, wenden Sie sich bitte an den [Microsoft Disability Answer Desk](#), um technische Unterstützung zu erhalten.

Das Supportteam am Disability Answer Desk ist in vielen gängigen Hilfstechnologien geschult und kann Unterstützung in englischer, spanischer, französischer und amerikanischer Gebärdensprache bieten. Besuchen Sie die [Microsoft Disability Answer Desk](#)-Website, um die Kontaktinformationen für Ihre Region zu finden.

# Verwenden Sie eine Bildschirmsprachausgabe zum Archivieren von Postfachelementen in der Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 13 minutes to read

Sie können die Sprachausgabe in der Exchange-Verwaltungskonsole (EAC) verwenden, um das Archivieren von Elementen in einem Exchange Online-Postfach zu aktivieren bzw. zu deaktivieren. Sie können die Sprachausgabe in der Exchange-Verwaltungskonsole auch verwenden, um Aufbewahrungsrichtlinien auf Postfächer anzuwenden. Erfahren Sie mehr über das [Archivieren von Postfächern in Exchange Online](#).

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zur Verwendung der Exchange-Verwaltungskonsole verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

Weitere Informationen zum Erstellen von Verteilergruppen finden Sie unter „Verwenden einer Sprachausgabe zum Erstellen einer neuen Verteilergruppe“ in der Exchange-Verwaltungskonsole.

### Verwenden des Browsers und der Tastatur zum Navigieren in EAC

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Pop-up-Fenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### Bestätigen Ihres Office 365-Abonnementplans

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten. Die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### Öffnen der EAC und Bestätigen Ihrer Administratorrolle

Zum Ausführen der Aufgaben in diesem Thema [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorrollengruppen [Organisationsverwaltung](#) und [Datensatzverwaltung](#) zugewiesen hat. [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Aktivieren der Postfacharchivierung für einen Benutzer

Durch die Postfacharchivierung in Exchange Online, die auch als In-Situ-Archivierung bezeichnet wird, erhalten Benutzer zusätzlichen Speicherplatz im Postfach. Wenn aktiviert, kann über Outlook und Outlook im Web auf Archivpostfächer zugegriffen werden, und diese bieten ein praktisches alternatives Repository für alte E-Mail-Nachrichten.

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis Sie zu **Empfänger** gelangen, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen. Sie hören „Postfächer, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE, um den Link **Postfächer** auszuwählen.
4. Wenn Sie nach dem Benutzer suchen, für den Sie die Archivierung aktivieren möchten, drücken Sie STRG+F6 und dann die TAB-TASTE, bis Sie „Schaltfläche „Suchen““ hören. Drücken Sie die EINGABETASTE.
5. Geben Sie den Namen des Benutzers vollständig oder teilweise ein, und drücken die EINGABETASTE.
6. Drücken Sie viermal STRG+F6, bis Sie den Namen des Benutzers in der Liste der Suchergebnisse hören. Wenn die Liste der Suchergebnisse mehrere Namen enthält, drücken Sie die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den gewünschten Namen hören.
7. Drücken Sie STRG+F6, um zum Detailbereich zu gelangen. Sie hören „Unified Messaging-Link“.
8. Drücken Sie die Tab-Taste etwa sechs Mal, bis Sie hören „Link Archivierung aktivieren...“

**Tipp:** Wenn der Benutzer bereits für die Archivierung aktiviert ist, hören Sie „Link Archivierung deaktivieren...“

9. Drücken Sie die EINGABETASTE. Sie hören „Möchten Sie das Archiv aktivieren?“ Drücken Sie, während der Fokus auf der Schaltfläche **OK** liegt, die EINGABETASTE.

**Tipp:** Wenn Sie die Archivierung für weitere Benutzer aktivieren möchten, den Fokus wieder auf die Liste der Postfächer durch Drücken von STRG + UMSCHALT + F6. Wählen Sie den Namen aus, indem Sie die nach-unten-Taste oder die nach-oben-Taste drücken, und wiederholen Sie die Schritte 7 bis 9.

**Hinweis:** Weitere Informationen finden Sie unter [Aktivieren oder deaktivieren Sie ein Archivpostfach im Exchange Online](#).

## Deaktivieren der Postfacharchivierung für einen Benutzer

Wenn Sie ein Archiv eines Benutzers deaktivieren wird der vorhandene Inhalt 30 Tage lang aufbewahrt. Dies bedeutet, dass der gesamte Inhalt nach wie vor intakt ist, wenn Sie das Archiv innerhalb dieser 30 Tage erneut aktivieren. Nach 30 Tagen werden jedoch sämtliche Informationen dauerhaft gelöscht. Wenn Sie das Archiv danach erneut aktivieren, wird ein neues Archivpostfach erstellt.

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis Sie zu **Empfänger** gelangen, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen. Sie hören „Postfächer, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE, um den Link **Postfächer** auszuwählen.
4. Wenn Sie nach dem Benutzer suchen, für den Sie die Archivierung aktivieren möchten, drücken Sie STRG+F6 und dann die TAB-TASTE, bis Sie „Schaltfläche „Suchen““ hören. Drücken Sie die EINGABETASTE.
5. Geben Sie den Namen des Benutzers vollständig oder teilweise ein, und drücken die EINGABETASTE.
6. Drücken Sie STRG + F6, bis Sie den Namen des Benutzers hören, dessen Postfacharchivierung Sie in der Suchergebnisliste deaktivieren möchten. Wenn die Liste der Suchergebnisse mehrere Namen enthält, drücken Sie die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den gewünschten Namen hören.

7. Drücken Sie STRG+F6, um zum Detailbereich zu gelangen. Sie hören „Unified Messaging-Link“.
8. Drücken Sie die Tab-Taste etwa sechs Mal, bis Sie hören "Link Archivierung deaktivieren..."
9. Drücken Sie die EINGABETASTE. Sie hören „Möchten Sie das Archiv deaktivieren?“ Drücken Sie, während der Fokus auf der Schaltfläche **OK** liegt, die EINGABETASTE.

## Anwenden einer Aufbewahrungsrichtlinie auf einen Benutzer

Mithilfe der Funktion der Messaging-Datensatzverwaltung (MRM) in Exchange Online können Sie den Lebenszyklus der E-Mails Ihrer Organisation verwalten und Aufbewahrungsrichtlinien festlegen. Aufbewahrungsrichtlinien geben an, wann bestimmte Arten von Postfachelementen - einschließlich normaler E-Mail-Nachrichten, gelöschter Elemente und Junk-Mail - verschoben, archiviert oder gelöscht werden sollten. Exchange Online wendet die MRM-Standardrichtlinie automatisch an, wenn Sie ein neues Postfach mit einem Archiv erstellen oder wenn Sie ein Archiv für einen vorhandenen Postfachbenutzer aktivieren.

**Hinweis:** Sie können der MRM-Standardrichtlinie anpassen, indem hinzufügen oder Entfernen von aufbewahrungstags oder Tag Einstellungen ändern. Sie können auch die Standardrichtlinie durch eine beliebige Aufbewahrungsrichtlinien ersetzen, die Sie erstellen. Zum Anzeigen, bearbeiten, oder erstellen Sie eine Aufbewahrungsrichtlinie auf im primären Navigationsbereich Exchange-Verwaltungskonsole, wählen Sie den Link Compliance Management und wählen Sie dann den Retention Policies Link auf der Menüleiste. [Erfahren Sie mehr über Aufbewahrungsrichtlinien](#).

Sie können die gleiche Aufbewahrungsrichtlinie für alle Benutzer anwenden, oder Sie können unterschiedliche Richtlinien auf bestimmte Benutzer anwenden.

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis Sie zu **Empfänger** gelangen, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen. Sie hören „Postfächer, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE, um den Link **Postfächer** auszuwählen.
4. Wenn Sie nach dem Benutzer suchen, für den Sie die Archivierung aktivieren möchten, drücken Sie STRG+F6 und dann die TAB-TASTE, bis Sie „Schaltfläche „Suchen““ hören. Drücken Sie die EINGABETASTE.
5. Geben Sie den Namen des Benutzers vollständig oder teilweise ein, und drücken die EINGABETASTE.
6. Drücken Sie viermal STRG+F6, bis Sie den Namen des Benutzers in der Liste der Suchergebnisse hören. Wenn die Liste der Suchergebnisse mehrere Namen enthält, drücken Sie die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den gewünschten Namen hören. Drücken Sie die EINGABETASTE.
7. Drücken Sie im Dialogfeld **Benutzerpostfach bearbeiten**, während der Fokus auf den Registerkartenamen liegt, die NACH-UNTEN-TASTE, bis der Fokus auf der Registerkarte **Postfachfunktionen** liegt.
8. Drücken Sie die TAB-TASTE bis zum Kombinationsfeld **Aufbewahrungsrichtlinie. MRM-Standardrichtlinie** ist der Standardeintrag. Drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, um die verfügbaren Richtlinien zu durchlaufen. Wählen Sie die gewünschte Richtlinie für diesen Benutzer aus.
9. Drücken Sie die TAB-TASTE, bis die Schaltfläche **Speichern** den Fokus hat, und drücken Sie die EINGABETASTE. Die Listenansicht **Postfächer** hat wieder den Fokus.

## Informationen zu Eingabehilfen

Die [Microsoft-Eingabehilfen](#)-Website stellt weitere Informationen zu Hilfstechnologien bereit. Durch Bezug eines kostenlosen elektronischen Newsletters können Sie auf dem neuesten Stand der Entwicklung auf dem Gebiet der Eingabehilfen für Microsoft-Produkte bleiben. Wenn Sie den Newsletter abonnieren möchten, besuchen Sie die Seite [Microsoft Accessibility Update Newsletter-Abonnement](#).

#### **Technischer Support für Kunden mit Behinderungen**

Microsoft möchte die bestmögliche Erfahrung für alle Kunden bereitstellen. Wenn Sie eine Behinderung oder Fragen zur Barrierefreiheit haben, wenden Sie sich bitte an den [Microsoft Disability Answer Desk](#), um technische Unterstützung zu erhalten.

Das Supportteam am Disability Answer Desk ist in vielen gängigen Hilfstechnologien geschult und kann Unterstützung in englischer, spanischer, französischer und amerikanischer Gebärdensprache bieten. Besuchen Sie die [Microsoft Disability Answer Desk](#)-Website, um die Kontaktinformationen für Ihre Region zu finden.

# Verwenden Sie eine Bildschirmsprachausgabe so konfigurieren Sie für die Zusammenarbeit in der Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 17 minutes to read

Sie können mit der Sprachausgabe im Exchange Admin Center (EAC) in Exchange Online verschiedene Methoden der Zusammenarbeit konfigurieren. Diese Methoden enthalten möglicherweise öffentliche Ordner, Verteilergruppen, freigegebene Postfächer oder - in Verbindung mit SharePoint - Websitepostfächer.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zur Verwendung der Exchange-Verwaltungskonsole verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Popupfenstern, daher sollten Sie in Ihrem Browser unbedingt [Popupfenster für Office 365 aktivieren](#).

### **Bestätigen Ihres Office 365-Abonnementplans**

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### **Öffnen der EAC und Bestätigen Ihrer Administratorrolle**

Zum Ausführen der Aufgaben in diesem Thema [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorrollengruppen [Organisationsverwaltung](#) und [Datensatzverwaltung](#) zugewiesen hat. [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Einrichten öffentlicher Ordner

Mitglieder von Arbeitsgruppen können öffentliche Ordner als ein einfaches Verfahren zum Erfassen, Organisieren und Freigeben von Informationen für andere Benutzer in der Arbeitsgruppe verwenden.

Inhalte werden mithilfe öffentlicher Ordner in einer Hierarchie angeordnet, die einfach zu durchsuchen ist. Benutzer können nützliche Inhalte finden, indem sie die für ihre Arbeit relevanten Unterordner dieser Hierarchie durchsuchen. Die vollständige Hierarchie wird Benutzern in ihrer Outlook-Ordneransicht angezeigt. Öffentliche Ordner eignen sich auch zur Archivierung von Verteilergruppen. Öffentliche Ordner können E-Mail-aktiviert und

als Mitglied der Verteilergruppe hinzugefügt werden. Die an die Verteilergruppe gesendeten E-Mails werden dann automatisch zum öffentlichen Ordner hinzugefügt. Öffentliche Ordner ermöglichen zudem die einfache gemeinsame Nutzung von Dokumenten.

### **Erstellen eines Postfachs für öffentliche Ordner**

Zur Verwendung von öffentlichen Ordnern müssen Sie mindestens ein Postfach für öffentliche Ordner einrichten.

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis Sie zu den öffentlichen Ordnern gelangen, und drücken Sie die EINGABETASTE.
3. Um in der Menüleiste zu verschieben, drücken Sie STRG + F6. Sie hören "Öffentliche Ordner, sekundären Navigationslink..."
4. Wechseln Sie mit der TAB-TASTE zu **Postfächer für öffentliche Ordner**. Drücken Sie die EINGABETASTE.
5. Drücken Sie STRG+F6, um zur Symbolleiste zu gelangen. Sie hören „Schaltfläche ,Neues Postfach für öffentliche Ordner“. Drücken Sie die EINGABETASTE.
6. Im daraufhin geöffneten Dialogfeld **Postfach für öffentliche Ordner** besitzt das Textfeld **Name** den Fokus. Geben Sie den Namen für Ihr Postfach für öffentliche Ordner ein.

#### **TIP**

Postfächer für Öffentliche Ordner enthalten die Hierarchieinformationen sowie den Inhalt für Öffentliche Ordner. Ersten Postfachs für Öffentliche Ordner, den Sie erstellen, wird das primäre Postfach, das die eine nicht schreibgeschützte Kopie der Hierarchie für Öffentliche Ordner enthält. Alle zusätzlichen Öffentlichen Ordner-Postfächer, die Sie erstellen werden sekundäre Postfächer, die eine schreibgeschützte Kopie der Hierarchie enthalten.

7. Drücken Sie die TAB-TASTE, bis die Schaltfläche **Speichern** den Fokus hat, und drücken Sie die EINGABETASTE. Es kann bis zu einer Minute dauern, bis das Postfach für öffentliche Ordner erstellt wird. Dann hören Sie eine Benachrichtigung, die besagt, dass das Postfach in etwa 15 Minuten zur Verfügung steht.
8. Drücken Sie, während der Fokus auf der Schaltfläche **OK** liegt, die EINGABETASTE. Das neue Postfach für öffentliche Ordner wird der Listenansicht der Postfächer für öffentliche Ordner hinzugefügt.

[Weitere Informationen zum Erstellen öffentlicher Ordner.](#)

### **Erstellen eines öffentlichen Ordners**

Nachdem Sie ein Postfach für öffentliche Ordner erstellt haben, können Sie einen öffentlichen Ordner hinzufügen.

1. Drücken Sie, während der Fokus auf der Listenansicht der Postfächer für öffentliche Ordner liegt, zweimal STRG+UMSCHALT+F6, um zur Menüleiste zu wechseln. Sie hören „Öffentliche Ordner, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.
2. Drücken Sie STRG+F6, um zur Symbolleiste zu gelangen. Sie hören „Schaltfläche ,Neuer öffentlicher Ordner“. Drücken Sie die EINGABETASTE. Hiermit wird ein öffentlicher Ordner auf der Stammebene in der Hierarchie der öffentlichen Ordner erstellt.

#### TIP

Sie können einen Unterordner in einen vorhandenen öffentlichen Ordner erstellen. Zunächst mit dem Fokus in der Listenansicht Öffentliche Ordner aus dem übergeordneten Ordner, drücken Sie die nach-unten-Taste oder die nach-oben-Taste, und drücken Sie die Tab-Taste. Um den Ordner zu öffnen, drücken Sie die EINGABETASTE. Wenn Sie um auf der Symbolleiste zu verschieben, drücken Sie dann STRG + UMSCHALT + F6. Wählen Sie die **neuen öffentlichen Ordner** -Schaltfläche, die den Fokus hat, drücken Sie die EINGABETASTE, und fahren Sie mit Schritt 3. (Wenn Sie zurück zum übergeordneten Ordner, klicken Sie auf der Symbolleiste Tab, um die Schaltfläche **zum übergeordneten Ordner wechseln**, und drücken die EINGABETASTE möchten...)

3. Im daraufhin geöffneten Dialogfeld **Öffentlicher Ordner** besitzt das Textfeld **Name** den Fokus. Geben Sie den Namen für Ihren öffentlichen Ordner ein.
4. Drücken Sie die Tab-Taste, um in das Textfeld **Pfad** zu verschieben. In diesem schreibgeschützten Feld hören Sie den Pfad des öffentlichen Ordners an. Angenommen, wenn Sie einen öffentlichen Ordner auf der Stammebene erstellen, hören Sie "umgekehrten Schrägstrich..."
5. Drücken Sie die TAB-TASTE, bis die Schaltfläche **Speichern** den Fokus hat, und drücken Sie die EINGABETASTE. Der Name des neuen öffentlichen Ordners wird der Listenansicht der öffentlichen Ordner hinzugefügt.

#### Hinzufügen von Benutzern eines öffentlichen Ordners

Nachdem Sie einen öffentlichen Ordner erstellt haben, geben Sie die Benutzer an, die darauf zugreifen können. Geben Sie auch die Rollen dieser Benutzer im öffentlichen Ordner an, einschließlich ihrer Lese-/Schreibberechtigungen.

1. Drücken Sie, mit dem Fokus in der Listenansicht öffentlicher Ordner, die NACH-UNTEN- bzw. die NACH-OBEN-TASTE, um den öffentlichen Ordner auszuwählen, dem Sie Benutzer hinzufügen möchten.
2. Drücken Sie STRG+F6, um zum Detailbereich zu gelangen. Der Link **Aktivieren** der E-Mail-Einstellungen besitzt den Fokus.
3. Drücken Sie die TAB-TASTE, um zum Link **Verwalten** der Ordnerberechtigungen zu gelangen, und drücken Sie dann die EINGABETASTE.
4. Im daraufhin geöffneten Dialogfeld **Berechtigungen für öffentliche Ordner** besitzt die Schaltfläche **Hinzufügen** den Fokus. Drücken Sie die EINGABETASTE.
5. Im daraufhin geöffneten Dialogfeld besitzt die Schaltfläche **Durchsuchen** den Fokus. Drücken Sie die EINGABETASTE.
6. Im daraufhin geöffneten Dialogfeld **Empfänger auswählen** besitzt das Textfeld **Suche** den Fokus. Sie hören „Filter oder Suche bearbeiten“. Geben Sie den Namen des ersten Benutzers ganz oder teilweise ein, den Sie dem freigegebenen Postfach hinzufügen möchten, und drücken Sie dann die EINGABETASTE, um nach dem Namen zu suchen.
7. Drücken Sie etwa sechsmal die TAB-TASTE, bis Sie den Namen des Benutzers in der Liste der Suchergebnisse hören. Drücken Sie die EINGABETASTE.

#### TIP

Wenn die Liste der Suchergebnisse mehrere Namen enthält, drücken Sie die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den gewünschten Namen hören. Drücken Sie die EINGABETASTE.

8. Drücken Sie die TAB-TASTE, bis Sie zum Kombinationsfeld **Berechtigungsstufe** gelangen. Die standardmäßige Berechtigungsstufe ist **Editor mit Veröffentlichungsberechtigung**. Dies ermöglicht

ausgewählten Benutzern das Erstellen von Elementen und Unterordnern, das Lesen von Elementen sowie das Bearbeiten oder Löschen aller Elemente. Andere Berechtigungsstufen sind **Prüfer**, **Mitwirkender**, **Autor ohne Bearbeitungsberechtigung**, **Autor**, **Editor**, **Autor mit Veröffentlichungsberechtigung** und **Besitzer**. Sie können auch eine benutzerdefinierte Berechtigungsstufe erstellen.

9. Um die Berechtigungsstufe für den ausgewählten Benutzer auszuwählen, drücken Sie die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE.

#### TIP

Um die zulässigen Rechte für eine Berechtigungsstufe zu überprüfen, durchlaufen Sie mit der TAB-TASTE die 10 Kontrollkästchen, die die Rechte für die ausgewählte Berechtigungsstufe angeben. Wenn Sie die Einstellung eines Kontrollkästchens ändern, ändert sich die Berechtigungsstufe in **Benutzerdefiniert**. Wenn Sie die Berechtigungsstufe **Benutzerdefiniert** auswählen, werden alle Kontrollkästchen deaktiviert, damit Sie die gewünschten aktivieren können.

10. Drücken Sie die TAB-TASTE, bis die Schaltfläche **Speichern** den Fokus hat, und drücken Sie die EINGABETASTE. Der Benutzer und die zugehörige Berechtigungsstufe werden gespeichert und zur Tabelle der Benutzer im Dialogfeld **Berechtigungen für öffentliche Ordner** hinzugefügt.
11. Um einen weiteren Benutzer hinzuzufügen, aktivieren Sie die Schaltfläche **Hinzufügen**, die den Fokus hat, durch Drücken der EINGABETASTE. Wiederholen Sie die Schritte 5 bis 10. Tun Sie dies für alle Benutzer, die Sie dem neuen öffentlichen Ordner hinzufügen möchten.
12. Wenn Sie mit dem Hinzufügen von Benutzern fertig sind, wechseln Sie im Dialogfeld **Berechtigungen für öffentliche Ordner** mit der TAB-TASTE zur Schaltfläche **Speichern**, und drücken Sie die EINGABETASTE. Warten Sie einige Sekunden, bis die Informationen gespeichert werden. Eine Benachrichtigung gibt an, dass der Speichervorgang abgeschlossen ist, und Sie hören „Schaltfläche „Schließen““. Drücken Sie die EINGABETASTE, um die Benachrichtigung zu schließen. Die Hauptseitenansicht **Öffentliche Ordner** hat wieder den Fokus.

#### NOTE

Für öffentliche Ordner gelten Grenzwerte für die Größe, und Unterordner erben Berechtigungseinstellungen von übergeordneten Ordnern auf bestimmte Art und Weise. Darüber hinaus können Sie E-Mail-Einstellungen für einen öffentlichen Ordner aktivieren. [Weitere Informationen zum Erstellen öffentlicher Ordner](#).

## Erstellen einer Verteilergruppe

Eine weitere Methode zum Vereinfachen und Konfigurieren der Zusammenarbeit in Exchange Online ist eine Verteilergruppe - eine Sammlung von mindestens zwei Empfängern, die im freigegebenen Adressbuch angezeigt wird. Wenn eine E-Mail-Nachricht an eine Verteilergruppe gesendet wird, wird sie von allen Mitgliedern der Gruppe empfangen. Verteilergruppen können nach einem bestimmten Diskussionsthema (wie „Bewährte Methoden zur Ressourcenverwaltung“) oder nach Benutzern mit einer gemeinsamen Arbeitsstruktur - wie in einer Arbeitsgruppe oder einem Projektteam - angeordnet werden, die eine regelmäßige Kommunikation untereinander erfordert. [Verwenden einer Sprachausgabe zum Erstellen einer neuen Verteilergruppe im Exchange Admin Center](#). [Erfahren Sie mehr über das Verwalten von Verteilergruppen](#).

