Contents

Verwalten von Clients in Windows 10

Verwaltungstools in Windows 10

Erstellen erforderlicher Benutzerprofile

Verbinden mit einem PC, der Mitglied des Remote Azure Active Directory ist

Verknüpfen von Windows10 Mobile mit Azure Active Directory

Neue Richtlinien für Windows10

Gruppenrichtlinien, die nur für Windows10 Enterprise und Windows10 Education gelten

Verwalten der Einstellungs-App mit Gruppenrichtlinien

Welche Version von Windows verwende ich

Zurücksetzen von Windows 10 Mobile-Geräten

Wechsel zur modernen Verwaltung

Bereitstellungs- und Verwaltungshandbuch für Windows10 Mobile

Windows-Bibliotheken

Problembehandlung für Windows 10-Clients

Erweiterte Problembehandlung für Windows-Networking

Erweiterte Problembehandlung für WLAN-Verbindung

Erweiterte Problembehandlung für 802.1X-Authentifizierung

Datensammlung für die Problembehandlung der 802.1X-Authentifizierung

Erweiterte Problembehandlung für TCP/IP

Sammeln von Daten mithilfe des Netzwerkmonitors

Problembehandlung für TCP/IP-Verbindung

Problembehandlung für Portmangel

Problembehandlung für Remote Procedure Call (RPC)-Fehler

Erweiterte Problembehandlung für Windows-Start

Bestimmen der geeigneten Auslagerungsdateigröße für 64-Bit-Versionen von Windows

Generieren eines Kernels oder eines vollständigen Absturzabbilds

Einführung in die Auslagerungsdatei

Konfigurieren von Systemausfall- und Wiederherstellungsoptionen in Windows
Erweiterte Problembehandlung für Windows-Startprobleme
Erweiterte Problembehandlung für einfrierende Windows-basierte Computer
Erweiterte Problembehandlung für Stoppfehler und Bluescreens
Erweiterte Problembehandlung für Stoppfehler 7B oder Inaccessible_Boot_Device
Mobilgerätverwaltung für Lösungsanbieter
Änderungsverlauf für die Clientverwaltung

Clientverwaltung

20.12.2019 • 2 minutes to read

Gilt für:

- Windows 10

Informationen über Verwaltungstools, Aufgaben und bewährte Methoden für die Verwaltung von Windows10 und Windows10 Mobile-Clients in Ihrem Unternehmen.

THEMA	BESCHREIBUNG
Verwaltungstools in Windows10	Links zur Dokumentation für die Tools für IT-Spezialisten und erfahrene Benutzer finden Sie im Ordner „Verwaltung“.
Erstellen erforderlicher Benutzerprofile	Anweisungen für die Verwaltung der Einstellungen, die in verbindlichen Profilen allgemein definiert sind (allerdings nicht beschränkt auf): Symbole, die auf Desktop, Desktophintergründen, in Benutzereinstellungen in der Systemsteuerung, der Druckerauswahl und mehr angezeigt werden.
Verbinden mit in Azure Active Directory eingebundenen Remote-PCs	Anweisungen zum Herstellen einer Verbindung mit einem Remote-PC, der Azure Active Directory (Azure AD) beigetreten ist
Warum sollte Windows 10 Mobile mit Azure AD verknüpft werden?	Beschreibt die Überlegungen und Optionen für die Verwendung von Windows10 Mobile mit Azure AD in Ihrer Organisation.
Neue Richtlinien für Windows 10	Übersicht über neue Gruppenrichtlinieneinstellungen, die in Windows10 zur Verfügung stehen
Windows 10-Standardrichtlinie für Medien Entfernung	In Windows 10, Version 1809, wurde die standardmäßige Entfernungsrichtlinie für externe Speichermedien von "bessere Leistung" auf "schnell Entfernung" geändert.
Gruppenrichtlinien für die Editionen Enterprise und Education	Auflistung aller Gruppenrichtlinieneinstellungen, die spezifisch für Windows10 Enterprise und Windows10 Education gelten
Verwalten der Einstellungs-App mit Gruppenrichtlinien	Ab Windows10, Version 1703, können Sie jetzt die in der App „Einstellungen“ angezeigten Seiten mithilfe der Gruppenrichtlinie verwalten.
Zurücksetzen von Windows10 Mobile-Geräten	Anweisungen zum Zurücksetzen von einem Windows10 Mobile-Gerät mit den Optionen zum Zurücksetzen auf *Werkseinstellungen* oder *Zurücksetzen und Beibehalten*
Wechsel zur modernen ITPro-Verwaltung	Beschreibt die modernen Windows10 ITPro-Szenarien mit herkömmlichen, Hybrid- und Cloud-basierten Unternehmensanforderungen