## Arbeiten mit freigegebenen Postfächern

Freigegebene Postfächer vereinfachen einer Gruppe von Personen das Überwachen und Senden von E-Mails von einem gemeinsamen Konto aus, wie z. B. "info@contoso.com" oder "support@contoso.com"). Wenn ein Gruppenmitglied auf eine an das freigegebene Postfach gesendete Nachricht antwortet, sieht die E-Mail aus, als

wäre sie vom freigegebenen Postfach aus gesendet und nicht von dem Gruppenmitglied. [Verwenden einer Sprachausgabe zum Hinzufügen eines neuen freigegebenen Postfachs im Exchange Admin Center 2016](#). Erfahren Sie mehr über freigegebene Postfächer.

## Informationen zur Barrierefreiheit

Die [Microsoft-Eingabehilfen](#)-Website stellt weitere Informationen zu Hilfstechnologien bereit. Durch Bezug eines kostenlosen elektronischen Newsletters können Sie auf dem neuesten Stand der Entwicklung auf dem Gebiet der Eingabehilfen für Microsoft-Produkte bleiben. Wenn Sie den Newsletter abonnieren möchten, besuchen Sie die Seite [Microsoft Accessibility Update Newsletter-Abonnement](#).

### **Technischer Support für Kunden mit Behinderungen**

Microsoft möchte die bestmögliche Erfahrung für alle Kunden bereitstellen. Wenn Sie eine Behinderung oder Fragen zur Barrierefreiheit haben, wenden Sie sich bitte an den [Microsoft Disability Answer Desk](#), um technische Unterstützung zu erhalten.

Das Supportteam am Disability Answer Desk ist in vielen gängigen Hilfstechnologien geschult und kann Unterstützung in englischer, spanischer, französischer und amerikanischer Gebärdensprache bieten. Besuchen Sie die [Microsoft Disability Answer Desk](#)-Website, um die Kontaktinformationen für Ihre Region zu finden.

# Verwenden einer Sprachausgabe zum Erstellen einer neuen Verteilergruppe im Exchange Admin Center

18.12.2018 • 15 minutes to read

Mit einer Sprachausgabe und Tastenkombinationen können Sie eine neue Verteilergruppe im Exchange Admin Center (EAC) in Exchange Online erstellen. In diesem Thema wird erläutert, wie eine neue Verteilergruppe in Ihrer Exchange-Organisation erstellt und eine vorhandene Gruppe in Active Directory E-Mail-aktiviert wird.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zur Verwendung der Exchange-Verwaltungskonsole verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### Hinweise:

- Sind die verschiedenen Typen von Gruppen, die in diesem Thema behandelt werden:
  - **Verteilergruppen:** kann nur zum Übermitteln von Nachrichten verwendet werden.
  - **E-Mail-aktivierte Sicherheitsgruppen:** zum Übermitteln von Nachrichten sowie zum Erteilen von Berechtigungen (eine Sicherheitsgruppe ist ein *Sicherheitsprinzipal*, der Berechtigungen zugewiesen hat, können) verwendet werden.

Weitere Informationen finden Sie unter [Erstellen und Verwalten von Verteilergruppen in Exchange Online](#).

- Wenn Ihre Organisation eine gruppenbenennungsrichtlinie verfügt, wird er nur für Gruppen von Benutzern (nicht-Admins) erstellte angewendet. Weitere Informationen finden Sie unter [Erstellen einer Verteilergruppe Namensrichtlinie für in Exchange Online](#) und [Außerkraftsetzung der Verteilung-Gruppe Benennungsrichtlinie in Exchange Online](#).

### Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Popupfenstern, daher sollten Sie in Ihrem Browser unbedingt [Popupfenster für Office 365 aktivieren](#).

### Bestätigen Ihres Office 365-Abonnementplans

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten. Die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### Öffnen der EAC und Bestätigen Ihrer Administratorrolle

Zum Ausführen der Aufgaben in diesem Thema [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorrollengruppen [Organisationsverwaltung](#) und [Datensatzverwaltung](#) zugewiesen hat. [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Erstellen einer Verteilergruppe mithilfe der Exchange-Verwaltungskonsole

1. Drücken Sie in der Exchange-Verwaltungskonsole die TAB-TASTE, bis im primären Navigationsbereich **Empfänger** angezeigt wird. Sie hören „Empfänger, primäre Navigation“. Drücken Sie die EINGABETASTE.
2. Drücken Sie STRG + F6, um den Fokus auf der Menüleiste. Sie hören, "Postfächer, sekundären Navigationslink..."
3. Drücken Sie die nach-links-Taste, bis Sie "Groups, sekundären Navigationslink.. gehört"
4. Drücken Sie die EINGABETASTE. Sie hören „Gruppen Optionen“. Eine Liste von Verteilergruppen wird angezeigt.
5. Drücken Sie STRG+F6, um den Fokus auf das Menü **Verteilergruppe** zu verschieben. Sie hören „**Neu**“, die erste Schaltfläche.
6. Drücken Sie die LEERTASTE, um das Untermenü **Neu** zu öffnen.
7. Drücken Sie im Menü **Neu** so oft die NACH-UNTEN-TASTE, bis Sie „Verteilergruppe“ hören. Drücken Sie dann die EINGABETASTE. (In der Sprachausgabe hören Sie möglicherweise „Leere Zeile“ oder gar nichts. Die drei Elemente in diesem Menü sind **Verteilergruppe**, **Sicherheitsgruppe** und **Dynamische Verteilergruppe**. Wählen Sie das erste Element im Menü aus.) Die Seite **Neue Verteilergruppe** wird in einem neuen Browserfenster geöffnet.

### TIP

Das Fenster **Neue Verteilergruppe** enthält zwei Schaltflächen namens **Hinzufügen** und zwei namens **Entfernen**. Die erste Gruppe von **Hinzufügen** - und **Entfernen** -Schaltflächen wirkt sich auf das Feld **Besitzer auswählen** aus. Die zweite Gruppe bezieht sich auf das Feld **Mitglieder auswählen**.

8. Registerkarte mit den folgenden Optionen, und füllen Sie die Gruppendetails.

### TIP

Erforderliche Felder sind mit einem Sternchen gekennzeichnet. In Sprachausgaben hören Sie „Stern“ oder „Sternchen“ vor der Beschriftung. Beispiel: Für das erforderliche Feld **Anzeigename** hören Sie „Stern Anzeigename“ oder „Sternchen Anzeigename“. Außerdem hören Sie den Text für eine QuickInfo, die angezeigt wird, wenn Sie den Fokus auf eine Option verschieben.

- **\*Anzeigename**. Geben Sie den Namen ein, der im Adressbuch Ihrer Organisation angezeigt werden soll. Der Name wird in der **An:**-Zeile angezeigt, wenn eine E-Mail an diese Gruppe gesendet wird. Außerdem wird er in der Liste **Gruppen** im EAC angezeigt. Der Anzeigename ist erforderlich. Er sollte für Benutzer erkennbar und in der Gesamtstruktur eindeutig sein.
- **\*Alias**. Geben Sie einen Namen von maximal 64 Zeichen für den Alias der Gruppe ein. Wählen Sie einen innerhalb der Gesamtstruktur eindeutigen Namen. Wenn ein Benutzer den Alias in der **An:**-Zeile einer E-Mail eingibt, wird dieser zum Anzeigenamen der Gruppe aufgelöst.
- **\*E-Mail-Adresse**. Wenn Sie den Standardnamen für die E-Mail-Adresse dieser Gruppe ändern

möchten, geben Sie den gewünschten Namen ein. Der Standardwert ist der von Ihnen angegebene Alias.

- **Notizen.** Wenn Sie eine Beschreibung für diese Verteilergruppe hinzufügen möchten, geben Sie eine Notiz ein. Der eingegebene Text wird auf der Visitenkarte der Gruppe und im Adressbuch angezeigt.
- **Hinzufügen** Zum Öffnen des Fensters **Besitzer auswählen**, in dem Sie der Verteilergruppe Besitzer hinzufügen können, wählen Sie **Hinzufügen** aus. Standardmäßig ist die Person, die eine Gruppe erstellt, der Besitzer und wird im Feld **Besitzer** aufgeführt. Jede Gruppe muss mindestens einen Besitzer aufweisen. Hilfe zur Verwendung des Fensters **Besitzer auswählen** finden Sie unter „Verwenden einer Sprachausgabe im Fenster ‚Besitzer auswählen‘“ weiter unten in diesem Thema.
- **Entfernen.** Zum Entfernen eines ausgewählten Namens aus dem Feld **Besitzer** verwenden Sie diese Option.
- \*\* \*Besitzer\*\*. Diese Option Listet die Namen der Verteilergruppe Inhaber. Sprachausgabe lesen Sie den ausgewählten Namen, nicht die Bezeichnung. Hören Sie beispielsweise "Sara Davis, Schaltfläche..."
- **Gruppenbesitzer als Mitglieder hinzufügen.** Dieses Kontrollkästchen ist standardmäßig aktiviert.
- **Hinzufügen** Wählen Sie diese Option zum Hinzufügen von Mitgliedern zur Verteilergruppe. Standardmäßig sind die Gruppenbesitzer Mitglieder und werden im Feld **Mitglieder** aufgeführt. Wenn Sie die Schaltfläche **Hinzufügen** auswählen, wird das Fenster **Mitglieder auswählen** geöffnet, und Sie können die gewünschten Namen suchen oder auswählen. Zum Zurückkehren zum Fenster **Neue Verteilergruppe** wählen Sie die Schaltfläche **OK** aus. Die genauen Schritte finden Sie unter „Verwenden einer Sprachausgabe zum Hinzufügen eines Mitglieds zu einer Verteilergruppe“.
- **Entfernen.** Entfernt den ausgewählten Namen aus dem Feld **Mitglieder**.
- **Mitglieder.** Diese Option listet die Namen der Mitglieder der Verteilergruppe auf. In der Sprachausgabe hören Sie möglicherweise „Bitte warten“ oder nichts, wenn diese Liste leer ist.
- **Wählen Sie aus, ob für den Beitritt zur Gruppe eine Genehmigung des Besitzers erforderlich ist.** Sprachausgaben lesen die ausgewählte Option vor. Der Standardwert lautet **Offen**. Um die Genehmigung für den Gruppenbeitritt von Personen zu fordern, wählen Sie mit den Pfeiltasten eine der anderen beiden Optionen aus: **Geschlossen** oder **Genehmigung des Besitzers**.
- **Wählen Sie aus, ob die Gruppe ohne Genehmigung verlassen werden kann.** Sprachausgaben lesen die ausgewählte Option vor. Der Standardwert lautet **Offen**. Um die Genehmigung für das Verlassen der Gruppe zu fordern, wählen Sie mit den Pfeiltasten **Geschlossen** aus.

9. Wenn Sie fertig sind, wechseln Sie mit der TAB-TASTE zur Schaltfläche **Speichern**, und drücken Sie die EINGABETASTE.

#### **NOTE**

Standardmäßig ist für neue Verteilergruppen die Authentifizierung aller Absender erforderlich. Auf diese Weise wird verhindert, dass externe Absender Nachrichten an Verteilergruppen senden können. Um eine Verteilergruppe für das Annehmen von Nachrichten von allen Absendern zu konfigurieren, müssen Sie die Einstellungen für die Einschränkungen der Nachrichtenübermittlung für die betreffende Verteilergruppe ändern.

## **Überprüfen der erfolgreichen Erstellung einer Verteilergruppe**

1. Drücken Sie im EAC die TAB-TASTE, bis Sie zu **Empfänger** gelangen, und drücken Sie die EINGABETASTE.
2. Drücken Sie STRG+F6, um den Fokus auf die Menüleiste zu verschieben. Sie hören „Postfächer, sekundäre Navigation“.
3. Drücken Sie die NACH-LINKS-TASTE, bis Sie „Gruppen, sekundäre Navigation“ hören, und drücken Sie dann die EINGABETASTE. Die Tabelle mit den aktuellen Verteilergruppen wird angezeigt.
4. Drücken Sie STRG+F6, bis Sie den Namen einer Verteilergruppe hören. Dies zeigt an, dass sich der Fokus auf der Tabelle der Verteilergruppen befindet.
5. Verwenden Sie die NACH-OBEN-TASTE und die NACH-UNTEN-TASTE, um die soeben erstellte Verteilergruppe zu suchen. Die Sprachausgabe liest den Anzeigenamen, den Gruppentyp und die E-Mail-Adresse vor.

#### **Verwenden einer Sprachausgabe im Fenster „Besitzer auswählen“**

Klicken Sie im **neuen Verteilergruppe Hinzufügen** Schaltfläche für die \* **Besitzer** Dialogfenster Fenster **Besitzer auswählen**, welche einige Sprachausgabe Probleme haben. So fügen Sie einen Besitzer hinzu.

1. Wechseln Sie im Fenster **Neue Verteilergruppe** mit der TAB-TASTE zur Schaltfläche **Hinzufügen**, und drücken Sie die EINGABETASTE. Das Fenster **Besitzer auswählen** wird geöffnet, und der Fokus liegt auf einem Suchfeld.
2. Geben Sie ganz oder teilweise den Namen des Benutzers ein, den Sie hinzufügen möchten, und drücken Sie dann die EINGABETASTE. In der Tabelle **Anzeigename** wird eine Liste von Namen angezeigt. Wenn keine Namen vorhanden sind, drücken Sie UMSCHALT+TAB, bis Sie „Filter oder Suche bearbeiten“ oder den Text der vorherigen Suche hören, und geben Sie dann den neuen Suchtext ein.
3. Um einen Namen auszuwählen, ist Tab, bis Sie einem Namen hören, der angibt, die den Fokus auf den Namen in der Tabelle **Anzeigename**. (In JAWS, hören Sie "aus der Tabelle" und der Name des ersten Benutzers aufgelistet...)
4. Verwenden Sie die Pfeiltasten, um den gewünschten Namen auszuwählen.
5. Drücken Sie die TAB-TASTE, bis Sie „Schaltfläche „Hinzufügen““ hören, und drücken Sie dann die LEERTASTE. Der Name wird zu einem Textfeld hinzugefügt. Jeder Name, den Sie hinzufügen, enthält einen Link **Entfernen**.
6. Um weitere Namen hinzuzufügen, wechseln Sie mit der TAB-TASTE zur Schaltfläche **Suchen**, und wiederholen Sie die vorherigen Schritte.
7. Zum Abschluss wechseln Sie mit der TAB-TASTE zur Schaltfläche **OK** und drücken die EINGABETASTE. Das Fenster **Besitzer auswählen** wird geschlossen, und der Fokus befindet sich auf dem Feld **Besitzer** im Fenster **Neue Verteilergruppe**.

## Technischer Support für Kunden mit Behinderungen

Microsoft möchte die bestmögliche Erfahrung für alle Kunden bereitstellen. Wenn Sie eine Behinderung oder Fragen zur Barrierefreiheit haben, wenden Sie sich bitte an den [Microsoft Disability Answer Desk](#), um technische Unterstützung zu erhalten.

Das Supportteam am Disability Answer Desk ist in vielen gängigen Hilfstechnologien geschult und kann Unterstützung in englischer, spanischer, französischer und amerikanischer Gebärdensprache bieten. Besuchen Sie die [Microsoft Disability Answer Desk](#)-Website, um die Kontaktinformationen für Ihre Region zu finden.

# Verwenden Sie eine Bildschirmsprachausgabe zum Konfigurieren von e-Mail-Flussregeln in der Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 18 minutes to read

Eine Bildschirmsprachausgabe und Tastenkombinationen verwenden, können Sie Mail Flow Regeln (auch als Transportregeln bezeichnet) erstellen in Exchange Online in der Exchange-Verwaltungskonsole (EAC) für bestimmte Ereignisse im Nachrichten suchen, die durch Ihre Organisation geleitet und Ausführen einer Aktion auf. Der Hauptunterschied zwischen e-Mail-Flussregeln sowie für Postfachregeln, die Sie in einer e-Mail-Client-Anwendung (wie Outlook) eingerichtet würde ist, dass e-Mail-Flussregeln Ausführen einer Aktion auf Nachrichten während der Übertragung im Gegensatz zur laufenden nach dem die Nachricht übermittelt wird. Transportregeln enthalten außerdem einen umfangreicheren Satz von Bedingungen, Ausnahmen und Aktionen, der Sie die Flexibilität, viele Arten von Messagingrichtlinien implementieren bereitstellt.

**Hinweis:** Weitere Informationen zum e-Mail-Flussregeln finden Sie unter [E-Mail-Fluss Regeln \(Transportregeln\) in Exchange Online](#).

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abo und die Administratorrolle zum Durchführen dieser Aufgabe verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Pop-up-Fenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### Bestätigen Ihres Office 365-Abo

Exchange Online ist in Office 365 Business- und Enterprise-Abo-Plänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### Öffnen der EAC und Bestätigen Ihrer Administratorrolle

In diesem Thema [verwenden, öffnen Sie die Exchange-Verwaltungskonsole eine Bildschirmsprachausgabe](#) Kontrollkästchen, und, die Ihre Office 365 globale Administrator zur Administratorrolle [Organization Management](#) und [Records Management](#) zugewiesen hat Aufgaben behandelt Gruppen. Hier erfahren Sie, wie Sie [eine Bildschirmsprachausgabe zur Identifizierung der Administratorrolle in der Exchange-Verwaltungskonsole verwenden](#).

# Erstellen einer Nachrichtenflussregel

1. In der Exchange-Verwaltungskonsole, um den Fokus auf den ersten Hyperlink im Navigationsbereich – **Dashboard** – drücken Sie STRG + F6 zweimal. Sie hören "Dashboard primären Navigationslink..."
2. Drücken Sie im Navigationsbereich zum Verschieben des Fokus auf den Link **E-Mail-Fluss** so oft die TAB-TASTE, bis Sie „E-Mail-Fluss, primärer Navigationslink“ hören. Drücken Sie die EINGABETASTE.
3. Um den Fokus auf die e-Mail-Nachricht drücken Fluss Einstellungen im Inhaltsbereich der Seite, von denen die erste der **Regeln** Link ist, STRG + F6. Sie hören "Regeln, sekundären Navigationslink..."
4. Um eine neue Regel zu erstellen, verschieben Sie den Fokus auf die Schlüssel **Neu**, indem Sie die TAB-TASTE drücken, bis Sie „Neue Schaltfläche“ hören. Drücken Sie die EINGABETASTE. Sie hören „Menü“. Drücken Sie die NACH-UNTEN-TASTE, um die Option **Neue Regel erstellen** aus der Liste der Optionen auszuwählen, die für die Schaltfläche geöffnet wird. Sie hören „Neue Regel erstellen“. Drücken Sie die EINGABETASTE.
5. Wie der Fokus auf das Textfeld **Name** im Popupfenster **neue Regel**, hören Sie "Neue Regel, nennen, zu bearbeiten." Geben Sie den Namen der neuen Regel. Wenn der nächsten Option im Fenster verschieben möchten, drücken Sie die Tab-Taste.
6. Wie der Fokus auf das Dropdown- **diese Regel anwenden, wenn** Sie hören "diese Regel anwenden" If "; Kombinationsfeld." Drücken Sie die nach-unten- oder nach-oben-Taste, bis Sie die Bedingung hören, den, die Sie aktivieren möchten. Drücken Sie die EINGABETASTE. Wie des Fokus zu der ersten-Benutzeroberfläche (UI)-Element in das Popup-Fenster, das für die ausgewählte Bedingung geöffnet wird bewegen, hören Sie den Namen des Popupfensters gefolgt vom Namen des ersten Elements im Fenster Benutzeroberfläche. In der folgenden Tabelle finden Sie eine Übersicht über die Elemente der Benutzeroberfläche in jede Bedingung Popup-Fenster. . |Zum Auswählen einer Option drücken Sie die EINGABETASTE.|Sie können auch die LEERTASTE drücken, um die Markierung für Kontrollkästchen zu aktivieren oder zu deaktivieren.| |-----|-----|• Der Absender ist
  - Der Empfänger ist.
  - Der Absender ist Mitglied von
  - Der Empfänger ist Mitglied von|• **Suche, Aktualisieren** und **Weitere** Schaltflächen.
  - **Anzeigename** und **E-Mail-Adresse** Spaltenüberschriften.
  - Liste der Namen und e-Mail-Adressen.
  - **Hinzufügen** Schaltfläche und das Textfeld, das die ausgewählten Namen enthält.
  - **Namen überprüfen** Schaltfläche und das Textfeld Geben Sie den Namen ein, die Sie prüfen möchten.
  - **OK** und **Abbrechen** -Schaltflächen.| |• Der Absender befindet sich in
    - Der Empfänger befindet sich in|• Dropdown-Feld, das eine Liste der Speicherorte geöffnet wird.
    - OK und Abbrechen-Schaltflächen.| |• Betreff oder Nachrichtentext enthält
    - Die Absenderadresse enthält
    - Die Empfängeradresse enthält
    - Die Inhalt mindestens einer Anlage enthält|• Bearbeiten und Entfernen von Schaltflächen.
    - Textfeld, in dem Sie Wörter und eine Schaltfläche **Hinzufügen** , um jeden Eintrag hinzufügen eingeben.
    - Liste der Einträge.
  - **OK** und **Abbrechen** -Schaltflächen.| |[Auf alle Nachrichten anwenden]|||Kein Popupfenster wird geöffnet]

## TIP

Zum Verschieben des Fokus auf jede Einstellung, die in einem Popupfenster aufgeführt ist, drücken Sie die Tab-Taste. Wenn Sie jede Einstellung auswählen, hören Sie Informationen für sie. Klicken Sie zum Öffnen des Dropdown-Listenfeld Listen drücken Sie LEERTASTE. Wechseln zwischen, und wählen Sie Optionen im Dropdown-Listenfeld Listen, drücken Sie die nach-unten-Taste. Wenn Sie ausgewählt haben, drücken Sie die EINGABETASTE. Sie können auch die LEERTASTE aktivieren oder deaktivieren Sie die Auswahl für Kontrollkästchen.

7. Nachdem Sie Ihre Einstellungen Bedingung im entsprechenden Popupfenster akzeptiert haben, verschieben Sie zur nächsten Option im Popupfenster **neue Regel** durch Drücken der Tab-Taste.
8. Wie der Fokus auf das Dropdownfeld **Gehen Sie folgendermaßen vor**, hören Sie "die folgenden, Kombinationsfeld." Drücken Sie die nach-unten- oder nach-oben-Taste, bis Sie die Aktion gehört, den, die Sie aktivieren möchten. Drücken Sie die EINGABETASTE. Wie der Fokus auf das erste Element der Benutzeroberfläche in das Popup-Fenster, das geöffnet wird für den ausgewählten Vorgang, hören Sie den Namen des Popupfensters gefolgt vom Namen des ersten Elements im Fenster Benutzeroberfläche. In der folgenden Tabelle finden Sie eine Übersicht über die UI-Elemente in jeder Aktion Popup-Fenster.

AKTION	BENUTZEROBERFLÄC HENELEMENTE IM POPUPFENSTER			
<ul style="list-style-type: none"> <li>• Weiterleiten der Nachricht zur Genehmigung an</li> <li>• Umleiten der Nachricht an</li> <li>• Bcc der Nachricht an</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Suche</b>, <b>Aktualisieren</b> und <b>Weitere</b> Schaltflächen.</li> <li>• <b>Anzeigename</b> und <b>E-Mail-Adresse</b> Spaltenüberschriften</li> <li>• Liste der Namen und e-Mail-Adressen.</li> <li>• <b>Hinzufügen</b> Schaltfläche und das Textfeld, das die ausgewählten Namen enthält.</li> <li>• <b>Namen überprüfen</b> Schaltfläche und das Textfeld Geben Sie den Namen ein, die Sie prüfen möchten.</li> <li>• <b>OK</b> und <b>Abbrechen</b> - Schaltflächen.</li> </ul>			
	Textfeld, in dem Sie die Erläuterung eingeben Schaltflächen OK und Abbrechen	Löschen der Nachricht ohne Benachrichtigung	<ul style="list-style-type: none"> <li>• Textfeld, in dem Sie die Erläuterung OK angeben</li> <li>• <b>OK</b> und <b>Abbrechen</b> - Schaltflächen.</li> </ul>	
	Haftungsausschluss anfügen			Es wird kein Popupfenster geöffnet, aber es wird ein Link zur Eingabe von Text und ein Link zur Auswahl in das Fenster nach dem Dropdownfeld eingefügt.

AKTION	BENUTZEROBERFLÄC HENELEMENTE IM POPUPFENSTER		
	<p>Wenn Sie den Link Text eingeben auswählen, wird ein Popupfenster geöffnet, das ein Textfeld enthält, in das Sie den Haftungsausschluss eingeben, sowie die Schaltflächen <b>OK</b> und <b>Abbrechen</b>.</p> <p>Keine Popup-Fenster wird geöffnet, aber ein Link <b>Text eingeben</b> und einen Link <b>auswählen</b> werden im Fenster nach dem Dropdown Feld eingefügt.</p> <ul style="list-style-type: none"> <li>Wenn Sie den Link <b>: Geben Sie Text</b> auswählen, wird ein Popup-Fenster geöffnet, die ein Textfeld enthält, in dem der Haftungsausschluss und die Schaltflächen <b>OK</b> und <b>Abbrechen</b> eingeben.</li> <li>Wenn Sie den Link <b>wählen eine</b> auswählen, wird ein Popup-Fenster geöffnet, die ein Dropdown-Listenfeld, das eine Liste der Aktionen fallback geöffnet wird, für den Fall, dass der Haftungsausschluss eingefügt werden kann und die Schaltflächen <b>OK</b> und <b>Abbrechen</b> enthält.</li> </ul>		

#### 9. Während sich der Fokus auf das Kontrollkästchen **Diese Regel mit folgendem Schweregrad überwachen**:

**überwachen:** verschiebt, hören Sie „Aktiviert“ oder „Deaktiviert“, je nachdem, ob das Feld aktiviert ist oder nicht, gefolgt von „Diese Regel mit folgendem Schweregrad überwachen; Kontrollkästchen“.

#### 10. Wie der Fokus auf das Kontrollkästchen **diese Regel mit Schweregrad**, Sie "Aktiviert" oder "Deaktiviert" hören, je nachdem, ob das Kontrollkästchen aktiviert ist, gefolgt von "diese Regel mit Schweregrad, das Kontrollkästchen überwachen." Aktivieren oder deaktivieren Sie das Kontrollkästchen für den, drücken Sie die LEERTASTE. Sie hören "Aktiviert" oder "Deaktiviert". Führen Sie einen der folgenden beiden Aktionen.

- Wenn Sie das Kontrollkästchen **diese Regel mit Schweregrad** ausgewählt, wenn Sie die Tab-Taste drücken, verschiebt den Fokus an ein Dropdown-Listenfeld, die Schweregrade ( **Niedrig**, **Mittel** oder **Hoch** ) enthält. Drücken Sie die nach-oben- oder nach-unten-Taste, um zwischen Schweregrade in der Liste zu verschieben. Hören Sie den Namen der einzelnen Schweregrad. Um einen Schweregrad auszuwählen, drücken Sie die EINGABETASTE. Wenn der nächsten Option im Fenster verschieben möchten, drücken Sie die Tab-Taste.
- Drücken Sie die Tab-Taste, wenn Sie das Kontrollkästchen **diese Regel mit Schweregrad** zur nächsten verfügbaren Option klicken Sie im Fenster Verschieben ausgewählt haben.

11. Als der Fokus wechselt zum ersten der drei verfügbaren Modi für die Regel, hören Sie den Namen des ersten Modus (**erzwingen**) gefolgt von "Radio Button". Führen Sie einen der folgenden drei Aktionen.

- Der Modus **erzwingen** ist standardmäßig aktiviert. Verschieben, und wählen Sie den nächsten Modus, drücken Sie die nach-unten-Taste. Nachdem Sie den Modus, den Sie in den nächsten Bereich der Optionen, klicken Sie im Fenster verschieben möchten ausgewählt haben, den drücken Sie die Tab-Taste.
- Wenn Sie den **Test mit Richtlinientipps** Modus ausgewählt haben, drücken Sie die nach-unten-Taste. Sie hören "Test mit Richtlinientipps" gefolgt von "Radio Button". Verschieben, und wählen Sie den nächsten Modus, drücken Sie die nach-unten-Taste. Nachdem Sie den Modus, den Sie in den nächsten Bereich der Optionen, klicken Sie im Fenster verschieben möchten ausgewählt haben, den drücken Sie die Tab-Taste.
- Wenn Sie den **Test ohne Richtlinientipps** Modus ausgewählt haben, drücken Sie die nach-unten-Taste. Sie hören "Test ohne Richtlinientipps" gefolgt von "Radio Button". Verschieben, und wählen Sie den nächsten Modus, drücken Sie die nach-unten-Taste. Nachdem Sie den Modus, den Sie in den nächsten Bereich der Optionen, klicken Sie im Fenster verschieben möchten ausgewählt haben, den drücken Sie die Tab-Taste.

12. Der Fokus auf den Link **Weitere Optionen**, hören Sie "Weitere Optionen Link." Wenn Sie weitere Optionen für die Regel hinzufügen möchten, drücken Sie die EINGABETASTE. Das Fenster werden die folgenden neun Benutzeroberflächenelemente hinzugefügt.

- Nach dem Dropdownfeld **Gehen Sie wie folgt vor:** wird die Schaltfläche **Aktion hinzufügen** hinzugefügt.
- Nach der Schaltfläche **Aktion hinzufügen** wird die Schaltfläche **Ausnahme hinzufügen** hinzugefügt.
- Nach den Optionen für die Modi für die Regel werden die folgenden Benutzeroberflächenelemente hinzugefügt:
  - Kontrollkästchen Diese Regel an folgendem Datum aktivieren; gefolgt von einem Dropdownfeld für Datum und einem Dropdownfeld für Uhrzeit
- **Aktivieren Sie diese Regel auf das Datum in der folgenden** Kontrollkästchen, gefolgt von einem Datum im Dropdownfeld und eine Uhrzeit Dropdown-Feld.
- **Deaktivieren Sie diese Regel auf das Datum in der folgenden** Kontrollkästchen, gefolgt von einem Datum im Dropdownfeld und eine Uhrzeit Dropdown-Feld.
- **Beenden der Verarbeitung weiterer Regeln** überprüfen Feld.
- **Deferr die Nachricht, wenn Verarbeitung nicht abgeschlossen** überprüfen Feld.
- **Übereinstimmung Absenderadresse in Nachricht** Dropdown-Listenfeld, die Option **Kopfzeile, Umschlag** und **Kopf- oder Umschlag** enthält.
- **Kommentartext** Feld.

13. Um die neue Regel zu speichern, den Fokus auf die Schaltfläche **Speichern** durch Drücken der Tab-Taste, bis Sie "Speichern Button." gehört Drücken Sie die EINGABETASTE..

14. Während der Fokus zurück zur Schaltfläche **Neu** im Inhaltsbereich **Regeln** der Seite wechselt, hören Sie „Regeln, Schaltfläche ' Neu'." Die neue Regel ist standardmäßig aktiviert.

**TIP**

Um eine neue Regel zu deaktivieren, drücken Sie die TAB-TASTE, um die Elemente des Inhaltsbereichs **Regeln** der Seite zu durchlaufen, verwenden Sie die NACH-OBEN-TASTE und die NACH-UNTEN-TASTE, um eine Regel auszuwählen, und drücken Sie dann die LEERTASTE. Um die Einstellungen für eine ausgewählte Regel zu hören, drücken Sie die TAB-TASTE, bis sich der Fokus auf den Detailbereich für die ausgewählte Regel verschiebt. Daraufhin hören Sie die Details für die Regel.

# Verwenden Sie eine Bildschirmsprachausgabe Definieren von Regeln, die Ver- oder Entschlüsseln von e-Mail-Nachrichten in der Exchange- Verwaltungskonsole in Exchange Online

18.12.2018 • 17 minutes to read

In der Exchange-Verwaltungskonsole (EAC) in Exchange Online können Sie e-Mail-Flussregeln (auch als Transportregeln bezeichnet) zum Aktivieren oder Deaktivieren von Office 365 Message Encryption erstellen. Auf diese Weise können Sie ausgehende e-Mail-Nachrichten verschlüsseln und Entfernen der Verschlüsselung von verschlüsselten Nachrichten, die von innerhalb Ihrer Organisation oder von Antworten auf verschlüsselte Nachrichten, die von Ihrer Organisation gesendet.

**Hinweis:** Weitere Informationen zu verschlüsseln, wechseln Sie zur [Verschlüsselung in Office 365](#). Ihre Organisation muss [Windows Azure Rights Management für Office 365-Nachrichtenverschlüsselung eingerichtet](#) haben, zum Ausführen der Aufgaben in diesem Thema wird.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zum Durchführen dieser Aufgabe verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Popupfenstern, daher sollten Sie in Ihrem Browser unbedingt [Popupfenster für Office 365 aktivieren](#).

### **Bestätigen Ihres Office 365-Abonnementplans**

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### **Öffnen der EAC und Bestätigen Ihrer Administratorrolle**

Zum Ausführen der Aufgaben in diesem Thema [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorrollengruppen [Organisationsverwaltung](#) und [Datensatzverwaltung](#) zugewiesen hat. [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

# Erstellen einer e-Mail-Flussregel zum Verschlüsseln von e-Mail-Nachrichten

1. In der Exchange-Verwaltungskonsole, um den Fokus auf den ersten Hyperlink im Navigationsbereich – **Dashboard** – drücken Sie STRG + F6 zweimal. Sie hören "Dashboard primären Navigationslink..."
2. Drücken Sie im Navigationsbereich zum Verschieben des Fokus auf den Link **E-Mail-Fluss** so oft die TAB-TASTE, bis Sie „E-Mail-Fluss, primärer Navigationslink“ hören. Drücken Sie die EINGABETASTE.
3. Um den Fokus auf die e-Mail-Nachricht drücken Fluss Einstellungen im Inhaltsbereich der Seite, von denen die erste der **Regeln** Link ist, STRG + F6. Sie hören "Regeln, sekundären Navigationslink..."
4. Um eine neue Regel zu erstellen, verschieben Sie den Fokus auf die Schlüssel **Neu**, indem Sie die TAB-TASTE drücken, bis Sie „Neue Schaltfläche“ hören. Drücken Sie die EINGABETASTE. Sie hören „Menü“. Drücken Sie die NACH-UNTEN-TASTE, um die Option **Neue Regel erstellen** aus der Liste der Optionen auszuwählen, die für die Schaltfläche geöffnet wird. Sie hören „Neue Regel erstellen“. Drücken Sie die EINGABETASTE.
5. Wie der Fokus auf das Textfeld **Name** im Popupfenster **neue Regel**, hören Sie "Neue Regel, nennen, zu bearbeiten." Geben Sie den Namen der neuen Regel (beispielsweise Verschlüsseln von e-Mail für e-Mail-Adresse). Wenn der nächsten Option im Fenster verschieben möchten, drücken Sie die Tab-Taste.
6. Wie der Fokus auf das Dropdown- **diese Regel anwenden, wenn** Sie hören "diese Regel anwenden" If ; Kombinationsfeld." Drücken Sie die nach-unten- oder nach-oben-Taste, bis Sie die Bedingung hören, den, die Sie aktivieren möchten. Drücken Sie die EINGABETASTE. Wenn Sie zum Verschlüsseln von Nachrichten für einen bestimmten e-Mail-Adresse möchten, führen Sie beispielsweise die folgenden fünf Schritte.
  - a. Drücken Sie im Dropdownfeld **Diese Regel anwenden, wenn** die NACH-UNTEN-TASTE, bis Sie hören „Der Empfänger ist“. Drücken Sie die EINGABETASTE.
  - b. Der Fokus auf die Schaltfläche **Suchen** im Popupfenster **Elemente auswählen** verschoben wird, das geöffnet wird, hören Sie "Select Members, suchen..."
  - c. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
    - a. Die Spalte **Anzeigenamen**. Sie hören "Anzeigename, Spaltenüberschrift..."
    - b. Die Liste der Namen der einzelnen Personen in Ihrer Organisation in der Spalte **Name**. Sie hören den Namen der ersten Person gefolgt von "Schaltfläche..."
    - c. Die erste Person in der Liste. Sie hören den Namen der ersten Person, gefolgt von „Zeile“.
  - d. Die erste Person in der Liste. Sie hören den Namen der ersten Person, gefolgt von „Zeile“.
  - e. Um die Änderungen zu akzeptieren, verschieben Sie den Fokus auf die Schlüssel **OK**, indem Sie die TAB-TASTE drücken, bis Sie „OK“ hören. Drücken Sie die EINGABETASTE.
7. Wie der Fokus wieder auf die **neue Regel** Popupfenster verschiebt, hören Sie "neue Regel..."
8. Um den Fokus auf den Link **Weitere Optionen** im Popupfenster **Neue Regel** zu verschieben, drücken Sie die TAB-TASTE, bis Sie „Weitere Optionen, Link“ hören. Drücken Sie die EINGABETASTE.

#### TIP

Wenn Sie den Link **Weitere Optionen** auswählen, werden der Seite weitere Benutzeroberflächenelemente und den Kombinationsfeldern werden weitere Optionen hinzugefügt. Um Zugriff auf die Option **Nachrichtensicherheit ändern** zu haben, die Sie im nächsten Schritt auswählen müssen, müssen Sie den Link **Weitere Optionen** auswählen.

9. Um den Fokus wieder auf das Dropdown- **Gehen Sie** im Popupfenster **neue Regel** zu verschieben, drücken Sie Umschalt + Tab, bis Sie hören "Führen Sie die folgenden, Kombinationsfeld." Führen Sie die folgenden zwei Schritte aus.
  - a. Wählen Sie im Dropdownfeld **Gehen Sie wie folgt vor:** die Option **Nachrichtensicherheit ändern** aus, und drücken Sie die NACH-UNTEN-TASTE, bis Sie „Nachrichtensicherheit ändern“ hören. Drücken Sie die EINGABETASTE.
  - b. Während sich der Fokus auf eine Liste von Sicherheitsoptionen für Nachrichten verschiebt, hören Sie die erste Option in der Liste, „Rechteschutz anwenden“. Um die Option **Office 365-Nachrichtenverschlüsselung anwenden** auszuwählen, drücken Sie die NACH-UNTEN-TASTE, bis Sie „Office 365-Nachrichtenverschlüsselung anwenden“ hören. Drücken Sie die EINGABETASTE.
10. Um die neue Regel zu speichern, verschieben Sie den Fokus auf die Schaltfläche **Neu**, indem Sie die TAB-TASTE drücken, bis Sie „Neue Schaltfläche“ hören. Drücken Sie die EINGABETASTE.
11. Während der Fokus zurück zur Schaltfläche **Neu** im Inhaltsbereich **Regeln** der Seite wechselt, hören Sie „Regeln, Schaltfläche ' Neu'.“ Die neue Regel ist standardmäßig aktiviert.

#### TIP

Um eine neue Regel zu deaktivieren, drücken Sie die TAB-TASTE, um die Elemente des Inhaltsbereichs **Regeln** der Seite zu durchlaufen, verwenden Sie die NACH-OBEN-TASTE und die NACH-UNTEN-TASTE, um eine Regel auszuwählen, und drücken Sie dann die LEERTASTE. Um die Einstellungen für eine ausgewählte Regel zu hören, drücken Sie die TAB-TASTE, bis sich der Fokus auf den Detailbereich für die ausgewählte Regel verschiebt. Daraufhin hören Sie die Details für die Regel.

## Erstellen einer e-Mail-Flussregel zum Entschlüsseln von e-Mail-Nachrichten

1. In der Exchange-Verwaltungskonsole, um den Fokus auf den ersten Hyperlink im Navigationsbereich – **Dashboard** – drücken Sie STRG + F6 zweimal. Sie hören "Dashboard primären Navigationslink..."
2. Drücken Sie im Navigationsbereich zum Verschieben des Fokus auf den Link **E-Mail-Fluss** so oft die TAB-TASTE, bis Sie „E-Mail-Fluss, primärer Navigationslink“ hören. Drücken Sie die EINGABETASTE.
3. Um den Fokus auf die e-Mail-Nachricht drücken Fluss Einstellungen im Inhaltsbereich der Seite, von denen die erste der **Regeln** Link ist, STRG + F6. Sie hören "Regeln, sekundären Navigationslink..."
4. Um eine neue Regel zu erstellen, verschieben Sie den Fokus auf die Schaltfläche **Neu**, indem Sie die TAB-TASTE drücken, bis Sie „Neue Schaltfläche“ hören. Drücken Sie die EINGABETASTE. Sie hören „Menü“. Drücken Sie die NACH-UNTEN-TASTE, um die Option **Neue Regel erstellen** aus der Liste der Optionen auszuwählen, die für die Schaltfläche geöffnet wird. Sie hören „Neue Regel erstellen“. Drücken Sie die EINGABETASTE.
5. Während sich der Fokus auf das Textfeld **Name** im Popupfenster **Neue Regel** verschiebt, hören Sie „Neue Regel, Name, Bearbeiten“. Geben Sie den Namen der neuen Regel ein, z. B. „Verschlüsselung für eingehende E-Mails entfernen“. Um zur nächsten Option im Fenster zu gelangen, drücken Sie die TAB-TASTE.

6. Wie der Fokus auf das Dropdown- **diese Regel anwenden, wenn** Sie hören "diese Regel anwenden" If "; Kombinationsfeld." Drücken Sie die nach-unten- oder nach-oben-Taste, bis Sie die Bedingung hören, den, die Sie aktivieren möchten. Drücken Sie die EINGABETASTE. Wenn Sie alle eingehende Nachrichten für Ihre Organisation entschlüsseln möchten, führen Sie beispielsweise die folgenden vier Schritte.

- a. Drücken Sie im Dropdownfeld **Diese Regel anwenden, wenn** die NACH-UNTEN-TASTE, bis Sie hören „Der Empfänger befindet sich“. Drücken Sie die EINGABETASTE.
- b. Wie der Fokus zu einer Liste der Speicherorte im Popupfenster **Wählen Sie Empfänger Speicherort** verschoben, das geöffnet wird wird, hören Sie "Empfänger Speicherort auswählen..."
- c. Zum Wechseln zwischen, und wählen Sie einen Speicherort in der Liste, drücken Sie die nach-unten-Taste. Hören Sie den Namen der verschiedenen Speicherorte. Beispiel: um **innerhalb der Organisation Speicherort** auszuwählen, drücken Sie die nach-unten-Taste, bis Sie "innerhalb die Organisation.. hören
- d. Um die Änderungen zu akzeptieren, verschieben Sie den Fokus auf die Schlüssel **OK**, indem Sie die TAB-TASTE drücken, bis Sie „OK“ hören. Drücken Sie die EINGABETASTE.

7. Wie der Fokus wieder auf die **neue Regel** Popupfenster verschiebt, hören Sie "neue Regel..."
8. Um den Fokus auf den Link **Weitere Optionen** im Popupfenster **Neue Regel** zu verschieben, drücken Sie die TAB-TASTE, bis Sie „Weitere Optionen, Link“ hören. Drücken Sie die EINGABETASTE.

#### TIP

Wenn Sie den Link **Weitere Optionen** auswählen, werden der Seite weitere Benutzeroberflächenelemente und den Kombinationsfeldern werden weitere Optionen hinzugefügt. Um Zugriff auf die Option **Nachrichtensicherheit ändern** zu haben, die Sie im nächsten Schritt auswählen müssen, müssen Sie den Link **Weitere Optionen** auswählen.

9. Um den Fokus wieder auf das Dropdown- **Gehen Sie** im Popupfenster **neue Regel** zu verschieben, drücken Sie Umschalt + Tab, bis Sie hören "Führen Sie die folgenden, Kombinationsfeld." Führen Sie die folgenden zwei Schritte aus.
  - a. Wählen Sie im Dropdownfeld **Gehen Sie wie folgt vor:** die Option **Nachrichtensicherheit ändern** aus, und drücken Sie die NACH-UNTEN-TASTE, bis Sie „Nachrichtensicherheit ändern“ hören. Drücken Sie die EINGABETASTE.
  - b. Während sich der Fokus auf eine Liste von Sicherheitsoptionen für Nachrichten verschiebt, hören Sie die erste Option in der Liste, „Rechteschutz anwenden“. Um die Option **Office 365-Nachrichtenverschlüsselung entfernen** auszuwählen, drücken Sie die NACH-UNTEN-TASTE, bis Sie „Office 365-Nachrichtenverschlüsselung entfernen“ hören. Drücken Sie die EINGABETASTE.
10. Um die neue Regel zu speichern, verschieben Sie den Fokus auf die Schaltfläche **Neu**, indem Sie die TAB-TASTE drücken, bis Sie „Neue Schaltfläche“ hören. Drücken Sie die EINGABETASTE.
11. Während der Fokus zurück zur Schaltfläche **Neu** im Inhaltsbereich **Regeln** der Seite wechselt, hören Sie „Regeln, Schaltfläche ' Neu'.“ Die neue Regel ist standardmäßig aktiviert.