THEMA	BESCHREIBUNG
Bereitstellungs- und Verwaltungshandbuch für Windows10 Mobile	Hinweise und Anweisungen für die Bereitstellung von Windows10 Mobile
Windows-Bibliotheken	Hinweise und Anweisungen für die Verwaltung von Windows10-Bibliotheken wie „Eigene Dokumente“, „Eigene Bilder“ und „Eigene Musik“.
Mobile Geräteverwaltung für Lösungsanbieter	Verfahrens- und Referenzdokumentation für Lösungsanbieter, die mobile Geräteverwaltung (Mobile Device Management, MDM) für Windows10-Geräte bereitstellen.
Änderungsverlauf für die Clientverwaltung	In diesem Thema sind neue und aktualisierte Themen in der Clientverwaltungsdokumentation für Windows 10 und Windows 10 Mobile aufgeführt.

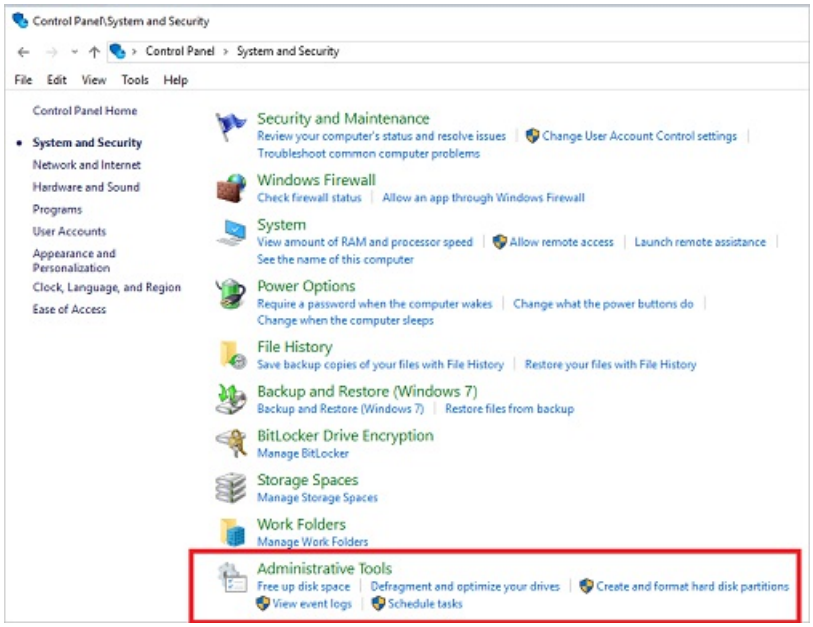
Verwaltungstools in Windows 10

29.10.2019 • 2 minutes to read

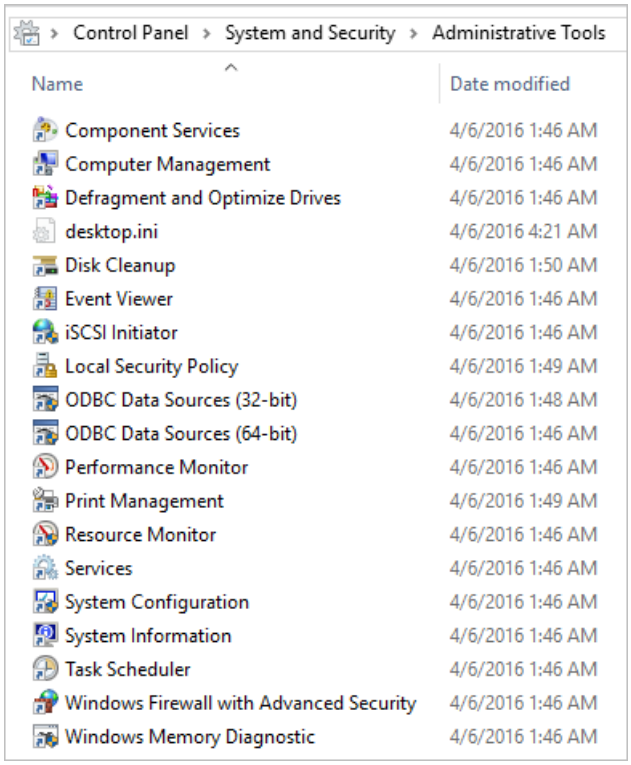
Betrifft

- Windows 10

„Verwaltung“ ist ein Ordner in der Systemsteuerung mit Tools für Systemadministratoren und fortgeschrittene Benutzer.



Je nachdem, welche Windows-Edition Sie verwenden, können in dem Ordner unterschiedliche Tools enthalten sein.



Diese Tools waren in früheren Versionen von Windows enthalten, und die zugehörige Dokumentation für jedes

Tool sollte Ihnen bei der Verwendung dieser Tools in Windows10 helfen. Die folgende Liste enthält Links zur Dokumentation für jedes Tool.

- Komponentendienste
- Computerverwaltung
- Laufwerke defragmentieren und optimieren
- Datenträgerbereinigung
- Ereignisanzeige
- iSCSI-Initiator
- Lokale Sicherheitsrichtlinie
- ODBC-Datenquellen
- Performance Monitor (Leistungsüberwachung)
- Druckverwaltung
- Ressourcenmonitor
- Dienste
- Systemkonfiguration
- Systeminformationen
- Aufgabenplanung
- Windows-Firewall mit erweiterter Sicherheit
- Windows-Speicherdiagnose

TIP