#### TIP

Um eine neue Regel zu deaktivieren, drücken Sie die TAB-TASTE, um die Elemente des Inhaltsbereichs **Regeln** der Seite zu durchlaufen, verwenden Sie die NACH-OBEN-TASTE und die NACH-UNTEN-TASTE, um eine Regel auszuwählen, und drücken Sie dann die LEERTASTE. Um die Einstellungen für eine ausgewählte Regel zu hören, drücken Sie die TAB-TASTE, bis sich der Fokus auf den Detailbereich für die ausgewählte Regel verschiebt. Daraufhin hören Sie die Details für die Regel.

# Verwenden Sie eine Bildschirmsprachausgabe so bearbeiten Sie den Anzeigenamen des Postfachs in der Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 4 minutes to read

Verwenden von Tastenkombinationen und der Sprachausgabe zum Hinzufügen oder Bearbeiten des Anzeigenamen eines Postfachs in der Exchange-Verwaltungskonsole (EAC) in Exchange Online.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zum Durchführen dieser Aufgabe verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden.

Verwenden Sie für optimale Ergebnisse, wenn Sie in der Exchange-Verwaltungskonsole in Exchange Online arbeiten Internet Explorer als Browser. [Erfahren Sie mehr über die Tastenkombinationen für Internet Explorer](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole ist erforderlich, dass die Verwendung von Popup-Fenster, in Ihrem Browser sicher, dass Sie für Office 365 [Popupfenster ermöglicht](#) werden.

### Bestätigen Ihres Office 365-Abonnementplans

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen zu den Exchange Online-Funktionen in Ihrem Abonnement erhalten Sie unter [What Office 365 business product or license do I have?](#) und [Exchange Online Service Description](#).

## Bearbeiten des Anzeigenamen eines Postfachs

1. Drücken Sie in der Exchange-Verwaltungskonsole STRG+F6, um zum Textkörper zu navigieren. Sie hören „Willkommen“.
2. Drücken Sie die TAB-TASTE, bis Sie „Postfächer“ hören. Dies ist der erste Link nach „Empfänger“.
3. Drücken Sie die EINGABETASTE, um den Link auszuwählen und zur Seite **Postfächer** zu wechseln.  
Dadurch gelangen Sie zur Registerkarte **Postfächer** auf der Seite **Postfächer**. Der Fokus befindet sich auf der Registerkarte **Postfächer**.
4. Drücken Sie STRG+F6 zweimal, um zum Bereich **Postfach** zu gelangen. Sie hören den ersten Namen in der Liste von Postfächern.
5. Verwenden Sie die Pfeiltasten, um das Postfach auszuwählen, die Sie aktualisieren möchten. Sie hören den Namen jedes Postfachbenutzers.

6. Wenn Sie das Postfach gefunden haben, das Sie bearbeiten möchten, drücken Sie die EINGABETASTE. Ein Popupfenster wird geöffnet. Sie hören die URL dieses Popupfensters. Der Fokus befindet sich auf der Registerkarte **Allgemein** auf der Seite **Postfach bearbeiten**.
7. Wenn Sie in das Feld **Anzeigename den Namen** auf der Registerkarte **Allgemein** erhalten möchten, drücken Sie die Tab-Taste. Sie hören "Anzeigename..."
8. Geben Sie den neuen Anzeigenamen ein.
9. Um zur Schaltfläche **Speichern** zu gelangen, drücken Sie die TAB-TASTE (Sie hören „Schaltfläche ,Speichern‘, und drücken Sie die EINGABETASTE. Dadurch gelangen Sie zurück zur Registerkarte **Postfachliste**. Der Fokus befindet sich auf dem Namen, den Sie soeben bearbeitet haben.

**TIP**

Es kann einige Minuten dauern, bis das neue Postfach gespeichert ist und das Popupfenster geschlossen wird. Während dieser Wartezeit hören Sie kein weiteres Feedback.

# Verwenden einer Sprachausgabe zum Exportieren und Überprüfen von Überwachungsprotokollen im Exchange Admin Center

18.12.2018 • 20 minutes to read

Mithilfe der Sprachausgabe in der Exchange-Verwaltungskonsole (EAC) in Exchange Online können Sie Postfachüberwachungsprotokolle exportieren und überprüfen. Bei aktivierter Postfachüberwachung protokolliert Exchange Postfachüberwachungsinformationen im Postfachüberwachungsprotokoll, wenn ein Benutzer, bei dem es sich nicht um den Besitzer des Postfachs handelt, auf das Postfach zugreift. Jeder Protokolleintrag enthält Informationen darüber, wer auf das Postfach zugegriffen hat und welche Aktionen ausgeführt wurden.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zum Durchführen dieser Aufgabe verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Popupfenstern, daher sollten Sie in Ihrem Browser unbedingt [Popupfenster für Office 365 aktivieren](#).

### **Bestätigen Ihres Office 365-Abonnementplans**

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### **Öffnen der EAC und Bestätigen Ihrer Administratorrolle**

Zum Exportieren und Überprüfen von Postfachüberwachungsprotokollen [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorrollengruppen „Organisationsverwaltung“ und „Datensatzverwaltung“ zugewiesen hat. Erfahren Sie mehr über das [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

### **Konfigurieren der Postfachüberwachungsprotokollierung**

Bevor Sie exportieren können und Überwachungsprotokolle überprüfen, müssen Sie oder ein anderes Admin aktivieren muss Postfach postfachüberwachungsprotokollierung und Konfigurieren von Outlook zum XML-Anlagen zuzulassen. Die folgenden Aufgaben werden in Exchange Online PowerShell ausgeführt. Weitere Informationen finden Sie auf [postfachüberwachungsprotokolle exportieren](#).

# Exportieren eines Postfachüberwachungsprotokolls

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis der Fokus auf **Verwaltung der Compliance** liegt, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen.
4. Drücken Sie die TAB-TASTE, bis der Fokus auf **Überwachung** liegt. Sie hören „Überwachung, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.
5. Zugriff auf die Listenansicht im Hauptfenster drücken Sie STRG + F6. Sie hören "Audit meldet..."
6. Drücken Sie die TAB-TASTE etwa sechsmal, bis Sie „**Postfachüberwachungsprotokolle exportieren**“ hören, und drücken Sie die EINGABETASTE.
7. **Postfachüberwachungsprotokolle exportieren** im Dialogfeld, das geöffnet wird, das **Startdatum** Jahr Kombinationsfeld den Fokus hat, und hören Sie "Jahr des Kombinationsfelds **Startdatum** ..."

## TIP

Standardmäßig wird das Startdatum auf zwei Wochen vor dem gestrigen Datum festgelegt. Wenn aktiviert, werden im Postfachüberwachungsprotokoll normalerweise Einträge für 90 Tage gespeichert.

- a. Geben Sie, falls erforderlich, das Jahr des Startdatums für die Überwachungsprotokolle ein. Sie können das Jahr des Startdatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
  - b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Startdatums ein bzw. wählen Sie ihn aus.
  - c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Startdatums ein bzw. wählen Sie ihn aus.
8. Registerkarte im Kombinationsfeld **Enddatum** Jahr. Sie hören "Year-End Date Kombinationsfelds..."

## TIP

Der Standardwert des Enddatums ist das heutige Datum.

- a. Geben Sie, falls erforderlich, das Jahr des Enddatums für die Überwachungsprotokolle ein. Sie können das Jahr des Enddatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
  - b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Enddatums ein bzw. wählen Sie ihn aus.
  - c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Enddatums ein bzw. wählen Sie ihn aus.
9. Zugriff auf die Schaltfläche **Wählen Sie Benutzer aus**, drücken Sie zweimal die Tab-Taste. Sie hören "diese Postfächer suchen oder leer lassen, um alle Postfächer von nicht-Besitzer zugegriffen suchen..."

**TIP**

Wenn Sie die Überwachungsprotokolle für alle Postfächer exportieren möchten, nicht, wählen Sie keine Benutzer aus, und fahren Sie mit Schritt 10 fort. Wenn das Feld **Diese Benutzer durchsuchen** leer ist, umfasst die Suche alle Postfächer.

- a. Drücken Sie die EINGABETASTE, um das Dialogfeld **Postfach auswählen**, mit den Fokus auf die Schaltfläche **Benutzer auswählen** zu öffnen. Das Feld **Suchen** den Fokus hat, und hören Sie "Filter oder Suche bearbeiten". Geben Sie alle oder einen Teil des Namens des ersten Postfachs, dessen Überwachungsprotokolle zu exportieren, und drücken dann zum Suchen des Namens eingeben.
- b. Drücken Sie zur Auswahl eines Postfachs viermal die TAB-TASTE, bis Sie den Namen des Postfachbesitzers in der Liste der Suchergebnisse hören. Wenn die Liste der Suchergebnisse mehrere Postfächer enthält, drücken Sie die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen des Postfachbesitzers hören.

**TIP**

Es können mehrere aufeinanderfolgende Postfächer ausgewählt werden. Zum Arbeiten mit allen Postfächern lassen Sie das Feld **Suche** leer, oder geben Sie ganz oder teilweise die Postfachnamen ein, die Sie hinzufügen möchten. Wechseln Sie mit der TAB-TASTE zu den Suchergebnissen. Drücken Sie die NACH-UNTEN-TASTE, um jeden Namen zu hören. Wenn alle hinzufügen möchten, drücken Sie STRG+A. Wenn Sie mehrere nacheinander aufgelistete Postfächer hinzufügen möchten, drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, bis Sie den ersten Postfachnamen hören, den Sie hinzufügen möchten. Halten Sie die UMSCHALTTASTE gedrückt, drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, bis Sie den letzten Postfachnamen hören, den Sie hinzufügen möchten, und lassen Sie dann die UMSCHALTTASTE los. Alle Postfächer zwischen dem ersten und letzten Postfachnamen werden ausgewählt.

- c. Drücken Sie die EINGABETASTE, um die ausgewählten Postfächer zu der Liste hinzuzufügen, die in den Überwachungsprotokollexport eingeschlossen werden soll. Die Liste der Postfächer behält den Fokus, sodass Sie weitere Postfächer hinzufügen können, indem Sie sie auswählen und die EINGABETASTE drücken.

**TIP**

Zum Überprüfen der hinzugefügten Postfächer wechseln Sie mit der TAB-TASTE zur Schaltfläche **Hinzufügen**. Um die Liste der Postfächer anzuhören, drücken Sie die TAB-TASTE erneut. Sie hören den ersten Postfachnamen in der Liste. Um den zweiten Postfachnamen in der Liste zu hören, drücken Sie noch einmal die TAB-TASTE. Drücken Sie weiterhin die TAB-TASTE, bis Sie die Namen aller hinzugefügten Postfächer gehört haben. Um ein Postfach aus der Liste zu löschen, aktivieren Sie den Link **Entfernen** durch Drücken der EINGABETASTE, wenn Sie den Postfachnamen hören.

- d. Um ein anderes Postfach oder eine andere Gruppe von Postfächern zu suchen, drücken Sie mehrmals die TAB-TASTE, bis Sie hören „Filter oder Suche bearbeiten“. Geben Sie ganz oder teilweise den Namen der nächsten Postfächer ein, die Sie hinzufügen möchten, und drücken die EINGABETASTE. Wiederholen Sie die Schritte b und c. Tun Sie dies für alle Postfächer, die Sie hinzufügen möchten.
- e. Um ein externes Postfach hinzuzufügen, drücken Sie die TAB-TASTE, bis Sie hören „Namen überprüfen bearbeiten, Text eingeben“. (In Sprachausgabe hören Sie „Bearbeiten“.) Geben Sie die E-Mail-Adresse des externen Empfängers ein, drücken Sie UMSCHALT+TAB, um die Schaltfläche **Namen überprüfen** auszuwählen, und drücken Sie dann die EINGABETASTE. Dadurch wird die E-Mail-Adresse überprüft und zur Liste der Postfächer hinzugefügt.

**TIP**

Beachten Sie: Wenn Sie eine externe E-Mail-Adresse eingeben und die EINGABETASTE drücken, wird die Adresse der Liste hinzugefügt und das Dialogfeld geschlossen. Wenn Sie noch nicht fertig sind, verwenden Sie stattdessen die Schaltfläche **Namen überprüfen**, um sie hinzuzufügen.

- f. Wenn Sie mit dem Hinzufügen von Postfächern fertig sind, wechseln Sie mit der TAB-TASTE zur Schaltfläche **OK**, und drücken Sie die EINGABETASTE. Das Dialogfeld **Postfachüberwachungsprotokolle exportieren** hat erneut den Fokus, und im Textfeld „Diese Postfächer suchen“ sind die ausgewählten Postfächer aufgelistet.
10. Wechseln Sie mit der TAB-TASTE zum Kombinationsfeld **Suchen nach Zugriff durch**. Dies gibt an, welche Arten von Nicht-Besitzern in den Überwachungsprotokollen angezeigt werden sollen.
  - Wenn in den Überwachungsprotokollen alle Nicht-Besitzer angezeigt werden sollen, müssen Sie nichts weiter tun, da dies der Standardwert ist.
  - Um eine bestimmte Gruppe von Nicht-Besitzern anzugeben, z. B. **Externe Benutzer** (Microsoft-Datencenteradministratoren) oder **Administratoren und delegierte Benutzer** oder **Administratoren**, drücken Sie die NACH-UNTEN-TASTE, um zum gewünschten Benutzertyp zu wechseln, und drücken Sie dann die EINGABETASTE.
11. Drücken Sie die Tab-Taste zweimal auf die Schaltfläche Weiter **Wählen Sie Benutzer** zugreifen. Sie hören "die Überwachungsbericht senden an Personenauswahl Schaltfläche". Drücken Sie die EINGABETASTE, um das Dialogfeld **Elemente auswählen** zu öffnen. Schaltfläche "Suchen" besitzt den Fokus.
12. Wenn Sie einen Benutzer in Ihrer Organisation suchen möchten, drücken Sie die EINGABETASTE, geben Sie den Namen des ersten Empfängers des Überwachungsprotokolls ganz oder teilweise ein, und drücken Sie dann die EINGABETASTE.
13. Drücken Sie mehrere Male die TAB-TASTE, bis Sie den Namen des Benutzers in der Liste der Suchergebnisse hören.
14. Um den Benutzer zur Liste der Empfänger des Überwachungsprotokolls hinzuzufügen, drücken Sie die NACH-UNTEN-TASTE, bis Sie den Namen des Benutzers hören, und drücken Sie dann die EINGABETASTE. Die Liste der Benutzer behält den Fokus, sodass Sie weitere Empfänger hinzufügen können, indem Sie ihre Postfächer auswählen und die EINGABETASTE drücken.

**TIP**

So überprüfen Sie die Empfänger, die Sie hinzugefügt haben, die TAB, um die Schaltfläche **Hinzufügen**. Um die Liste der Empfänger zu hören, drücken Sie die Tab-Taste erneut. Der erste Name wird gelesen. Um den zweiten Namen in der Liste zu hören, drücken Sie die Tab-Taste noch einmal. Fahren Sie fort, die Tab-Taste drücken, bis Sie die Namen aller Empfänger hören, die Sie hinzugefügt haben. Um einen Empfänger aus der Liste löschen möchten, aktivieren Sie den Link **Entfernen** durch Drücken der EINGABETASTE, wenn Sie den Benutzernamen hören.

4. Um einen anderen Namen bzw. eine Gruppe von Namen in Ihrer Organisation zu suchen, drücken Sie mehrmals die TAB-TASTE, bis Sie hören „Filter oder Suche bearbeiten“. Geben Sie ganz oder teilweise den Namen des nächsten Benutzers ein, den Sie hinzufügen möchten, und drücken die EINGABETASTE. Wiederholen Sie die Schritte b und c. Führen Sie dies für alle Berichtsempfänger in Ihrer Organisation aus.
5. Um einen externen Empfänger hinzuzufügen, drücken Sie die TAB-TASTE, bis Sie hören „Namen überprüfen bearbeiten, Text eingeben“. (In Sprachausgabe hören Sie „Bearbeiten“.) Geben Sie die E-Mail-Adresse des externen Empfängers ein, drücken Sie UMSCHALT+TAB, um die Schaltfläche **Namen überprüfen** auszuwählen, und drücken Sie dann die EINGABETASTE. Dadurch wird die E-Mail-Adresse

überprüft und zur Liste der Empfänger hinzugefügt.

#### TIP

Beachten Sie: Wenn Sie eine externe E-Mail-Adresse eingeben und die EINGABETASTE drücken, wird der Empfänger der Liste hinzugefügt und das Dialogfeld geschlossen. Wenn Sie noch nicht fertig sind, verwenden Sie stattdessen die Schaltfläche **Namen überprüfen**, um sie hinzuzufügen.

6. Wenn Sie mit dem Hinzufügen von Benutzern fertig sind, wechseln Sie mit der TAB-TASTE zur Schaltfläche **OK**, und drücken Sie die EINGABETASTE. Das Dialogfeld **Postfachüberwachungsprotokolle exportieren** hat erneut den Fokus, und im Textfeld **Überwachungsbericht senden an:** sind die Empfänger des Überwachungsprotokolls aufgelistet.
7. Registerkarte auf die Schaltfläche **Exportieren**, und drücken Sie die EINGABETASTE. Exchange ruft Einträge in das postfachüberwachungsprotokoll, die die Suchkriterien erfüllen, speichert sie in eine Datei namens " SearchResult.xml " und fügt dann die XML-Datei an eine e-Mail-Nachricht an die Empfänger der ausgewählten Audit Log innerhalb von 24 Stunden gesendet.

#### TIP

Wenn Sie eine Fehlermeldung hören, dass die Elemente, die Sie öffnen möchten, nicht gefunden wurden, überprüfen Sie, ob die Überwachungsprotokollierung für die ausgewählten Postfächer aktiviert ist. Überprüfen Sie außerdem, dass sich die ausgewählten Datumsangaben innerhalb des zulässigen Bereichs befinden. Die Datumsangaben müssen nach dem Datum liegen, an dem die Überwachungsprotokollierung aktiviert wurde, und standardmäßig innerhalb der letzten 90 Tage.

## Überprüfen eines Postfachüberwachungsprotokolls

1. Öffnen Sie Outlook, und melden Sie sich bei Ihrem Postfach (bzw. bei dem Postfach an, an das das Postfachüberwachungsprotokoll gesendet wurde).
2. Öffnen Sie im Posteingang die Nachricht, die von Exchange oder Outlook mit einem Betreff gesendet wurde, der „Postfachüberwachungsprotokoll-Suche“ und eine XML-Dateianlage mit dem Namen „ SearchResult.xml “ enthält. Der Text der E-Mail enthält die Suchkriterien für dieses exportierte Überwachungsprotokoll.

#### TIP

Wenn Outlook nicht für XML-Anlagen konfiguriert ist, können Sie die E-Mail-Nachricht möglicherweise empfangen, jedoch die XML-Anlage nicht öffnen. Wenn Sie die Nachricht nicht finden, müssen Sie möglicherweise länger warten. Empfänger erhalten das exportierte Überwachungsprotokoll in der Regel innerhalb von 24 Stunden, aber in einigen Fällen kann es ein paar Tage dauern.

3. Wählen Sie die Anlage der Nachricht aus, und geben Sie an, dass Sie die XML-Datei herunterladen möchten.
4. Öffnen Sie die Datei „ SearchResult.xml “ in Excel. Jeder Protokolleintrag enthält Informationen über Nicht-Besitzer des Postfachs, wer auf das Postfach zugegriffen hat und welche Aktionen ausgeführt wurden. Das Überwachungsprotokoll enthält u.a. die folgenden Felder:

DIESES FELD FÜR DAS POSTFACHÜBERWACHUNGSPROTOKOLL

Besitzer

STELLT DIE FOLGENDEN INFORMATIONEN BEREIT:

Der Besitzer des Postfachs, auf das von einem Nicht-Besitzer zugegriffen wurde

DIESES FELD FÜR DAS POSTFACHÜBERWACHUNGSPROTOKOLL	STELLT DIE FOLGENDEN INFORMATIONEN BEREIT:
LastAccessed	Das Datum und die Uhrzeit des letzten Postfachzugriffs
Vorgang	Die Aktion, die durch den Nicht-Besitzer ausgeführt wurde
OperationResult	Gibt an, ob die vom Nicht-Besitzer ausgeführte Aktion erfolgreich war.
LogonType	Die Art des Nicht-Besitzer-Zugriffs, z. B. Administrator, Stellvertretung oder externer Microsoft-Datencenteradministrator
ClientIPAddress	Die IP-Adresse des Computers, mit dem der Nicht-Besitzer auf das Postfach zugegriffen hat.
LogonUserDN	Der Anzeigename des Nicht-Besitzers
Betreff	Die Betreffzeile der Nachricht, die von der Aktion des Nicht-Besitzers betroffen war

# Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center

18.12.2018 • 4 minutes to read

Zum Ausführen administrativer Aufgaben im Exchange-Verwaltungskonsole (EAC) in Exchange Online benötigen Sie die entsprechenden administrativen Berechtigungen, die nach Rollen gruppiert und zugewiesen werden. Mithilfe einer Sprachausgabe und bestimmten Tastenkombinationen können Sie Ihre Administratorrolle sowie die Rolle identifizieren, die Ihnen für bestimmte Aufgaben zugewiesen werden muss.

## NOTE

Informationen zum Öffnen von EAC finden Sie unter [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#). Weitere Informationen zu Administratorrollengruppen finden Sie unter [Grundlegendes zu Verwaltungsrollengruppen](#).

1. In der Exchange-Verwaltungskonsole zum Verschieben des Fokus **Dashboard**, das die erste Verknüpfung im Navigationsbereich ist, drücken Sie STRG + F6 zweimal. Sie hören "Dashboard primären Navigationslink..."
2. Drücken Sie im Navigationsbereich zum Verschieben des Fokus auf den Link **Berechtigungen** so oft die TAB-TASTE, bis Sie „Berechtigungen, primärer Navigationslink“ hören. Drücken Sie die EINGABETASTE.
3. Um den Fokus auf den Link zu den Administratorrollen im Inhaltsbereich der Seite zu verschieben, drücken Sie STRG+F6. Sie hören „Administratorrollen, sekundärer Navigationslink“.
4. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE für jedes Element:
  - a. Den Hauptinhalt für Administratorrollen. Sie hören „Rollengruppen“.
  - b. Die **Name**-Spalte. Sie hören "Spaltenüberschrift Name..."
  - c. Die Liste der administratorrollengruppen in der Spalte **Name**. Sie hören den Namen der die erste Rollengruppe, **Verwaltung der Richtlinientreue**, gefolgt von "Zeile..."
5. Verwenden Sie in der Liste der Administratorrollengruppen zum Wechseln zwischen den Gruppennamen und zum Auswählen eines Gruppennamens die NACH-OBEN- und NACH-UNTEN-TASTEN. Wenn Sie eine Gruppe auswählen, hören Sie ihren Namen, gefolgt von „Zeile“.
6. Wählen Sie die Administratorrollengruppe aus, die die Rolle enthält, die Sie für eine Aufgabe benötigen.

## TIP

Wenn Sie nicht wissen, welche Rolle für einen bestimmten Vorgang benötigt wird, wählen Sie die Administratorrollengruppe aus, die Ihrer Meinung nach Rollen im Zusammenhang mit der Aufgabe enthält. Führen Sie Schritt 6 aus, und achten Sie besonders auf die zugewiesenen Rollen.

7. Drücken Sie STRG + F6, um den Fokus auf im Detailbereich für die Rollengruppe "Admin".

- Wenn Sie Sprachausgabe verwenden, hören Sie alle Details für die Administratorrollengruppe, einschließlich einer Beschreibung der Gruppe, zugewiesener Rollen, verwalteter Mitglieder und des Schreibrreichs.
- Wenn Sie JAWS verwenden und die Beschreibung der Administratorrollengruppe hören möchten, drücken Sie die NACH-UNTEN-TASTE und dann, um den Rest des Texts im Detailbereich zu hören, ALT+NACH-UNTEN.

8. Wenn Sie Ihren Namen nicht unter den Mitgliedern hören, wurde Ihnen nicht die geeignete Rolle zum Durchführen der Aufgabe zugewiesen. Weitere Informationen erhalten Sie von Ihrem Office 365-Administrator.

# Verwenden Sie eine Bildschirmsprachausgabe zum Verwalten von Anti-Malware Protection in der Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 13 minutes to read

Exchange Online bietet einen mehrstufigen Schutz, der jegliche bekannte Schadsoftware abwehrt. Alle Nachrichten werden auf Schadsoftware (Viren und Spyware) geprüft, und wenn Schadsoftware erkannt wird, wird die Nachricht gelöscht. Administratoren müssen die standardmäßig aktivierten Filtertechnologien weder einrichten noch verwalten. Administratoren können jedoch unternehmensspezifische Filteranpassungen in der Exchange-Verwaltungskonsole (EAC) vornehmen - mithilfe von Sprachausgabe und Tastenkombinationen.

## NOTE

Um mehr über das Schützen der E-Mail-Nachrichten Ihrer Organisation vor Schadsoftware in Exchange Online zu erfahren, gehen Sie zu [Antispam- und Antischadsoftwareschutz](#).

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zum Durchführen dieser Aufgabe verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Pop-up-Fenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### Bestätigen Ihres Office 365-Abonnementplans

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrer Abonnementplan, wechseln Sie zur [welche Office 365-Business-Produkt oder Lizenz habe ich?](#) und [Exchange Online Service Description](#).

### Öffnen der EAC und Bestätigen Ihrer Administratorrolle

Zum Ausführen der Aufgaben in diesem Thema [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorrollengruppen [Organisationsverwaltung](#) und [Verwaltung von Nachrichtenschutz](#) zugewiesen hat. Erfahren Sie mehr über das [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

# Verschieben des Fokus auf Ihre Filtereinstellungen für Schadsoftware in EAC

Für die in diesem Thema behandelten Schritte zur Anpassung der Filtereinstellungen für Schadsoftware verschieben Sie zunächst wie folgt den Fokus auf die Filtereinstellungen für Schadsoftware in der EAC:

1. In der Exchange-Verwaltungskonsole, um den Fokus auf den ersten Hyperlink im Navigationsbereich – **Dashboard** – zweimal drücken Sie STRG + F6. Sie hören "Dashboard primären Navigationslink..."
2. Drücken Sie im Navigationsbereich zum Verschieben des Fokus auf den Link **Schutz** so oft die TAB-TASTE, bis Sie „Schutz, primärer Navigationslink“ hören. Drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um den Fokus auf die Schutzeinstellungen im Inhaltsbereich der Seite zu verschieben, von denen der erste der Link **Schadsoftwarefilter** ist. Sie hören „Schadsoftwarefilter, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.

## Hinzufügen eines neuen Schadsoftwarefilters

1. [Verschieben des Fokus auf Ihre Filtereinstellungen für Schadsoftware in EAC](#)
2. Drücken Sie STRG+F6, um den Fokus zur Schaltfläche **Neu** zu verschieben. Sie hören „Schaltfläche 'Neu'“. Drücken Sie die EINGABETASTE.
3. Bewegen des Fokus zu Feld **Name** im Inhaltsbereich der **Antischadsoftware - Richtlinie** Popup-Fenster, das geöffnet wird, hören Sie "Antischadsoftware-Richtlinie, Name, Edit.."
4. Geben Sie im Popupfenster **Antischadsoftware-Richtlinie** neue Filtern an, z. B. Name, Beschreibung, Reaktion bei Schadsoftwareerkennung und Benachrichtigungen.

### TIP

Diese Seite enthält keinen Navigationsbereich. Drücken Sie die TAB-TASTE zum Verschieben des Fokus auf die einzelnen Einstellungen auf der Seite. Wenn Sie eine Einstellung auswählen, hören Sie Informationen zu dieser Einstellung. Zum Öffnen von Menüs drücken Sie die LEERTASTE. Zum Wechseln zwischen Menüoptionen und Auswählen von Menüoptionen drücken Sie die Pfeiltasten. Zum Auswählen einer Option drücken Sie die EINGABETASTE. Sie können auch die LEERTASTE drücken, um eine Kontrollkästchenmarkierung zu aktivieren oder zu deaktivieren .

5. Nachdem Sie die Tab-Taste auf der Registerkarte über alle Einstellungen auf der Seite geklickt haben, sind die letzten beiden Elemente auf der Seite die Schaltfläche **Speichern** und die Schaltfläche **Abbrechen**. Um eine der Schaltflächen aktivieren möchten, drücken Sie die EINGABETASTE.
6. Wie das **Antischadsoftware - Richtlinie** Popup-Fenster wird geschlossen, und der Fokus wieder auf die Schaltfläche Neu im Malware Filter Inhaltsbereich, hören Sie "Malware Filter, neue Schaltfläche..."

## Bearbeiten eines Schadsoftwarefilters

1. [Verschieben des Fokus auf Ihre Filtereinstellungen für Schadsoftware in EAC](#)
2. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
  - Die **Name** -Spalte. Sie hören "Spaltenüberschrift Name..."
  - Die Liste der Malware Filter in der Spalte **Name**. Sie hören den Namen des ersten Malware Filter gefolgt von "Schaltfläche..."

- Der erste Schadsoftwarefilter in der Liste. Sie hören den Namen des ersten Schadsoftwarefilters, gefolgt von „Zeile“.
3. Drücken Sie zum Verschieben des Fokus auf einen Ihrer Schadsoftwarefilter die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen des Filters hören, den Sie bearbeiten möchten. Drücken Sie die EINGABETASTE.
  4. Bewegen des Fokus zu Feld **Name** im Inhaltsbereich der **Antischadsoftware - Richtlinie** Popup-Fenster, das geöffnet wird, hören Sie "Antischadsoftware-Richtlinie, Name, Edit.."
  5. Geben Sie im Popupfenster **Antischadsoftware-Richtlinie** neue Filtern an, z. B. Name, Beschreibung, Reaktion bei Schadsoftwareerkennung und Benachrichtigungen.

#### TIP

Diese Seite enthält keinen Navigationsbereich. Drücken Sie die TAB-TASTE zum Verschieben des Fokus auf die einzelnen Einstellungen auf der Seite. Wenn Sie eine Einstellung auswählen, hören Sie Informationen zu dieser Einstellung. Zum Öffnen von Menüs drücken Sie die LEERTASTE. Zum Wechseln zwischen Menüoptionen und Auswählen von Menüoptionen drücken Sie die Pfeiltasten. Zum Auswählen einer Option drücken Sie die EINGABETASTE. Sie können auch die LEERTASTE drücken, um eine Kontrollkästchenmarkierung zu aktivieren oder zu deaktivieren .

6. Nachdem Sie die Tab-Taste auf der Registerkarte über alle Einstellungen auf der Seite geklickt haben, sind die letzten beiden Elemente auf der Seite die Schaltfläche **Speichern** und die Schaltfläche **Abbrechen**. Um eine der Schaltflächen aktivieren möchten, drücken Sie die EINGABETASTE.
7. Als **Antischadsoftware - Richtlinie** Popup-Fenster wird geschlossen, und der Fokus wechselt zurück zum Inhaltsbereich **Malware Filter** Sie hören "Malware filtern..."

## Löschen eines Schadsoftwarefilters

1. [Verschieben des Fokus auf Ihre Filtereinstellungen für Schadsoftware in EAC](#)
2. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
  - Die **Name** -Spalte. Sie hören "Spaltenüberschrift Name..."
  - Die Liste der Malware Filter in der Spalte **Name** . Sie hören den Namen des ersten Malware Filter gefolgt von "Schaltfläche..."
  - Der erste Schadsoftwarefilter in der Liste. Sie hören den Namen des ersten Schadsoftwarefilters, gefolgt von „Zeile“.
3. Drücken Sie zum Verschieben des Fokus auf einen Ihrer Schadsoftwarefilter die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen des Filters hören, den Sie löschen möchten.

#### TIP

Sie müssen einen Malware Filter deaktivieren, bevor Sie ihn löschen können. Informationen zum Deaktivieren ein Filters wechseln Sie zu [Aktivieren oder Deaktivieren einer schadsoftwarefilter](#) in diesem Thema.

4. Drücken Sie ENTF. Sie hören „Warnung, Möchten Sie die Richtlinie wirklich löschen?“ gefolgt vom Namen der Richtlinie. Um die Schaltfläche **Ja** auszuwählen, drücken Sie die EINGABETASTE. Um die Schaltfläche **Nein** auszuwählen, drücken Sie die TAB-TASTE und dann die EINGABETASTE.

## Aktivieren oder Deaktivieren eines Schadsoftwarefilters

1. [Verschieben des Fokus auf Ihre Filtereinstellungen für Schadsoftware in EAC](#)
2. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
  - Die **Name** -Spalte. Sie hören "Spaltenüberschrift Name..."
  - Die Liste der Malware Filter in der Spalte **Name**. Sie hören den Namen des ersten Malware Filter gefolgt von "Schaltfläche..."
  - Der erste Schadsoftwarefilter in der Liste. Sie hören den Namen des ersten Schadsoftwarefilters, gefolgt von „Zeile“.
3. Drücken Sie zum Verschieben des Fokus auf einen Ihrer Schadsoftwarefilter die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen des Filters hören, den Sie aktivieren oder deaktivieren möchten.
4. Zum Umschalten zwischen dem Aktivieren und Deaktivieren des Filters drücken Sie die LEERTASTE.

## Hören der Details für einen Schadsoftwarefilter

1. [Verschieben des Fokus auf Ihre Filtereinstellungen für Schadsoftware in EAC](#)
2. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
  - Die **Name** -Spalte. Sie hören "Spaltenüberschrift Name..."
  - Die Liste der Malware Filter in der Spalte **Name**. Sie hören den Namen des ersten Malware Filter gefolgt von "Schaltfläche..."
  - Der erste Schadsoftwarefilter in der Liste. Sie hören den Namen des ersten Schadsoftwarefilters, gefolgt von „Zeile“.
3. Drücken Sie zum Verschieben des Fokus auf einen Ihrer Schadsoftwarefilter die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen des Filters hören, dessen Details Sie hören möchten.
4. Drücken Sie die TAB-TASTE, um den Fokus auf den Detailbereich für den Schadsoftwarefilter zu verschieben. Sie hören die Details für den Filter.

# Verwenden einer Sprachausgabe zum Verwalten des Antispamschutzes in Exchange Online

18.12.2018 • 21 minutes to read

Exchange Online bietet Spamfilterfunktionen, die Ihr Netzwerk vor per E-Mail übertragenen Spamnachrichten schützen. Administratoren müssen diese standardmäßig aktivierten Filtertechnologien weder einrichten noch verwalten. Administratoren können jedoch unternehmensspezifische Filteranpassungen im Exchange Admin Center (EAC) vornehmen - und das alles mit Sprachausgabe und Tastenkombinationen.

## NOTE

Weitere Informationen zum Schutz Ihrer Organisation vor Spam in Exchange Online finden Sie unter [Anti-Spam and Anti-Malware Protection](#).

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie die entsprechende Office 365-Abonnement und Admin Rolle in der Exchange-Verwaltungskonsole ausgeführt haben. Klicken Sie dann die Exchange-Verwaltungskonsole öffnen und die ersten Schritte. Weitere Informationen zu der Exchange-Verwaltungskonsole finden Sie unter [Exchange Admin center in Exchange Online](#).

### Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Pop-up-Fenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### Bestätigen Ihres Office 365-Abonnementplans

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### Öffnen der EAC und Bestätigen Ihrer Administratorrolle

Zum Ausführen der Aufgaben in diesem Thema [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorrollengruppen [Organisationsverwaltung](#) und [Verwaltung von Nachrichtenschutz](#) zugewiesen hat. Erfahren Sie mehr über das [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Anpassen der Spamfiltereinstellungen

Exchange Online verwendet proprietäre Antispamtechnologie zur Erreichung hoher Genauigkeitsraten. Es bietet eine strikte Verbindungs- und Inhaltsfilterung für alle eingehenden Nachrichten.

### Verschieben des Fokus zu Ihren Spamfiltereinstellungen in EAC

Für die in diesem Thema behandelten Schritte zur Anpassung der Spamfiltereinstellungen verschieben Sie zunächst wie folgt den Fokus auf die Spamfiltereinstellungen in EAC:

1. In der Exchange-Verwaltungskonsole, um den Fokus auf den ersten Hyperlink im Navigationsbereich – **Dashboard** – drücken Sie STRG + F6 zweimal. Sie hören "Dashboard primären Navigationslink..."
2. Drücken Sie im Navigationsbereich zum Verschieben des Fokus auf **Schutz** so oft die TAB-TASTE, bis Sie „Schutz, primärer Navigationslink“ hören. Drücken Sie die EINGABETASTE.
3. Um den Fokus auf die Protection-Einstellungen im Inhaltsbereich der Seite, von denen die, der, der erste auf den Link **Malware Filter** ist, drücken Sie STRG + F6. Sie hören "Malware Filter, sekundäre Navigation verknüpfen..."
4. Zum Verschieben des Fokus auf den Link **Spamfilter** drücken Sie die TAB-TASTE, bis Sie hören „Spamfilter, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.

### Hinzufügen eines neuen Spamfilters

1. [Verschieben des Fokus zu Ihren Spamfiltereinstellungen in EAC](#).
2. Drücken Sie STRG+F6, um den Fokus zur Schaltfläche **Neu** zu verschieben. Sie hören „Schaltfläche ,Neu“. Drücken Sie die EINGABETASTE.
3. Bewegen des Fokus zu Feld **Name** im Inhaltsbereich **Filterrichtlinie für Spam** -Popup-Fenster, das geöffnet wird, hören Sie "Filterrichtlinie für Spam, Name, Edit..
4. In der \*\* Filterrichtlinie für Spam \*\* Popup-Fenster, neue filtereinstellungen wie Name, Beschreibung, Spam und Massen Aktionen festzulegen, blockierte Kontakte, Listen, internationale Spam und erweiterte Optionen zulassen.

#### TIP

Diese Seite enthält keinen Navigationsbereich. Drücken Sie die TAB-TASTE zum Verschieben des Fokus auf die einzelnen Einstellungen auf der Seite. Wenn Sie eine Einstellung auswählen, hören Sie Informationen zu dieser Einstellung. Zum Öffnen von Menüs drücken Sie die LEERTASTE. Zum Wechseln zwischen Menüoptionen und Auswählen von Menüoptionen drücken Sie die Pfeiltasten. Zum Auswählen einer Option drücken Sie die EINGABETASTE. Sie können auch die LEERTASTE drücken, um eine Kontrollkästchenmarkierung zu aktivieren oder zu deaktivieren .

5. Nachdem Sie die Tab-Taste auf der Registerkarte über alle Einstellungen auf der Seite geklickt haben, werden die letzten beiden Elemente auf der Seite die Schaltfläche **Speichern** und die \*\* Abbrechen \*\* Schaltfläche. Um eine der Schaltflächen aktivieren möchten, drücken Sie die EINGABETASTE.
6. Wie das **Richtlinie für Spam-Filter** Popup-Fenster wird geschlossen, und der Fokus wieder auf die Schaltfläche **neu** im **Spam-Filter** Inhaltsbereich, hören Sie "Spam-Filter, neue Schaltfläche..."

### Bearbeiten eines vorhandenen Spamfilters

1. [Verschieben des Fokus zu Ihren Spamfiltereinstellungen in EAC](#).
2. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
  - Die **Name** -Spalte. Sie hören "Spaltenüberschrift Name..."
  - Die Liste der Spam-Filter in der Spalte **Name** . Sie hören den Namen des ersten Spam-Filter gefolgt von

"Schaltfläche...

- Der erste Spamfilter in der Liste. Sie hören den Namen des ersten Spamfilters gefolgt von „Zeile“.
3. Drücken Sie zum Verschieben des Fokus auf einen Ihrer Spamfilter die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen des Filters hören, den Sie bearbeiten möchten. Drücken Sie die EINGABETASTE.
4. Wie der Fokus auf den Link im Navigationsbereich im Popupfenster **Spam-Filter-Richtlinie bearbeiten**, das geöffnet wird, die **Allgemein** für den Filter, hören Sie "Spam-Filter Policy, ausgewählte, allgemeine bearbeiten..."
5. Klicken Sie im Navigationsbereich im Popupfenster **Spam-Filter-Richtlinie bearbeiten** der Pfeiltasten zwischen verschieben, und wählen die Links im Navigationsbereich auf der Seite mit den Einstellungen entsprechend bearbeitet werden können: **Allgemein, Spam und Massen-Aktionen., Sperrlisten, Listen ermöglichen, internationale Spam und Erweiterte Optionen.**

**TIP**

Wenn ein Link im Navigationsbereich ausgewählt ist, drücken Sie die TAB-TASTE, um den Fokus in den Inhaltsbereich der Seite zu verschieben. Um die Elemente im Inhaltsbereich zu durchlaufen und auszuwählen, drücken Sie die TAB-TASTE. Wenn Sie eine Einstellung auswählen, hören Sie Informationen zu dieser Einstellung. Zum Öffnen von Menüs drücken Sie die LEERTASTE. Zum Wechseln zwischen Menüoptionen und Auswählen von Menüoptionen drücken Sie die Pfeiltasten. Zum Auswählen einer Option drücken Sie die EINGABETASTE. Sie können auch die LEERTASTE drücken, um eine Kontrollkästchenmarkierung zu aktivieren oder zu deaktivieren .

6. Nachdem Sie die Einstellungen für den Filter angepasst und zur Registerkarte alle Links im Popupfenster **Spam-Filter-Richtlinie bearbeiten** über die Tab-Taste gedrückt haben, sind die letzten beiden Elemente auf der Seite die Schaltfläche **Speichern** und die Schaltfläche **Abbrechen**. Um eine der Schaltflächen aktivieren möchten, drücken Sie die EINGABETASTE.
7. Als das Popup-Fenster geschlossen und der Fokus wechselt zurück zum **Spam-Filter** Inhaltsbereich hören Sie "Spam-Filter..."

### Löschen eines Spamfilters

1. [Verschieben des Fokus zu Ihren Spamfiltereinstellungen in EAC.](#)
2. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
  - Die **Name** -Spalte. Sie hören "Spaltenüberschrift Name..."
  - Die Liste der Spam-Filter in der Spalte **Name**. Sie hören den Namen des ersten Spam-Filter gefolgt von "Schaltfläche..."
  - Der erste Spamfilter in der Liste. Sie hören den Namen des ersten Spamfilters gefolgt von „Zeile“.
3. Drücken Sie zum Verschieben des Fokus auf einen Ihrer Spamfilter die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen des Filters hören, den Sie löschen möchten.

**TIP**

Sie müssen einen Spam-Filter deaktivieren, bevor Sie ihn löschen können. Wechseln Sie zu [Aktivieren oder deaktivieren einen Spam-Filter](#) in diesem Thema, um weitere Informationen zum Deaktivieren eines Filters.

4. Drücken Sie ENTF. Sie hören „Warnung, Möchten Sie die Richtlinie wirklich löschen?“ gefolgt vom Namen der Richtlinie. Um die Schaltfläche **Ja** auszuwählen, drücken Sie die EINGABETASTE. Um die Schaltfläche

**Nein** auszuwählen, drücken Sie die TAB-TASTE und dann die EINGABETASTE.

### Aktivieren oder Deaktivieren eines Spamfilters

1. [Verschieben des Fokus zu Ihren Spamfiltereinstellungen in EAC.](#)
2. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
  - Die **Name** -Spalte. Sie hören "Spaltenüberschrift Name..."
  - Die Liste der Spam-Filter in der \*\* Namen \*\* Spalte. Sie hören den Namen des ersten Spam-Filter gefolgt von "Schaltfläche..."
  - Der erste Spamfilter in der Liste. Sie hören den Namen des ersten Spamfilters gefolgt von „Zeile".
3. Drücken Sie zum Verschieben des Fokus auf einen Ihrer Spamfilter die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen des Filters hören, den Sie aktivieren oder deaktivieren möchten.
4. Zum Umschalten zwischen dem Aktivieren und Deaktivieren des Filters drücken Sie die LEERTASTE.

### Hören der Details für einen Spamfilter

1. [Verschieben des Fokus zu Ihren Spamfiltereinstellungen in EAC.](#)
2. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
  - Die **Name** -Spalte. Sie hören "Spaltenüberschrift Name..."
  - Die Liste der Spam-Filter in der Spalte **Name**. Sie hören den Namen des ersten Spam-Filter gefolgt von "Schaltfläche..."
  - Der erste Spamfilter in der Liste. Sie hören den Namen des ersten Spamfilters gefolgt von „Zeile".
3. Drücken Sie zum Verschieben des Fokus auf einen Ihrer Spamfilter die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen des Filters hören, dessen Details Sie hören möchten.
4. Drücken Sie die TAB-TASTE, um den Fokus auf den Detailbereich für den Spamfilter zu verschieben. Sie hören die Details für den Filter.

## Anpassen der Einstellungen für ausgehende Spammnachrichten

Sie können auch die proprietäre Antispamtechnologie in Exchange Online verwenden, um Spam in ausgehender E-Mail zu filtern.

### Verschieben des Fokus zu Ihren Einstellungen für ausgehende Spammnachrichten in EAC

Für die in diesem Thema behandelten Schritte zur Anpassung der Einstellungen für ausgehende Spammnachrichten verschieben Sie zunächst wie folgt den Fokus auf die Einstellungen für ausgehende Spammnachrichten in EAC:

- In der Exchange-Verwaltungskonsole, um den Fokus auf den ersten Hyperlink im Navigationsbereich – **Dashboard** – drücken Sie STRG + F6 zweimal. Sie hören "Dashboard primären Navigationslink..."
- Drücken Sie im Navigationsbereich zum Verschieben des Fokus auf den Link **Schutz** so oft die TAB-TASTE, bis Sie „Schutz, primärer Navigationslink" hören. Drücken Sie die EINGABETASTE.
- Um den Fokus auf die Protection-Einstellungen im Inhaltsbereich der Seite, von denen die, der, der erste auf den Link **Malware Filter** ist, drücken Sie STRG + F6. Sie hören "Malware Filter, sekundäre Navigation verknüpfen..."
- Zum Verschieben des Fokus auf den Link **Ausgehende Spammnachrichten** drücken Sie die TAB-TASTE, bis Sie hören „Ausgehende Spammnachrichten, sekundärer Navigationslink". Drücken Sie die

EINGABETASTE.