Wenn die mit einem Tool in der folgenden Liste verknüpften Inhalte nicht die erforderlichen Informationen zur Verwendung des betreffenden Tools enthalten, senden Sie uns über die Funktion **War diese Seite hilfreich?** auf der Seite **Verwaltungstools in Windows 10** einen Kommentar. Wenn Sie uns genauer angeben, welche Informationen Sie zu einem Tool benötigen, hilft uns dies bei der Planung zukünftiger Inhalte.

Verwandte Themen

Diagnosedatenanzeige

Erstellen erforderlicher Benutzerprofile

20.12.2019 • 6 minutes to read

Gilt für:

- Windows 10

Ein obligatorisches Benutzerprofil ist ein Roaming-Benutzerprofil, das von einem Administrator vorkonfiguriert wurde, um Einstellungen für Benutzer festzulegen. Zu den häufig in einem verbindlichen Profil definierten Einstellungen gehören (aber nicht ausschließlich): auf dem Desktop angezeigte Symbole, Desktop Hintergründe, Benutzereinstellungen in der Systemsteuerung, Druckerauswahl und vieles mehr. Während der Sitzung eines Benutzers vorgenommene Konfigurationsänderungen, die normalerweise in einem Roaming-Benutzerprofilgespeichert werden, werden nicht gespeichert, wenn ein obligatorisches Benutzerprofil zugewiesen wird.

Verbindliche Benutzerprofile sind nützlich, wenn die Standardisierung wichtig ist, z.B. auf einem Kioskgerät oder in den Bildungseinstellungen. Nur Systemadministratoren können Änderungen an obligatorischen Benutzerprofilen vornehmen.

Wenn der Server, auf dem das obligatorische Profil gespeichert ist, nicht verfügbar ist, beispielsweise wenn der Benutzer nicht mit dem Unternehmensnetzwerk verbunden ist, können Benutzer mit obligatorischen Profilen sich mit der lokal zwischengespeicherten Kopie des verbindlichen Profils anmelden, sofern vorhanden. Andernfalls wird der Benutzer mit einem temporären Profil angemeldet.