## Bearbeiten der Einstellungen für ausgehende Spammnachrichten

1. [Verschieben des Fokus zu Ihren Einstellungen für ausgehende Spammnachrichten in EAC.](#)
2. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
  - Die **Name**-Spalte. Sie hören "Spaltenüberschrift Name..."
  - Die Liste der ausgehenden Spam-Filter in der Spalte **Name**. Sie hören den Namen des ersten ausgehenden Spammnachrichten Filters gefolgt von "Schaltfläche..."
  - Der erste Filter für ausgehendes Spam in der Liste. Sie hören den Namen des ersten Filters für ausgehendes Spam, gefolgt von „Zeile“.
3. Drücken Sie zum Verschieben des Fokus auf einen Ihrer Filter für ausgehendes Spam die NACH-OBEN- oder NACH-UNTEN-TASTE, bis Sie den Namen des Filters hören, den Sie bearbeiten möchten. Drücken Sie die EINGABETASTE.
4. Wie der Fokus auf den Link **Allgemein** im Popupfenster **Spam-Filter-Richtlinie bearbeiten** im Navigationsbereich verschoben, das geöffnet wird wird, hören Sie "Spam-Filter Policy, ausgewählte, allgemeine bearbeiten..."
5. Drücken Sie im Navigationsbereich im Popupfenster **Spamfilterrichtlinie bearbeiten** die NACH-OBEN- oder NACH-UNTEN-TASTE, um zwischen Links im Navigationsbereich zu wechseln und diese auszuwählen. Die Links entsprechen den Optionen, die Sie bearbeiten können: **Allgemein** und **Einstellungen für ausgehenden Spam**.

### TIP

Wenn ein Link im Navigationsbereich ausgewählt ist, drücken Sie die TAB-TASTE, um den Fokus in den Inhaltsbereich der Seite zu verschieben. Um die Elemente im Inhaltsbereich zu durchlaufen und auszuwählen, drücken Sie die TAB-TASTE. Wenn Sie eine Einstellung auswählen, hören Sie Informationen zu dieser Einstellung. Zum Öffnen von Menüs drücken Sie die LEERTASTE. Zum Wechseln zwischen Menüoptionen und Auswählen von Menüoptionen drücken Sie die Pfeiltasten. Zum Auswählen einer Option drücken Sie die EINGABETASTE. Sie können auch die LEERTASTE drücken, um die Markierung für Kontrollkästchen zu aktivieren oder zu deaktivieren .

6. Nachdem Sie die Optionen in den Einstellungen für ausgehenden Spam angepasst und mit der TAB-TASTE alle Links im Fenster durchlaufen haben, sind die beiden letzten Elemente auf der Seite die Schaltfläche **Speichern** und die Schaltfläche **Abbrechen**. Drücken Sie die EINGABETASTE, um eine Schaltfläche zu aktivieren.
7. Als **Spam-Filter-Richtlinie bearbeiten** Popup-Fenster wird geschlossen, und der Fokus wechselt zurück zum Spam-Filter Inhaltsbereich, hören Sie "Spam-Filter..."

## Hören der Details zu einer Einstellung für ausgehenden Spam

1. [Verschieben des Fokus zu Ihren Einstellungen für ausgehende Spammnachrichten in EAC.](#)
2. Zum Verschieben des Fokus auf jedes der folgenden drei Elemente der Benutzeroberfläche drücken Sie die TAB-TASTE:
  - Die **Name**-Spalte. Sie hören "Spaltenüberschrift Name..."
  - Die Liste der ausgehenden Spam-Filter in der Spalte **Name**. Sie hören den Namen des ersten ausgehenden Spammnachrichten Filters gefolgt von "Schaltfläche..."
  - Der erste Filter für ausgehendes Spam in der Liste. Sie hören den Namen des ersten Filters für ausgehendes Spam, gefolgt von „Zeile“.

ausgehendes Spam, gefolgt von „Zeile“.

3. Drücken Sie zum Verschieben des Fokus auf einen Ihrer Filter für ausgehenden Spam die NACH-OBEN- oder NACH-UNTEN-TASTE, bis Sie den Namen des Filters hören, dessen Details Sie hören möchten.
4. Drücken Sie die TAB-TASTE, um den Fokus auf den Detailbereich für den Filter für ausgehenden Spam zu verschieben. Sie hören die Details für den Filter.

# Verwenden Sie eine Bildschirmsprachausgabe So öffnen Sie die Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 5 minutes to read

Der Exchange-Verwaltungskonsole (EAC) ist eine webbasierte app, die Sie in einem Webbrowser Ihrer Exchange Online-Organisation verwalten kann. Eine Bildschirmsprachausgabe und Tastenkombinationen verwenden, können Sie der Exchange-Verwaltungskonsole öffnen und Ausführen von Verwaltungsaufgaben (basierend auf Ihren Berechtigungen).

## NOTE

Wenn Sie in der Exchange-Verwaltungskonsole verwenden, wird empfohlen, dass Sie Internet Explorer als Webbrowser verwenden. Weitere Informationen zu den Tastenkombinationen können Sie mithilfe der Exchange-Verwaltungskonsole zu navigieren und zu anderen Eingabehilfen-Features, die für Exchange Online zur Verfügung stehen, finden Sie unter [erfahren Sie mehr über die Tastenkombinationen für Internet Explorer](#) und [Eingabehilfen in Exchange Online](#).

1. Melden Sie sich beim Office 365-Konto Ihres Unternehmens an. Verschieben Sie im **App-Startfeld** den Fokus auf die **Admin** -App. Sie hören „Wechseln Sie zum Office 365 Admin Center, Link“. Drücken Sie die EINGABETASTE.

## TIP

Wenn Sie die Seite **Meine Apps** zum Öffnen Ihrer Apps verwenden, gelangen Sie schnell zur **Admin** -App (manchmal eine der letzten Apps in der Liste), indem Sie den Fokus auf das Feld **Apps suchen** verschieben (eines der ersten Elemente auf der Seite). In JAWS hören Sie „Menüs verlassen, Meine Apps, Bearbeiten, Text eingeben“. In der Sprachausgabe hören Sie „Apps suchen, Bearbeiten“. Geben Sie „admin“ ein, und verschieben Sie dann den Fokus auf das einzige Suchergebnis auf der Seite: **Admin** -App. Sie hören „Admin Link“. Drücken Sie die EINGABETASTE.

2. Wie das **Office 365 Administrationscenter** wird, in JAWS geöffnet, hören "Office 365, Office Administrationscenter, Home." In die Sprachausgabe, hören Sie "Office 365, bearbeiten..."
3. Um den Fokus auf den Link **Erweitern** Sie im Navigationsbereich, drücken Sie die Tab-Taste, bis Sie eine der folgenden zwei Optionen hören.
  - „Erweitern Navigationsmenüschaltfläche“. Um den Navigationsbereich zu erweitern, drücken Sie die LEERTASTE.
  - „Reduzieren Navigationsmenüschaltfläche“. Der Navigationsbereich ist bereits erweitert, somit ist keine Aktion erforderlich.
4. Drücken Sie die Tab-Taste, um den Fokus auf **Admin centers** (das letzte Element im Navigationsbereich), bis Sie hören "Admin zentriert..."
5. Um sicherzustellen, dass die Liste **Admin Center** erweitert wird, sodass Sie die Elemente darauf zugreifen können, drücken Sie die Tab-Taste. Klicken Sie dann, basierend auf der akustische Feedback, das Sie hören, führen Sie eine der folgenden beiden Aktionen.

- Wenn Sie hören „Exchange-Link, Exchange Admin Center in neuer Registerkarte öffnen“, ist die Liste bereits erweitert und Sie haben **Exchange** ausgewählt.
  - Wenn Sie einen anderen Wert als "Exchange-Verknüpfung, Open Exchange Administrationscenter in einer neuen Registerkarte" hören ist die Liste ausgeblendet. Drücken Sie Umschalt + Tab, um den Fokus wieder zurück in die Liste **Admin zentriert** verschieben. Drücken Sie die EINGABETASTE, um die Liste zu erweitern. In der erweiterten **Admin zentriert** Liste, um **Exchange**, wählen die Tab-Taste drücken, bis Sie hören "Exchange-Verknüpfung, Open Exchange-Verwaltungskonsole in einer neuen Registerkarte..
6. Drücken Sie die EINGABETASTE, um die **Exchange-Verwaltungskonsole** zu öffnen. Wie der **Exchange-Verwaltungskonsole** in einer neuen Registerkarte im Webbrower in JAWS, öffnet, hören Sie "Exchange-Verwaltungskonsole". In die Sprachausgabe hören Sie "Microsoft Exchange..."
  7. Zum Verschieben des Fokus **Dashboard** (den ersten Hyperlink), in der **Exchange-Verwaltungskonsole** im Navigationsbereich, drücken Sie STRG + F6 zweimal. In die Sprachausgabe hören Sie "Dashboard primären Navigationslink..."

**TIP**

Wenn für den Rest der Elemente im Navigationsbereich verschieben möchten, drücken Sie die Tab-Taste. Um ein Element zu öffnen, drücken Sie die EINGABETASTE. Drücken Sie STRG + F6, nachdem Sie ein Element, verschieben Sie direkt zu einem seiner Elemente im Inhaltsbereich auf einer Seite geöffnet haben. Zum Identifizieren der Admin-Rolle finden Sie unter Gruppen, die Sie zugewiesen wurde, die die Aufgaben zu, die in der Exchange-Verwaltungskonsole ausgeführt werden können bestimmen, [Verwenden Sie eine Bildschirmsprachausgabe, um die Admin-Rolle in der Exchange-Verwaltungskonsole zu ermitteln.](#)

# Verwenden Sie eine Bildschirmsprachausgabe zur Ausführung der eines Überwachungsberichts in der Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 46 minutes to read

Sie können mithilfe der Sprachausgabe im Exchange-Verwaltungskonsole (EAC) in Exchange Online Überwachungsberichte ausführen und nach Überwachungsinformationen suchen. Bestimmte Überwachungsberichte helfen Ihnen dabei, Konfigurationsprobleme zu behandeln, indem Sie spezifische, von Administratoren vorgenommene Änderungen nachverfolgen. Mit anderen Berichten können Sie gesetzliche Bestimmungen überwachen und Daten, die für Rechtsstreitigkeiten erforderlich sind, aufbewahren.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zur Verwendung der Exchange-Verwaltungskonsole verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Popupfenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### **Bestätigen Ihres Office 365-Abonnementplans**

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### **Öffnen von EAC und Bestätigen Ihrer Administratorrolle**

Zum Ausführen von Überwachungsberichten [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorrollengruppen „Organisationsverwaltung“ und „Datensatzverwaltung“ zugewiesen hat. Für die Ausführung von In-Situ-eDiscovery- und In-Situ-Speicher-Berichten überprüfen Sie, dass Sie der Rollengruppe „Discoveryverwaltung“ zugeordnet sind. Erfahren Sie mehr über das [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Suchen von Daten zum Behandeln von Konfigurations- und Sicherheitsproblemen

Behandeln Sie Konfigurationsprobleme, indem Sie die protokollierten Informationen über Postfachzugriffe von Nicht-Besitzern, Konfigurationsänderungen von Exchange Online und Updates von Administratorrollengruppen untersuchen. Diese Informationen sind auf der Registerkarte **Verwaltung der Compliance** und auf der Seite **Überwachung** von EAC verfügbar.

## Suchen nach Postfachzugriffen durch Nicht-Besitzer

Bei aktivierter Exchange-Postfachüberwachung für ein Postfach werden im Postfachüberwachungsprotokoll Informationen protokolliert, wenn ein Benutzer, bei dem es sich nicht um den Besitzer des Postfachs handelt, auf das Postfach zugreift. Jeder Protokolleintrag enthält Informationen darüber, wer auf das Postfach zugegriffen hat und welche Aktionen ausgeführt wurden. Suchen Sie bei der Behandlung von möglichen Sicherheitsproblemen nach Postfachzugriffen durch Nicht-Besitzer.

### NOTE

Vor der Suche für den Postfachzugriff nicht-Besitzer können, müssen Sie oder ein anderes Admin Mailbox Audit Protokollierung aktivieren in Exchange Online PowerShell ausgeführt wird. [Erfahren Sie mehr über einen nicht-Besitzer Postfach Access-Bericht ausführen.](#)

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis der Fokus auf **Verwaltung der Compliance** liegt, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen.
4. Drücken Sie die TAB-TASTE, bis der Fokus auf **Überwachung** liegt. Sie hören „Überwachung, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.
5. Zugriff auf die Listenansicht im Hauptfenster drücken Sie STRG + F6. Sie hören "Audit meldet..."
6. Drücken Sie die TAB-TASTE ungefähr dreimal, bis Sie hören „Bericht für Nicht-Besitzer-Postfachzugriff ausführen“. Drücken Sie die EINGABETASTE.
7. Im Dialogfeld **Suchen auf die Postfächer von nicht-Besitzer zugegriffen**, das geöffnet wird, das **Starten des Jahres** Kombinationsfeld den Fokus hat, und hören Sie "Start Datum Kombinationsfelds Jahr..."

### TIP

Standardmäßig wird das Startdatum auf zwei Wochen vor dem gestrigen Datum festgelegt. Wenn aktiviert, werden im Postfachüberwachungsprotokoll normalerweise Einträge für 90 Tage gespeichert.

- a. Geben Sie ggf. das Jahr des Startdatums für die Suche nach Konfigurationsänderungen durch den Administrator ein. Sie können das Jahr des Startdatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
  - b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Startdatums ein bzw. wählen Sie ihn aus.
  - c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Startdatums ein bzw. wählen Sie ihn aus.
8. Registerkarte an das **Ende des Jahres**-Kombinationsfeld. Sie hören "Year-End Date Kombinationsfelds..."

### TIP

Der Standardwert des Enddatums ist das heutige Datum.

- a. Geben Sie ggf. das Jahr des Enddatums für die Suche nach Konfigurationsänderungen durch den Administrator ein. Sie können das Jahr des Enddatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.

- b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Enddatums ein bzw. wählen Sie ihn aus.
  - c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Enddatums ein bzw. wählen Sie ihn aus.
9. Drücken Sie die TAB-TASTE, um auf die Schaltfläche **Suchen** zuzugreifen, und drücken Sie die EINGABETASTE.

#### TIP

Wenn Sie alle Postfächer nach Zugriffen durch Nicht-Besitzer durchsuchen möchten, wählen Sie keine bestimmten Postfächer aus, und gehen Sie zu Schritt 10. Wenn das Feld **Diese Postfächer durchsuchen** leer ist, umfasst die Suche alle Postfächer.

- a. Zum Öffnen des Dialogfelds **Postfach auswählen** drücken Sie, während der Fokus auf der Schaltfläche zum Auswählen von Postfächern liegt, die EINGABETASTE. Das Feld **Suche** besitzt den Fokus, und Sie hören „Filter oder Suche bearbeiten“. Geben Sie den Namen des ersten Postfachs ganz oder teilweise ein, das Sie in die Suche nach Postfachzugriffen durch Nicht-Besitzer einschließen möchten, und drücken Sie dann die EINGABETASTE, um nach dem Namen zu suchen.
- b. Drücken Sie zur Auswahl eines Postfachs etwa viermal die TAB-TASTE, bis Sie den Namen des Postfachbesitzers in der Liste der Suchergebnisse hören. Wenn die Liste der Suchergebnisse mehrere Postfächer enthält, drücken Sie die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen des Postfachbesitzers hören.

#### TIP

Es können mehrere aufeinanderfolgende Postfächer ausgewählt werden. Zum Arbeiten mit allen Postfächern lassen Sie das Feld **Suche** leer, oder geben Sie ganz oder teilweise die Postfachnamen ein, die Sie hinzufügen möchten. Wechseln Sie mit der TAB-TASTE zu den Suchergebnissen. Drücken Sie die NACH-UNTEN-TASTE, um jeden Namen zu hören. Wenn alle hinzufügen möchten, drücken Sie STRG+A. Wenn Sie mehrere nacheinander aufgelistete Postfächer hinzufügen möchten, drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, bis Sie den ersten Postfachnamen hören, den Sie hinzufügen möchten. Halten Sie die UMSCHALTTASTE gedrückt, drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, bis Sie den letzten Postfachnamen hören, den Sie hinzufügen möchten, und lassen Sie dann die UMSCHALTTASTE los. Alle Postfächer zwischen dem ersten und letzten Postfachnamen werden ausgewählt.

- c. Drücken Sie die EINGABETASTE, um die ausgewählten Postfächer zu der Liste hinzuzufügen, die in die Suche nach Postfachzugriffen durch Nicht-Besitzer eingeschlossen werden soll. Die Liste der Postfächer behält den Fokus, sodass Sie weitere Postfächer hinzufügen können, indem Sie sie auswählen und die EINGABETASTE drücken.

#### TIP

Zum Überprüfen der hinzugefügten Postfächer wechseln Sie mit der TAB-TASTE zur Schaltfläche **Hinzufügen**. Um die Liste der Postfächer anzuhören, drücken Sie die TAB-TASTE erneut. Sie hören den ersten Postfachnamen in der Liste. Um den zweiten Postfachnamen in der Liste zu hören, drücken Sie noch einmal die TAB-TASTE. Drücken Sie weiterhin die TAB-TASTE, bis Sie die Namen aller hinzugefügten Postfächer gehört haben. Um ein Postfach aus der Liste zu löschen, aktivieren Sie den Link **Entfernen** durch Drücken der EINGABETASTE, wenn Sie den Postfachnamen hören.

- d. Um ein anderes Postfach oder eine andere Gruppe von Postfächern zu suchen, drücken Sie mehrmals die TAB-TASTE, bis Sie hören „Filter oder Suche bearbeiten“. Geben Sie ganz oder

teilweise den Namen der nächsten Postfächer ein, die Sie hinzufügen möchten, und drücken die EINGABETASTE. Wiederholen Sie die Schritte b und c. Tun Sie dies für alle Postfächer, die Sie hinzufügen möchten.

- e. Um ein externes Postfach hinzuzufügen, drücken Sie die TAB-TASTE, bis Sie hören „Namen überprüfen bearbeiten, Text eingeben“. (In Sprachausgabe hören Sie „Bearbeiten“.) Geben Sie die E-Mail-Adresse des externen Empfängers ein, drücken Sie UMSCHALT+TAB, um die Schaltfläche **Namen überprüfen** auszuwählen, und drücken Sie dann die EINGABETASTE. Dadurch wird die E-Mail-Adresse überprüft und zur Liste der Postfächer hinzugefügt.

**TIP**

Beachten Sie: Wenn Sie eine externe E-Mail-Adresse eingeben und die EINGABETASTE drücken, wird die Adresse der Liste hinzugefügt und das Dialogfeld geschlossen. Wenn Sie noch nicht fertig sind, verwenden Sie stattdessen die Schaltfläche **Namen überprüfen**, um sie hinzuzufügen.

- f. Wenn Sie mit dem Hinzufügen von Postfächern fertig sind, wechseln Sie mit der TAB-TASTE zur Schaltfläche **OK**, und drücken Sie die EINGABETASTE. Das Dialogfeld **Nach Postfächern mit Zugriff durch Nicht-Besitzer suchen** hat wieder den Fokus, und im Textfeld **Diese Postfächer durchsuchen** sind die ausgewählten Postfächer aufgeführt.
10. Wechseln Sie mit der TAB-TASTE zum Kombinationsfeld **Suchen nach Zugriff durch**. Dies gibt an, welche Arten von Nicht-Besitzern im Bericht zum Postfachzugriff durch Nicht-Besitzer angezeigt werden soll.
- Wenn Sie die Überwachungsprotokolle nach Administratorzugriff durchsuchen möchten, müssen Sie nichts weiter tun, da dies der Standardwert ist.
  - Um die Überwachungsprotokolle nach einer anderen Gruppe von Nicht-Besitzern zu durchsuchen, z. B. **Alle Nicht-Besitzer, Externe Benutzer** (Microsoft-Datencenteradministratoren) oder **Administratoren und delegierte Benutzer**, drücken Sie die NACH-OBEN-TASTE, um zum gewünschten Benutzertyp zu wechseln.
11. Drücken Sie die TAB-TASTE, um auf die Schaltfläche **Suchen** zuzugreifen, und drücken Sie die EINGABETASTE.
12. Drücken Sie etwa viermal die TAB-TASTE, um auf die Suchergebnisse zuzugreifen. Wenn auf Postfächer im angegebenen Zeitraum durch einen Nicht-Besitzer des angegebenen Typs zugegriffen wurde, hören Sie den Namen des Postfachbesitzers und das Datum, zu dem durch einen Nicht-Besitzer auf das Postfach zugegriffen wurde. Wenn auf keines der Postfächer durch einen Nicht-Besitzer zugegriffen wurde, hören Sie „Es gibt keine Elemente, die in dieser Ansicht angezeigt werden können“. (In Sprachausgabe hören Sie „Enthält 0 Elemente“.)
13. Für weitere Details zu einem Postfachzugriff durch Nicht-Besitzer drücken Sie, während das Element in der Liste der Suchergebnisse ausgewählt ist, die TAB-TASTE, um in den Bereich **Details** zu wechseln. Zum Drucken des Inhalts des Bereichs **Details** drücken Sie die EINGABETASTE. Zum Anhören des Inhalts des Bereichs **Details** drücken Sie erneut die TAB-TASTE.
14. Um das Dialogfeld zu schließen, wechseln Sie mit der TAB-TASTE zur Schaltfläche **Schließen**, und drücken Sie die EINGABETASTE.

**TIP**

Sie können das Protokoll des Postfachzugriffs durch Nicht-Besitzer auch exportieren und in einer XML-Datei überprüfen. Weitere Informationen finden Sie unter [Verwenden einer Sprachausgabe zum Exportieren und Überprüfen von Überwachungsprotokollen im Exchange Admin Center](#).