Benutzerprofile werden zu obligatorischen Profilen, wenn der Administrator die Ntuser. dat-Datei (die Registrierungsstruktur) des Profils jedes Benutzers im Dateisystem des Profilservers von `NTuser.dat` in `NTuser.man` umbenennen. Die `.man` Erweiterung bewirkt, dass das Benutzerprofil ein schreibgeschütztes Profil ist.

Profilerweiterung für jede Windows-Version

Der Name des Ordners, in dem Sie das verbindliche Profil speichern, muss die richtige Erweiterung für das Betriebssystem verwenden, auf das Sie angewendet wird. In der folgenden Tabelle sind die richtigen Erweiterungen für jede Betriebssystemversion aufgeführt.

CLIENT BETRIEBSSYSTEM-VERSION	VERSION DES SERVER BETRIEBSSYSTEMS	PROFILERWEITERUNG
WindowsXP	Windows Server 2003 Windows Server 2003 R2	keine
Windows Vista Windows 7	Windows Server 2008 Windows Server 2008 R2	v2
Windows 8	Windows Server 2012	v3
Windows 8.1	Windows Server 2012 R2	v4
Windows 10, Versionen 1507 und 1511	n.a.	V5
Windows 10, Versionen 1607, 1703, 1709, 1803, 1809 und 1903	Windows Server 2016 und Windows Server 2019	V6

Weitere Informationen finden Sie unter Bereitstellen von Roaming-Benutzerprofilen, Anhang B und

Versionsverwaltung für Roaming-Benutzerprofile in Windows 10 und Windows Server Technical Preview.

Erstellen eines verbindlichen Benutzerprofils

Erstellen Sie zunächst ein Standardbenutzer Profil mit den gewünschten Anpassungen, führen Sie Sysprep mit CopyProfile in der Antwortdatei auf **true** aus, kopieren Sie das benutzerdefinierte Standardbenutzer Profil in eine Netzwerkfreigabe, und benennen Sie das Profil um, damit es zwingend erforderlich ist.

So erstellen Sie ein Standardbenutzer Profil

1. Registrieren Sie sich bei einem Computer, auf dem Windows 10 ausgeführt wird, als Mitglied der lokalen Administrator Gruppe. Verwenden Sie kein Domänenkonto.

   > **NOTE**
   > Verwenden Sie eine Übungseinheit oder einen zusätzlichen Computer, auf dem eine Neuinstallation von Windows 10 ausgeführt wird, um ein Standardbenutzer Profil zu erstellen. Verwenden Sie keinen Computer, der für Unternehmen erforderlich ist (also ein Produktionscomputer). Durch diesen Vorgang werden alle Domänenkonten vom Computer entfernt, einschließlich Benutzerprofilordnern.

2. Konfigurieren Sie die Computereinstellungen, die Sie in das Benutzerprofil einbeziehen möchten. So können Sie beispielsweise Einstellungen für den Desktop Hintergrund konfigurieren, Standard-apps deinstallieren, Branchen-apps installieren usw.

   > **NOTE**
   > Im Gegensatz zu früheren Versionen von Windows können Sie ein Start-und Taskleisten Layout nicht mit einem obligatorischen Profil anwenden. Alternative Methoden zum Anpassen des Start Menüs und der Taskleiste finden Sie unter Verwandte Themen.

3. Erstellen Sie eine Antwortdatei (Unattend. Xml) , mit der der CopyProfile -Parameter auf " **true**" festgelegt wird. Der CopyProfile-Parameter veranlasst Sysprep, den Profilordner des derzeit signierten Benutzers in das Standardbenutzer Profil zu kopieren. Sie können Windows System Image Managerverwenden, der Teil des Windows Assessment and Deployment Kit (ADK) ist, um die Datei "Unattend. xml" zu erstellen.

4. Deinstallieren Sie alle Anwendungen, die Sie nicht benötigen oder vom PC aus wünschen. Beispiele zum Deinstallieren von Windows 10-Anwendungen finden Sie unter Remove-AppxProvisionedPackage. Eine Liste der nicht installierbaren Anwendungen finden Sie Untergrund Legendes zu den unterschiedlichen apps, die in Windows 10 enthalten sind.