## Suchen nach Konfigurationsänderungen für ein Postfach

Mit der Administrator-Überwachungsprotokollierung zeichnet Exchange bestimmte Änderungen auf, die ein Administrator an der Konfiguration Exchange der Organisation vornimmt. Derartige Änderungen können das Hinzufügen von Benutzern, das Hinzufügen von öffentlichen Ordnern, das Erstellen von Richtlinien oder Regeln und Ähnliches umfassen. Diese Informationen können Sie zur Behandlung von Konfigurationsproblemen bzw. zum Ermitteln der Ursache von Sicherheits- oder Complianceproblemen heranziehen. [Erfahren Sie mehr über das Anzeigen des Administratorüberwachungsprotokolls.](#)

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis der Fokus auf **Verwaltung der Compliance** liegt, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen.
4. Drücken Sie die TAB-TASTE, bis der Fokus auf **Überwachung** liegt. Sie hören „Überwachung, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.
5. Zugriff auf die Listenansicht im Hauptfenster drücken Sie STRG + F6. Sie hören "Audit meldet..."
6. Drücken Sie etwa 12-mal die TAB-TASTE, bis Sie hören „Administratorüberwachungsprotokoll-Bericht ausführen“. Drücken Sie die EINGABETASTE.
7. **Anzeigen des Administratorüberwachungsprotokolls** im Dialogfeld, das geöffnet wird, das **Starten des Jahres** Kombinationsfeld den Fokus hat, und hören Sie "Start Datum Kombinationsfelds Jahr..."

### TIP

Standardmäßig wird das Startdatum auf zwei Wochen vor dem gestrigen Datum festgelegt. Im Postfachüberwachungsprotokoll werden normalerweise Einträge für 90 Tage gespeichert.

- a. Geben Sie ggf. das Jahr des Startdatums für die Suche nach Konfigurationsänderungen durch den Administrator ein. Sie können das Jahr des Startdatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
- b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Startdatums ein bzw. wählen Sie ihn aus.
- c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Startdatums ein bzw. wählen Sie ihn aus.
8. Registerkarte an das **Ende des Jahres** -Kombinationsfeld. Sie hören "Year-End Date Kombinationsfelds..."

### TIP

Der Standardwert des Enddatums ist das heutige Datum.

- a. Geben Sie ggf. das Jahr des Startdatums für die Suche nach Konfigurationsänderungen durch den Administrator ein. Sie können das Jahr des Enddatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
- b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Enddatums ein bzw. wählen Sie ihn aus.
- c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Enddatums ein bzw. wählen Sie ihn aus.

9. Drücken Sie die TAB-TASTE, um auf die Schaltfläche **Suchen** zuzugreifen, und drücken Sie die EINGABETASTE.
10. Drücken Sie etwa fünfmal die TAB-TASTE, um auf die Suchergebnisse zuzugreifen. Drücken Sie die NACH-UNTEN-TASTE bzw. die NACH-OBEN-TASTE, um die Liste der Konfigurationsänderungen im angegebenen Zeitraum zu hören. Für jedes Element hören Sie das Datum der Änderung, die Art der Konfigurationsänderung und den Namen des Administrators, der die Änderung vorgenommen hat. Wenn keine Konfigurationsänderungen vorhanden sind, hören Sie „Es gibt keine Elemente, die in dieser Ansicht angezeigt werden können“. (In Sprachausgabe, hören Sie „Enthält 0 Elemente“.)
11. Für weitere Details zu einer Konfigurationsänderung drücken Sie, während die Änderung in der Liste der Suchergebnisse ausgewählt ist, die TAB-TASTE, um in den Bereich **Details** zu wechseln. Zum Drucken des Inhalts des Bereichs **Details** drücken Sie die EINGABETASTE. Zum Anhören des Inhalts des Bereichs **Details** drücken Sie erneut die TAB-TASTE.
12. Um das Dialogfeld zu schließen, wechseln Sie mit der TAB-TASTE zur Schaltfläche **Schließen**, und drücken Sie die EINGABETASTE.

#### TIP

Sie können das Administratorüberwachungsprotokoll auch in eine XML-Datei exportieren und per E-Mail an die angegebenen Empfänger senden. Drücken Sie auf der Seite „Überwachung“ so oft die TAB-TASTE, bis Sie hören „Administratorüberwachungsprotokoll exportieren“. Drücken die EINGABETASTE, und bearbeiten Sie das angezeigte Dialogfeld **Administratorüberwachungsprotokoll exportieren**. Weitere Informationen finden Sie unter [Verwenden einer Sprachausgabe zum Exportieren und Überprüfen von Überwachungsprotokollen im Exchange Admin Center](#).

## Suchen nach Änderungen an Administratorrollengruppen

Sie können nach Änderungen an Administratorrollen suchen, die wie Konfigurationsänderungen im Administratorüberwachungsprotokoll aufgezeichnet werden. Mit einer gezielten Suche können Sie das Administratorüberwachungsprotokoll nach Änderungen durchsuchen, die an Rollengruppen vorgenommen wurden, die zum Zuweisen von Administratorberechtigungen an Benutzer dienen. [Erfahren Sie mehr über das Ausführen eines Berichts für Administratorrollengruppen](#).

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis der Fokus auf **Verwaltung der Compliance** liegt, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen.
4. Drücken Sie die TAB-TASTE, bis der Fokus auf „Überwachung“ liegt. Sie hören „Überwachung, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.
5. Zugriff auf die Listenansicht im Hauptfenster drücken Sie STRG + F6. Sie hören "Audit meldet..."
6. Drücken Sie etwa neunmal die TAB-TASTE, bis Sie hören „Administrator-Rollengruppenbericht ausführen“. Drücken Sie die EINGABETASTE.
7. Im Dialogfeld **Suchen nach Änderungen an Administrative Rollengruppen**, das geöffnet wird, das **Starten des Jahres** Kombinationsfeld den Fokus hat, und hören Sie "Start Datum Kombinationsfelds Jahr..."

#### TIP

Standardmäßig wird das Startdatum auf zwei Wochen vor dem gestrigen Datum festgelegt. Im Postfachüberwachungsprotokoll werden normalerweise Einträge für 90 Tage gespeichert.

- a. Geben Sie ggf. das Jahr des Startdatums für die Suche nach Änderungen an Administratorrollengruppen ein. Sie können das Jahr des Startdatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
- b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Startdatums ein bzw. wählen Sie ihn aus.
- c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Startdatums ein bzw. wählen Sie ihn aus.

8. Registerkarte an das **Ende des Jahres**-Kombinationsfeld. Sie hören "Year-End Date Kombinationsfelds..."

**TIP**

Der Standardwert des Enddatums ist das heutige Datum.

- a. Geben Sie ggf. das Jahr des Startdatums für die Suche nach Änderungen an Administratorrollengruppen ein. Sie können das Jahr des Enddatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
  - b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Enddatums ein bzw. wählen Sie ihn aus.
  - c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Enddatums ein bzw. wählen Sie ihn aus.
9. Zugriff auf die Schaltfläche **Rollengruppen auswählen**, drücken Sie zweimal die Tab-Taste. Sie hören "Diese Rollengruppen suchen oder lassen Sie dieses Feld leer, um alle geänderten Rollengruppen suchen..."

**TIP**

Wenn Sie alle Rollengruppen nach Änderungen durchsuchen möchten, wählen Sie keine bestimmten Rollengruppen aus, und gehen Sie zu Schritt 10. Wenn das Feld **Diese Rollengruppen durchsuchen** leer ist, umfasst die Suche alle Rollengruppen.

- a. Zum Öffnen des Dialogfelds **Rolle auswählen** drücken Sie, während der Fokus auf der Schaltfläche zum Auswählen von Rollengruppen liegt, die EINGABETASTE. Das Feld **Suche** besitzt den Fokus, und Sie hören „Filter oder Suche bearbeiten“. Geben Sie ganz oder teilweise den Namen der ersten Rollengruppe ein, die Sie in die Suche einschließen möchten, und drücken Sie dann die EINGABETASTE, um nach der Rollengruppe zu suchen.
- b. Drücken Sie zur Auswahl einer Rollengruppe etwa dreimal die TAB-TASTE, bis Sie den Namen der Rollengruppe in der Liste der Suchergebnisse hören. Wenn die Liste der Suchergebnisse Rollengruppen enthält, drücken Sie die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den Namen der Rollengruppe hören.

**TIP**

Es können mehrere aufeinanderfolgende Rollengruppen ausgewählt werden. Zum Arbeiten mit allen Rollengruppen lassen Sie das Feld **Suche** leer, oder geben Sie ganz oder teilweise die Rollengruppennamen ein, die Sie hinzufügen möchten. Wechseln Sie mit der TAB-TASTE zu den Suchergebnissen. Drücken Sie die NACH-UNTEN-TASTE, um jeden Namen zu hören. Wenn alle hinzufügen möchten, drücken Sie STRG+A. Wenn Sie mehrere nacheinander aufgelistete Rollengruppen hinzufügen möchten, drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, bis Sie den ersten Rollengruppennamen hören, den Sie hinzufügen möchten. Halten Sie die UMSCHALTTASTE gedrückt, drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, bis Sie den letzten Rollengruppennamen hören, den Sie hinzufügen möchten, und lassen Sie dann die UMSCHALTTASTE los. Alle Rollengruppen zwischen dem ersten und letzten Namen werden ausgewählt.

- c. Drücken Sie die EINGABETASTE, um die ausgewählten Rollengruppen der Liste für die Suche nach Rollengruppenänderungen hinzuzufügen. Die Liste der Rollengruppen behält den Fokus, sodass Sie weitere Rollengruppen hinzufügen können, indem Sie sie auswählen und die EINGABETASTE drücken.

**TIP**

Zum Überprüfen der hinzugefügten Rollengruppen wechseln Sie mit der TAB-TASTE zur Schaltfläche **Hinzufügen**. Um die Liste der Rollengruppen anzuhören, drücken Sie die TAB-TASTE erneut. Sie hören den ersten Rollengruppennamen in der Liste. Um den zweiten Rollengruppennamen in der Liste zu hören, drücken Sie noch einmal die TAB-TASTE. Drücken Sie weiterhin die TAB-TASTE, bis Sie die Namen aller hinzugefügten Rollengruppen gehört haben. Um eine Rollengruppe aus der Liste zu löschen, aktivieren Sie den Link **Entfernen** durch Drücken der EINGABETASTE, wenn Sie den Rollengruppennamen hören.

- d. Wenn Sie mit dem Hinzufügen von Rollengruppen fertig sind, wechseln Sie mit der TAB-TASTE zur Schaltfläche **OK**, und drücken Sie die EINGABETASTE. Das Dialogfeld **Nach Änderungen an Administratorrollengruppen suchen** besitzt wieder den Fokus, und das Textfeld **Diese Rollengruppen durchsuchen** enthält Ihre ausgewählten Rollengruppen.
10. Drücken Sie die TAB-TASTE, um auf die Schaltfläche **Suchen** zuzugreifen, und drücken Sie die EINGABETASTE.
11. Drücken Sie etwa viermal die TAB-TASTE, um auf die Suchergebnisse zuzugreifen. Wenn eine der ausgewählten Rollengruppen im ausgewählten Zeitraum geändert wurde, hören Sie den Namen der Rollengruppe und das Datum der Änderung. Wenn keine Rollengruppe geändert wurde, hören Sie „Es gibt keine Elemente, die in dieser Ansicht angezeigt werden können“. (In Sprachausgabe hören Sie „Enthält 0 Elemente“.)
12. Für weitere Details zu einer Rollengruppenänderung drücken Sie, während die Änderung in der Liste der Suchergebnisse ausgewählt ist, die TAB-TASTE, um in den Bereich **Details** zu wechseln. Zum Drucken des Inhalts des Detailbereichs drücken Sie die EINGABETASTE. Zum Anhören des Inhalts des Bereichs **Details** drücken Sie erneut die TAB-TASTE.
13. Um das Dialogfeld zu schließen, wechseln Sie mit der TAB-TASTE zur Schaltfläche **Schließen**, und drücken Sie die EINGABETASTE.

## Suchen von Daten zu Änderungen am Compliancestatus

Überwachen Sie die Einhaltung gesetzlicher Vorschriften und die Aufbewahrung von für Rechtsstreitigkeiten erforderlichen Daten, indem Sie nach Statusänderungen an Compliance-eDiscovery und -Archiv und am Beweissicherungsverfahren pro Postfach suchen. Diese Informationen sind auf der Registerkarte **Verwaltung der Compliance** und auf der Seite **Überwachung** von EAC verfügbar.

### Suchen nach Statusänderungen an Compliance-eDiscovery und -Archiv

Wenn Ihre Organisation gerichtlichen Ermittlungen (im Zusammenhang mit Unternehmensrichtlinien, Compliance oder Rechtsstreitigkeiten), Compliance-eDiscovery und Compliance-Archiv im Exchange entspricht kann Online-Discovery-Suche für relevante Inhalte innerhalb von Postfächern führen Sie Hilfe. Sie können das Administrator-Überwachungsprotokoll um Postfächer zu suchen, die auf halten oder von Compliance-eDiscovery oder Compliance-Archiv entfernt wurden, suchen. [Weitere Informationen zu Compliance - eDiscovery und -Archiv Berichte](#).

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis der Fokus auf **Verwaltung der Compliance** liegt, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen.
4. Drücken Sie die TAB-TASTE, bis der Fokus auf **Überwachung** liegt. Sie hören „Überwachung, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.
5. Zugriff auf die Listenansicht im Hauptfenster drücken Sie STRG + F6. Sie hören "Audit meldet..."
6. Drücken Sie etwa 15-mal die TAB-TASTE, bis Sie hören „Compliance-eDiscovery- und Archivbericht ausführen“. Drücken Sie die EINGABETASTE.
7. **Suchen nach Änderungen an In-Place eDiscovery, Compliance -Archive** im Dialogfeld, das geöffnet wird, das Kombinationsfeld Start-Jahr den Fokus hat, und hören Sie "Start Datum Kombinationsfelds Jahr..."

**TIP**

Standardmäßig wird das Startdatum auf zwei Wochen vor dem gestrigen Datum festgelegt. Im Postfachüberwachungsprotokoll werden normalerweise Einträge für 90 Tage gespeichert.

- a. Geben Sie ggf. das Jahr des Startdatums für die Suche nach Änderungen an eDiscovery und Archiven ein. Sie können das Jahr des Startdatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
  - b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Startdatums ein bzw. wählen Sie ihn aus.
  - c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Startdatums ein bzw. wählen Sie ihn aus.
8. Registerkarte an das **Ende des Jahres**-Kombinationsfeld. Sie hören "Year-End Date Kombinationsfelds..."

**TIP**

Der Standardwert des Enddatums ist das heutige Datum.

- a. Geben Sie ggf. das Jahr des Enddatums für die Suche nach Änderungen an eDiscovery und Archiven ein. Sie können das Jahr des Enddatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
- b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Enddatums ein bzw. wählen Sie ihn aus.
- c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Enddatums ein bzw. wählen Sie ihn aus.

9. Drücken Sie die TAB-TASTE, um auf die Schaltfläche **Suchen** zuzugreifen, und drücken Sie die EINGABETASTE.
10. Drücken Sie etwa dreimal die TAB-TASTE, um auf die Suchergebnisse zuzugreifen. Wenn eDiscovery-Suchen oder Archive im ausgewählten Zeitraum geändert wurden, hören Sie deren Namen. Wenn keine geändert wurden, hören Sie „Es gibt keine Elemente, die in dieser Ansicht angezeigt werden können“. (In Sprachausgabe hören Sie „Enthält 0 Elemente“.)
11. Für weitere Details zu einer eDiscovery- oder Archivänderung drücken Sie, während die Änderung in der Liste der Suchergebnisse ausgewählt ist, die TAB-TASTE, um in den Detailbereich zu wechseln. Zum Drucken des Inhalts des Bereichs **Details** drücken Sie die EINGABETASTE. Zum Anhören des Inhalts des Bereichs **Details** drücken Sie erneut die TAB-TASTE.
12. Um das Dialogfeld zu schließen, wechseln Sie mit der TAB-TASTE zur Schaltfläche **Schließen**, und drücken Sie die EINGABETASTE.

#### **Suchen nach Postfächern, die für Beweissicherungsverfahren aktiviert oder deaktiviert sind**

Wenn Ihre Organisation in ein Rechtsverfahren involviert ist, müssen Sie möglicherweise Schritte unternehmen, um E-Mail-Nachrichten zu sichern, die als Beweis dienen können. Mithilfe des Beweissicherungsverfahrens können Sie alle von bestimmten Personen gesendeten und empfangenen E-Mails bzw. alle in Ihrer Organisation gesendeten und empfangenen E-Mails für einen bestimmten Zeitraum aufbewahren. Durchsuchen Sie das Administratorüberwachungsprotokoll, um die Postfächer zu überwachen, deren Status des Beweissicherungsverfahrens (aktiviert oder deaktiviert) sich während eines bestimmten Zeitraums geändert hat. Erfahren Sie mehr über [Ausführen eines Beweissicherungsverfahren-Berichts pro Postfach](#).

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis der Fokus auf **Verwaltung der Compliance** liegt, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen.
4. Drücken Sie die TAB-TASTE, bis der Fokus auf **Überwachung** liegt. Sie hören „Überwachung, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.
5. Zugriff auf die Listenansicht im Hauptfenster drücken Sie STRG + F6. Sie hören "Audit meldet..."
6. Drücken Sie etwa 21-mal die TAB-TASTE, bis Sie hören „Beweissicherungsverfahren-Bericht pro Postfach ausführen“. Drücken Sie die EINGABETASTE.
7. **Suchen nach Änderungen an pro Postfach Aufbewahrung für eventuelle Rechtsstreitigkeiten** im Dialogfeld, das geöffnet wird, das **Starten des Jahres** Kombinationsfeld den Fokus hat, und hören Sie "Start Datum Kombinationsfelds Jahr..."

#### **TIP**

Standardmäßig wird das Startdatum auf zwei Wochen vor dem gestrigen Datum festgelegt. Im Postfachüberwachungsprotokoll werden normalerweise Einträge für 90 Tage gespeichert.

- a. Geben Sie ggf. das Jahr des Startdatums für die Suche nach Änderungen am Beweissicherungsverfahren ein. Sie können das Jahr des Startdatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
- b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Startdatums ein bzw. wählen Sie ihn aus.

- c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Startdatums ein bzw. wählen Sie ihn aus.
8. Registerkarte an das **Ende des Jahres**-Kombinationsfeld. Sie hören "Year-End Date Kombinationsfelds..."

**TIP**

Der Standardwert des Enddatums ist das heutige Datum.

- a. Geben Sie ggf. das Jahr des Enddatums für die Suche nach Änderungen am Beweissicherungsverfahren ein. Sie können das Jahr des Enddatums auch durch Drücken der NACH-OBEN-TASTE oder der NACH-UNTEN-TASTE auswählen.
- b. Wechseln Sie mit der TAB-TASTE zum Textfeld **Monat**, und geben Sie den Monat des Enddatums ein bzw. wählen Sie ihn aus.
- c. Wechseln Sie mit der TAB-TASTE zum Textfeld **Tag**, und geben Sie den Tag des Enddatums ein bzw. wählen Sie ihn aus.
9. Zugriff auf die Schaltfläche Auswahl von Benutzern, drücken Sie zweimal die Tab-Taste. Sie hören "diese Postfächer suchen oder leer lassen, um feststellen, dass alle Postfächer mit Rechtsstreitigkeiten Änderungen halten..."

**TIP**

Wenn Sie alle Postfächer nach Änderungen in Bezug auf das Beweissicherungsverfahren durchsuchen möchten, wählen Sie keine bestimmten Postfächer aus, und gehen Sie zu Schritt 10. Wenn das Feld **Diese Postfächer durchsuchen** leer ist, umfasst die Suche alle Postfächer.

- a. Zum Öffnen des Dialogfelds **Mitglieder auswählen** drücken Sie, während der Fokus auf der Schaltfläche zum Auswählen von Benutzern liegt, die EINGABETASTE. Die Schaltfläche **Suchen** besitzt den Fokus. Wenn Sie einen Benutzer in Ihrer Organisation suchen möchten, drücken Sie die LEERTASTE, geben Sie ganz oder teilweise den Namen des Benutzers ein, und drücken Sie dann die EINGABETASTE.
- b. Drücken Sie etwa siebenmal die TAB-TASTE, bis Sie den Namen des Benutzers in der Liste der Suchergebnisse hören.
- c. Um den Benutzer zur Liste der Postfächer in der Suche nach Änderungen am Beweissicherungsverfahren hinzuzufügen, drücken Sie die NACH-UNTEN-TASTE, bis Sie den Namen des Benutzers zu hören, und drücken Sie dann die EINGABETASTE. Die Liste der Benutzer behält den Fokus, sodass Sie weitere Benutzer hinzufügen können, indem Sie ihre Postfächer auswählen und die EINGABETASTE drücken.

**TIP**

So überprüfen Sie die Benutzer aus, die Sie hinzugefügt haben, die TAB, um die Schaltfläche **Hinzufügen**. Um die Liste der Benutzer zu hören, drücken Sie die Tab-Taste erneut. Der erste Name wird gelesen. Drücken Sie die Tab-Taste, um den zweiten Namen in der Liste zu hören, einmal. Fahren Sie fort, drücken die Tab-Taste, bis Sie die Namen aller Benutzer gehört, die Sie hinzugefügt haben. Um einen Benutzer aus der Liste löschen möchten, aktivieren Sie den Link **Entfernen** durch Drücken der EINGABETASTE, wenn Sie den Benutzernamen hören.

- d. Um einen externen Benutzer hinzuzufügen, drücken Sie die TAB-TASTE, bis Sie hören „Namen überprüfen bearbeiten, Text eingeben“. (In der Sprachausgabe hören Sie „Bearbeiten“.) Geben Sie die E-Mail-Adresse des externen Benutzers ein, drücken Sie UMSCHALT+TAB, um die Schaltfläche **Namen**

**überprüfen** auszuwählen, und drücken Sie dann die EINGABETASTE. Dadurch wird die E-Mail-Adresse überprüft und zur Liste der Benutzer hinzugefügt.

**TIP**

Beachten Sie: Wenn Sie eine externe E-Mail-Adresse eingeben und die EINGABETASTE drücken, wird der Benutzer zur Liste hinzugefügt und das Dialogfeld geschlossen. Wenn Sie noch nicht fertig sind, verwenden Sie stattdessen die Schaltfläche **Namen überprüfen**, um sie hinzuzufügen.