> **NOTE**
> Es wird dringend empfohlen, unerwünschte oder nicht benötigte apps zu deinstallieren, da dadurch die Anmeldezeiten für Benutzer beschleunigt werden.

1. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken **Sie die Eingabe**Taste.

   ```
   sysprep /oobe /reboot /generalize /unattend:unattend.xml
   ```

   (Sysprep. exe befindet sich unter: C:\Windows\System32\sysprep. Standardmäßig sucht Sysprep in diesem Ordner nach Unattend. Xml.)

TIP

Wenn Sie eine Fehlermeldung erhalten, die besagt, dass "Sysprep Ihre Windows-Installation nicht überprüfen konnte", öffnen Sie%windir%\System32\Sysprep\Panther\setupact.log, und suchen Sie nach einem Eintrag wie den folgenden:

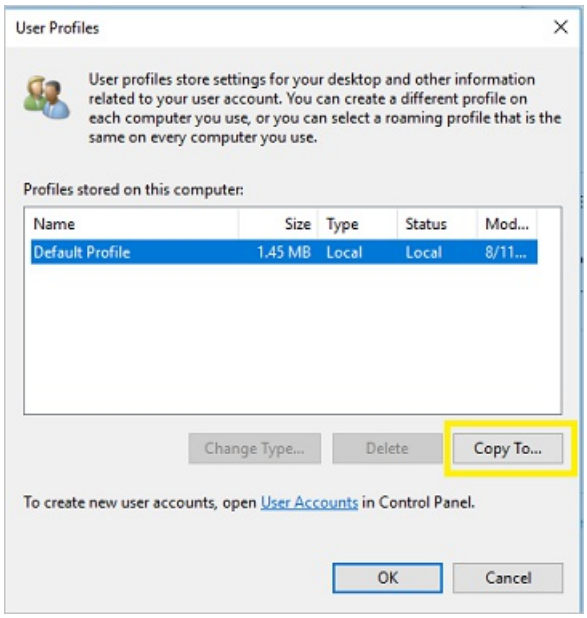
```
2016-08-11 14:19:20, Error                 SYSPRP Package
Microsoft.BingTranslator_4.4.0.0_x86__8wekyb3d8bbwe was installed for a user, but not
provisioned for all users. This package will not function properly in the sysprep image.
```

Verwenden Sie das Cmdlet Remove-AppxProvisionedPackage und Remove-AppxPackage-ALLUSERS in Windows PowerShell, um die im Protokoll aufgelistete APP zu deinstallieren.

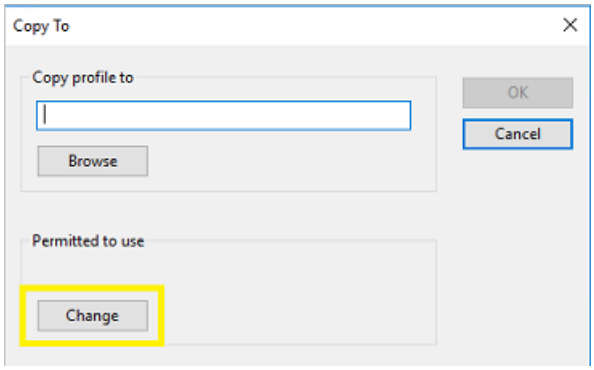
2. Mit dem Sysprep-Prozess wird der PC neu gestartet, und der Bildschirm für die Erstausführung wird gestartet. Schließen Sie die Einrichtung ab, und melden Sie sich dann mit einem Konto, das über lokale Administratorrechte verfügt, beim Computer an.

3. Klicken Sie mit der rechten Maustaste auf Start, **wechseln Sie zur Systemsteuerung (Ansicht** durch große oder kleine Symbole) #a0 **System** > **Erweiterte Systemeinstellungen**, und klicken Sie im Abschnitt **Benutzerprofile** auf **Einstellungen** .