- e. Wenn Sie mit dem Hinzufügen von Benutzern fertig sind, wechseln Sie mit der TAB-TASTE zur Schaltfläche **OK**, und drücken Sie die EINGABETASTE. Das Dialogfeld **Nach Änderungen am Beweissicherungsverfahren pro Postfach suchen** besitzt wieder den Fokus, und im Textfeld **Diese Postfächer durchsuchen** sind die Postfächer aufgeführt, die nach Änderungen in Bezug auf Beweissicherungsverfahren durchsucht werden sollen.
10. Drücken Sie die TAB-TASTE, um auf die Schaltfläche **Suchen** zuzugreifen, und drücken Sie die EINGABETASTE.
11. Drücken Sie etwa dreimal die TAB-TASTE, um auf die Suchergebnisse zuzugreifen. Wenn der Status des Beweissicherungsverfahrens für Postfächer im ausgewählten Zeitraum geändert wurde, hören Sie den Namen des Postfachbesitzers. Wenn auf keines der Postfächer durch einen Nicht-Besitzer zugegriffen wurde, hören Sie „Es gibt keine Elemente, die in dieser Ansicht angezeigt werden können“. (In der Sprachausgabe hören Sie „Enthält 0 Elemente“.)
12. Für weitere Details zu einer Änderung des Beweissicherungsverfahrens drücken Sie, während die Änderung in der Liste der Suchergebnisse ausgewählt ist, die TAB-TASTE, um in den Detailbereich zu wechseln. Zum Drucken des Inhalts des Detailbereichs drücken Sie die EINGABETASTE. Zum Anhören des Inhalts des Detailbereichs rücken Sie erneut die TAB-TASTE.
13. Um das Dialogfeld zu schließen, wechseln Sie mit der TAB-TASTE zur Schaltfläche **Schließen**, und drücken Sie die EINGABETASTE.

# Verwenden Sie eine Bildschirmsprachausgabe verfolgen eine e-Mail-Nachricht in der Exchange-Verwaltungskonsole in Exchange Online

18.12.2018 • 14 minutes to read

Mithilfe der Sprachausgabe in der Exchange-Verwaltungskonsole (EAC) in Exchange Online können Sie E-Mail-Nachrichten nachverfolgen. Dies ist hilfreich, wenn Benutzer wissen möchten, ob ihre Nachrichten verzögert bzw. möglicherweise bei der Übermittlung verloren gegangen sind. Mit der Nachrichtenablaufverfolgung können Sie Nachricht auf ihrem Weg durch Exchange Online verfolgen und ermitteln, ob eine bestimmte E-Mail empfangen, abgelehnt, zurückgestellt oder zugestellt wurde.

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zum Durchführen dieser Aufgabe verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole](#).

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen](#).

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Popupfenstern, daher sollten Sie in Ihrem Browser unbedingt [Pop-up-Fenster für Office 365 aktivieren](#).

### **Bestätigen Ihres Office 365-Abonnementplans**

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten, die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung](#).

### **Öffnen der EAC und Bestätigen Ihrer Administratorrolle**

Zum Nachverfolgen einer Nachricht [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Office 365-Administrator für Ihnen die Administratorrollengruppen „Organisationsverwaltung“, „Complianceverwaltung“ und „Helpdesk“ zugewiesen hat. Erfahren Sie mehr über das [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center](#).

## Erstellen einer neuen Nachrichtenablaufverfolgung

Sie stellen möglicherweise fest, dass Sie eine Nachrichtenablaufverfolgung benötigen, wenn ein Benutzer sich an Sie wendet, weil Nachrichten nicht zugestellt oder verzögert zugestellt werden. Sie können eine Nachricht anhand verschiedener Kriterien nachverfolgen, z. B. anhand der E-Mail-Adresse, des Datumsbereichs, des Übermittlungsstatus und der Nachrichten-ID.

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis Sie zu **E-Mail-Fluss** gelangen, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen.
4. Drücken Sie die TAB-TASTE, bis Sie zu **Nachrichtenablaufverfolgung** gelangen. Sie hören „Nachrichtenablaufverfolgung, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.
5. Drücken Sie STRG+F6, um auf die Listenansicht des Hauptfensters zuzugreifen. Sie hören „Kombinationsfeld ,Nachricht wurde gesendet oder empfangen', Letzte 48 Stunden“.
6. Der Fokus liegt auf dem Kombinationsfeld **Datumsbereich**, und die Standardeinstellung lautet **Letzte 48 Stunden**. Um die anderen Optionen, einschließlich **Letzte 24 Stunden**, **Letzte 7 Tage** und **Benutzerdefiniert**, zu durchlaufen, drücken Sie die NACH-OBEN- oder NACH-UNTEN-TASTE.

**TIP**

Wenn Sie **Benutzerdefiniert** auswählen, können Sie die Zeitzone, Startdatum und -uhrzeit sowie Enddatum und -uhrzeit eingeben. Diese Felder sind nur verfügbar, wenn Sie **Benutzerdefiniert** im Kombinationsfeld **Datumsbereich** auswählen. Beachten Sie, dass möglicherweise keine Daten für Nachrichten vorhanden sind, die weniger als vier Stunden alt sind. Eine Nachrichtenablaufverfolgung kann nicht für eine Nachricht ausgeführt werden, die älter als 90 Tage ist.

7. Drücken Sie die TAB-TASTE, um zum Kombinationsfeld **Übermittlungsstatus** zu gelangen. Folgende Optionen stehen zur Verfügung: **Alle** (Standardeinstellung), **Übermittelt**, **Fehlgeschlagen**, **Ausstehend**, **Erweitert**, **Isoliert**, **Als Spam gefiltert** und **Unbekannt**. Drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, bis der gewünschte Übermittlungsstatus ausgewählt ist.
8. Drücken Sie die TAB-TASTE, bis Sie zum Textfeld **Nachrichten-ID** gelangen. Dies ist ein optionales Feld, aber Sie können damit Suchergebnisse eingrenzen. Die Nachrichten-ID oder Client-ID wird vom sendenden System generiert und ist in der Kopfzeile der Nachricht mit dem Token **Nachrichten-ID:** zu finden. Die Nachrichten-ID kann spitze Klammern (<>) enthalten.
9. Um in der Nachrichtenablaufverfolgung Absender (einen oder mehrere) anzugeben, drücken Sie die TAB-TASTE, bis Sie zur Schaltfläche **Absender hinzufügen** gelangen, und drücken Sie die EINGABETASTE. Im Dialogfeld **Mitglieder auswählen** befindet sich der Fokus auf der Schaltfläche **Suchen**.
  - a. Wenn Sie einen Benutzer in Ihrer Organisation suchen möchten, drücken Sie die EINGABETASTE, geben Sie den Namen des Benutzers ganz oder teilweise ein, und drücken Sie dann die EINGABETASTE.
  - b. Drücken Sie etwa siebenmal die TAB-TASTE, bis Sie den Namen des Benutzers in der Liste der Suchergebnisse hören.
  - c. Um den Benutzer zur Liste der Absender für die Nachrichtenablaufverfolgung hinzuzufügen, drücken Sie die NACH-UNTEN-TASTE, bis Sie den Namen des Benutzers hören, und drücken Sie dann die EINGABETASTE. Die Liste der Benutzer behält den Fokus, sodass Sie weitere Benutzer hinzufügen können, indem Sie ihre Postfächer auswählen und die EINGABETASTE drücken.

**TIP**

So überprüfen Sie die Benutzer aus, die Sie hinzugefügt haben, die TAB, um die Schaltfläche **Hinzufügen**. Um die Liste der Benutzer zu hören, drücken Sie die Tab-Taste erneut. Der erste Name wird gelesen. Um den zweiten Namen in der Liste zu hören, drücken Sie die Tab-Taste noch einmal. Fahren Sie fort, drücken die Tab-Taste, bis Sie die Namen aller Benutzer gehört, die Sie hinzugefügt haben. Um einen Benutzer aus der Liste löschen möchten, aktivieren Sie den Link **Entfernen** durch Drücken der EINGABETASTE, wenn Sie den Benutzernamen hören.

- d. Um einen externen Benutzer oder eine E-Mail-Adresse mit einem Platzhalter (z. B. \*@contoso.com) anzugeben, drücken Sie die TAB-TASTE, bis Sie „Namen überprüfen bearbeiten, Text eingeben“ hören. (In der Sprachausgabe hören Sie „Bearbeiten“.) Geben Sie die E-Mail-Adresse des externen Benutzers oder die Adresse mit einem Platzhalter ein. Um die Schaltfläche **Namen überprüfen** auszuwählen, drücken Sie UMSCHALT+TAB, und drücken Sie dann die EINGABETASTE. Dadurch wird die E-Mail-Adresse überprüft und zur Liste der Benutzer hinzugefügt.

**TIP**

Wenn Sie einen Platzhalter angeben, können nicht auch vollständige E-Mail-Adressen zur Nachrichtenablaufverfolgung hinzugefügt werden. > Beachten Sie: Wenn Sie eine externe E-Mail-Adresse eingeben und die EINGABETASTE drücken, wird der Benutzer zur Liste hinzugefügt und das Dialogfeld geschlossen. Wenn Sie noch nicht fertig sind, verwenden Sie stattdessen die Schaltfläche **Namen überprüfen**, um sie hinzuzufügen.

- e. Wenn Sie alle Benutzer, Tab, um die Schaltfläche **OK** hinzugefügt haben, und drücken Sie die EINGABETASTE. Die Seite **Nachricht Trace** erneut den Fokus hat, und das Textfeld **Absender** Listet die Absender, den, die Sie für die nachrichtenablaufverfolgung angegeben.
10. Um der Nachrichtenablaufverfolgung zusätzlich zu den Absender oder anstelle der Absender einen Empfänger hinzuzufügen, wechseln Sie mit der TAB-TASTE zur Schaltfläche **Empfänger** hinzufügen, und drücken Sie die EINGABETASTE. Im Dialogfeld **Mitglieder auswählen** befindet sich der Fokus auf der Schaltfläche **Suchen**. Wiederholen Sie Schritt 9, um der Nachrichtenablaufverfolgung einen oder mehrere Empfänger hinzuzufügen.
11. Drücken Sie auf der Seite **Nachrichtenablaufverfolgung** die TAB-TASTE, bis Sie zur Schaltfläche **Suchen** gelangen, und drücken Sie die EINGABETASTE. Die Seite **Ergebnisse der Nachrichtenablaufverfolgung** Seite wird geöffnet, und es werden das Datum, der Absender, der Empfänger, der Betreff sowie der Status der Nachricht(en) angezeigt, die das Ergebnis der Nachrichtenablaufverfolgung sind.

**TIP**

Wenn Sie eine Nachrichtenverfolgung für Nachrichten ausführen, die weniger als 7 Tage alt sind, sollten die Nachrichten innerhalb von 5 bis 30 Minuten erscheinen. Wenn Sie eine Ablaufverfolgung für Nachrichten ausführen, die älter als 7 Tage sind, kann es einige Stunden dauern, bis Ergebnisse ausgegeben werden. Wenn die Seite **Ergebnisse der Nachrichtenablaufverfolgung** zunächst leer erscheint, prüfen Sie sie später noch einmal. Eine einfache Möglichkeit hierfür besteht darin, diese Seite geöffnet zu lassen, in der Symbolleiste in regelmäßigen Abständen über die TAB-TASTE zur Schaltfläche **Aktualisieren** zu wechseln und dann die EINGABETASTE zu drücken.

12. Um die Seite **Ergebnisse der Nachrichtenablaufverfolgung** zu schließen, wechseln Sie über die TAB-TASTE zur Schaltfläche „Schließen“, und drücken Sie die EINGABETASTE.

## Überprüfen des Status von ausstehenden oder abgeschlossenen Nachrichtenablaufverfolgungen

Es kann einige Minuten bis einige Stunden dauern, bis die Ergebnisse der Nachrichtenablaufverfolgung zurückgegeben werden. Sie können den Status von ausstehenden oder abgeschlossenen Nachrichtenablaufverfolgungen überprüfen.

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis Sie zu **E-Mail-Fluss** gelangen, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen.
4. Drücken Sie die TAB-TASTE, bis Sie zu **Nachrichtenablaufverfolgung** gelangen. Sie hören „Nachrichtenablaufverfolgung, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE.
5. Zugriff auf die Listenansicht im Hauptfenster drücken Sie STRG + F6. Sie hören "Nachricht gesendet oder empfangen wurde das Kombinationsfeld..."
6. Der Fokus liegt auf dem Kombinationsfeld **Datumsbereich**. Um zum Link **Ausstehende oder abgeschlossene Ablaufverfolgungen anzeigen** zu gelangen, drücken Sie UMSCHALT+TAB. Drücken Sie die EINGABETASTE. Die Seite **Ausstehende oder abgeschlossene Ablaufverfolgungen** wird geöffnet und zeigt den Titel des Berichts, das Datum der Übermittlung, den Berichtstatus sowie Nachrichten an.
7. Um die Seite zu aktualisieren, stellen Sie sicher, dass der Fokus auf der Schaltfläche **Aktualisieren** liegt (dies ist die Standardeinstellung), und drücken Sie dann die EINGABETASTE.
8. Um die Seite **Ausstehende oder abgeschlossene Ablaufverfolgungen** zu schließen, wechseln Sie über die TAB-TASTE zur Schaltfläche **Schließen**, und drücken Sie die EINGABETASTE.

**NOTE**

Weitere Informationen hierzu finden Sie unter [Ausführen einer Nachrichtenablaufverfolgung und Anzeigen der Ergebnisse](#).

# Verwenden Sie eine Bildschirmsprachausgabe mobilen Clients in der Exchange-Verwaltungskonsole in Exchange Online entwickelt

18.12.2018 • 10 minutes to read

Sie können die Sprachausgabe in der Exchange-Verwaltungskonsole (EAC) verwenden, um die Verwendung mobiler Geräte für Benutzer von Exchange Online zu ermöglichen, die dann über Mobiltelefone und Tablets auf Informationen in ihren Office 365-Postfächern zugreifen können. [Erfahren Sie mehr zu Clients und Mobilgeräten in Exchange Online.](#)

## Erste Schritte

Navigieren Sie mit Internet Explorer und Tastenkombinationen, und stellen Sie sicher, dass Sie über das entsprechende Office 365-Abonnement und die Administratorrolle zur Verwendung der Exchange-Verwaltungskonsole verfügen. Öffnen Sie dann die Exchange-Verwaltungskonsole, und beginnen Sie.

### **Verwenden des Browsers und der Tastatur zum Navigieren in der Exchange-Verwaltungskonsole**

Exchange Online, das die Exchange-Verwaltungskonsole enthält, ist eine webbasierte Anwendung. Die Tastenkombinationen und die Navigation können sich daher von Exchange 2016 unterscheiden. [Barrierefreiheit in der Exchange-Verwaltungskonsole.](#)

Die besten Ergebnisse bei der Arbeit mit der Exchange-Verwaltungskonsole in Exchange Online erhalten Sie, wenn Sie Internet Explorer als Browser verwenden. [Erfahren Sie mehr über Internet Explorer-Tastenkombinationen.](#)

Viele Aufgaben in der Exchange-Verwaltungskonsole erfordern die Verwendung von Popupfenstern, daher sollten Sie in Ihrem Browser unbedingt [Popupfenster für Office 365 aktivieren.](#)

### **Bestätigen Ihres Office 365-Abonnementplans**

Exchange Online ist in Office 365 Business- und Enterprise-Abonnementplänen enthalten. Die Funktionen können jedoch je nach Plan abweichen. Wenn Ihre Exchange-Verwaltungskonsole eine in diesem Artikel beschriebene Funktion nicht enthält, ist diese in Ihrem Plan möglicherweise nicht enthalten.

Weitere Informationen über die Exchange Online-Funktionen in Ihrem Abonnementplan finden Sie unter [Über welches Office 365 Business-Produkt oder welche Lizenz verfüge ich?](#) und [Exchange Online-Dienstbeschreibung.](#)

### **Öffnen der EAC und Bestätigen Ihrer Administratorrolle**

Zum Ausführen der Aufgaben in diesem Thema [Verwenden einer Sprachausgabe zum Öffnen des Exchange Admin Center](#), und überprüfen Sie, ob Ihr globaler Administrator für Office 365 Ihnen die Administratorrollengruppen [Organisationsverwaltung](#) und [Datensatzverwaltung](#) zugewiesen hat. [Verwenden einer Sprachausgabe zum Identifizieren Ihrer Administratorrolle im Exchange Admin Center.](#)

## Konfigurieren von Postfachrichtlinien für mobile Geräte und Zugriff

Sie können die Exchange-Verwaltungskonsole verwenden, um Postfachrichtlinien für mobile Geräte zu erstellen, die eine allgemeine Zusammenstellung von Regeln oder Sicherheitseinstellungen auf eine Gruppe von Benutzern anwenden. Wenn Sie keine eigene Postfachrichtlinie für mobile Geräte erstellen, wird die Standardrichtlinie angewendet, die die folgenden Einstellungen enthält:

- Zulassen der Synchronisierung von mobilen Geräten, die Richtlinien nicht vollständig unterstützen.

- Outlook Web App (OWA) für Geräte, unterstützt alle Kennwortrichtlinien und blockiert keine Geräte.
- Ein Kennwort ist optional.
- Eine Geräteverschlüsselung ist nicht erforderlich.

Zum Anzeigen, Bearbeiten oder Erstellen einer Postfachrichtlinie für ein mobiles Gerät wählen Sie im primären Navigationsbereich der Exchange-Verwaltungskonsole den Link **Mobil** aus, und klicken Sie dann in der Menüleiste auf den Link **Postfachrichtlinien für mobile Geräte**. Weitere Informationen zu den Optionen, die Sie hierfür festlegen können, finden Sie unter [Postfachrichtlinien für mobile Geräte](#).

Sie können auch Zugriffseinstellungen für Exchange ActiveSync-Zugriff angeben, eine Liste von Mobilgeräten in Quarantäne verwalten und Gerätezugriffsregeln einrichten. Wählen Sie hierzu im primären Navigationsbereich der Exchange-Verwaltungskonsole den Link **Mobil** aus, und klicken Sie dann in der Menüleiste auf den Link **Zugriff auf mobile Geräte**.

## Aktivieren von Exchange ActiveSync und Outlook Web App für Benutzer

Exchange ActiveSync ist ein Exchange-Synchronisierungsprotokoll, über das Mobiltelefone auf den Exchange-Server in Ihrer Organisation zugreifen können. Mit Exchange ActiveSync können Empfänger ihre mobilen Geräten verwenden, um auf E-Mails, Kalender, Kontakte und Aufgaben zuzugreifen. Sie können außerdem weiterhin auf diese Informationen zugreifen, während sie offline arbeiten. Erfahren Sie mehr über [Exchange ActiveSync](#).

Mit Outlook Web App können Benutzer von fast jedem Webbrowser aus auf ihr Exchange-Postfach zugreifen, auch von einem Browser auf ihren mobilen Geräten. [Erfahren Sie mehr über Outlook Web App](#).

### Aktivieren von Exchange ActiveSync und Outlook Web App für einen einzelnen Benutzer

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis Sie zu **Empfänger** gelangen, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen. Sie hören „Postfächer, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE, um den Link **Postfächer** auszuwählen.
4. Wenn Sie nach dem Benutzer suchen, für den Sie Exchange ActiveSync aktivieren möchten, drücken Sie STRG+F6 und dann die TAB-TASTE, bis Sie „Schaltfläche ,Suchen“ hören. Drücken Sie die EINGABETASTE.
5. Geben Sie den Namen des Benutzers vollständig oder teilweise ein, und drücken die EINGABETASTE.
6. Drücken Sie viermal STRG+F6, bis Sie den Namen des Benutzers in der Liste der Suchergebnisse hören. Wenn die Liste der Suchergebnisse mehrere Namen enthält, drücken Sie die NACH-OBEN-TASTE oder die NACH-UNTEN-TASTE, bis Sie den gewünschten Namen hören.
7. Drücken Sie STRG+F6, um zum Detailbereich zu gelangen. Sie hören „Unified Messaging-Link, Aktivieren“.
8. Drücken Sie die Tab-Taste. Sie hören „Mobile Geräte zu verknüpfen, Aktivieren von Exchange ActiveSync...“

#### TIP

Wenn der Benutzer für Exchange ActiveSync bereits aktiviert ist, hören Sie „Deaktivieren von Exchange ActiveSync...“

9. Drücken Sie die EINGABETASTE. Sie hören „Möchten Sie Exchange ActiveSync aktivieren?“ Drücken Sie, während der Fokus auf der Schaltfläche **OK** liegt, die EINGABETASTE.
10. Drücken Sie die TAB-TASTE. Sie hören „Link ,Mobile Geräte‘, OWA für Geräte aktivieren“.

**TIP**

Wenn der Benutzer bereits aktiviert ist, für die Outlook Web App für Geräte, hören Sie "Deaktivieren von OWA für Geräte..."

11. Drücken Sie die EINGABETASTE. Sie hören „Möchten Sie OWA für Geräte aktivieren?“ Drücken Sie, während der Fokus auf der Schaltfläche **OK** liegt, die EINGABETASTE.

**TIP**

Wenn Sie Exchange ActiveSync und Outlook Web App für weitere Benutzer aktivieren möchten, drücken Sie STRG+UMSCHALT+F6, um den Fokus wieder zu der Liste von Benutzern zu verschieben. Drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, bis Sie den gewünschten Namen hören, und wiederholen Sie die Schritte 7 bis 11.

**Aktivieren von Exchange ActiveSync und Outlook Web App für mehrere Benutzer gleichzeitig**

1. Drücken Sie in EAC so oft STRG+F6, bis der primäre Navigationsbereich den Fokus hat und Sie „Dashboard, primärer Navigationslink“ hören.
2. Drücken Sie die TAB-TASTE, bis Sie zu **Empfänger** gelangen, und drücken Sie die EINGABETASTE.
3. Drücken Sie STRG+F6, um zur Menüleiste zu gelangen. Sie hören „Postfächer, sekundärer Navigationslink“. Drücken Sie die EINGABETASTE, um den Link **Postfächer** auszuwählen.
4. Drücken Sie zweimal STRG+ F6zweimal, um zu der Liste von Benutzern zu gelangen. Drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, um zu dem ersten benachbarten Benutzer zu gelangen. Halten Sie die UMSCHALTTASTE gedrückt, und drücken Sie die NACH-UNTEN-TASTE oder die NACH-OBEN-TASTE, um weitere benachbarte Benutzer auszuwählen.

**TIP**

Drücken Sie STRG+A, um alle Benutzer auszuwählen.

5. Drücken Sie wiederholt die Tab-Taste, bis im Detailbereich **Bulk Edit** den Fokus hat, und Sie hören "Bulk Edit..
6. Drücken Sie die TAB-TASTE, bis Sie „Link aktivieren“ hören. Drücken Sie die EINGABETASTE.
7. Eine Warnung fragt „Möchten Sie Outlook im Web für alle ausgewählten Empfänger aktivieren?“ Drücken Sie, während der Fokus auf der Schaltfläche **OK** liegt, die EINGABETASTE.
8. Drücken Sie die TAB-TASTE etwa zehn Mal, bis Sie „Link anzeigen“ hören. Drücken Sie die TAB-TASTE noch einmal. Sie hören „Link aktivieren“. Drücken Sie die EINGABETASTE.
9. Eine Warnung fragt „Möchten Sie Exchange ActiveSync für alle ausgewählten Empfänger aktivieren?“ Drücken Sie, während der Fokus auf der Schaltfläche **OK** liegt, die EINGABETASTE.