4. Klicken Sie in **Benutzerprofile**auf **Standardprofil**, und klicken Sie dann auf **Kopieren nach**.



5. Klicken Sie in **Kopieren nach**unter **zulässige Verwendung**auf **ändern**.

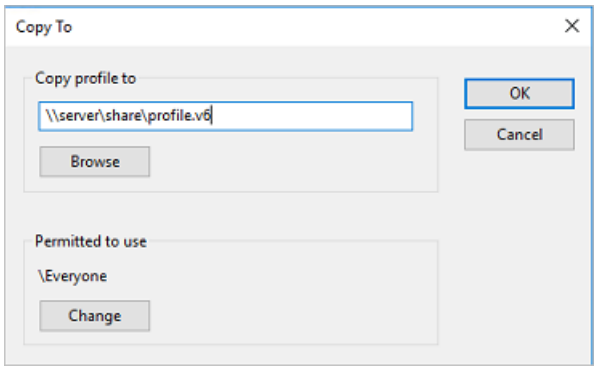


6. Geben `everyone` Sie in **Benutzer oder Gruppe auswählen**im Feld **Geben Sie den zu verwendenden Objektnamen ein den Namen ein** , klicken Sie auf **Namen überprüfen**, und klicken Sie dann auf **OK**.

7. Geben Sie in **Kopieren nach**in das Feld **Profil kopieren nach** den Pfad und den Ordnernamen ein, in dem das obligatorische Profil gespeichert werden soll. Der Ordnername muss die richtige Erweiterung für

die Version des Betriebssystems verwenden. Der Ordnername muss beispielsweise mit ". V6" enden, um ihn als Benutzerprofilordner für Windows 10, Version 1607, zu kennzeichnen.

- Wenn das Gerät der Domäne beigetreten ist und Sie mit einem Konto angemeldet sind, das über die Berechtigungen zum Schreiben in einen freigegebenen Ordner im Netzwerk verfügt, können Sie den Pfad für den freigegebenen Ordner eingeben.
- Wenn das Gerät nicht der Domäne beigetreten ist, können Sie das Profil lokal speichern und dann in den Speicherort des freigegebenen Ordners kopieren.



8. Klicken Sie auf **OK** , um das Standardbenutzer Profil zu kopieren.

So machen Sie das Benutzerprofil obligatorisch

1. Öffnen Sie im Datei-Explorer den Ordner, in dem Sie die Kopie des Profils gespeichert haben.

> **NOTE**
> Wenn der Ordner nicht angezeigt wird, klicken Sie auf **Ansichts** > **Optionen** > , um**Ordner-und Suchoptionen zu ändern**. Wählen Sie auf der Registerkarte **Ansicht** die Option **Ausgeblendete Dateien und Ordner anzeigen**aus, deaktivieren Sie **geschützte Betriebssystemdateien ausblenden**, klicken Sie auf **Ja** , um zu bestätigen, dass Sie die Betriebssystemdateien anzeigen möchten, und klicken Sie dann auf **OK** , um die Änderungen zu speichern.

2. Umbenennen `Ntuser.dat` in `Ntuser.man`.

Anwenden eines obligatorischen Benutzerprofils für Benutzer

In einer Domäne ändern Sie die Eigenschaften für das Benutzerkonto so, dass es in einem freigegebenen Ordner, der sich auf dem Server befindet, auf das verbindliche Profil verweist.

So wenden Sie Benutzer ein obligatorisches Benutzerprofil an

1. Öffnen Sie **Active Directory-Benutzer und-Computer** (DSA. msc).

2. Navigieren Sie zu dem Benutzerkonto, dem Sie das verbindliche Profil zuweisen möchten.

3. Klicken Sie mit der rechten Maustaste auf den Benutzernamen, und öffnen Sie **Eigenschaften**.

4. Geben Sie auf der Registerkarte **Profil** im Feld **Profilpfad** den Pfad zum freigegebenen Ordner ohne Erweiterung ein. Wenn der Ordnername beispielsweise \ \ \ \ *Server*Profile.V6 ist, geben Sie* \ \ \ **Server*\Profile.

5. Klicken Sie auf **OK**.

Es kann einige Zeit dauern, bis diese Änderung auf alle Domänencontroller repliziert wurde.

Anwenden von Richtlinien zur Verbesserung der Anmeldezeit

Wenn ein Benutzer mit einem obligatorischen Profil konfiguriert ist, startet Windows 10 so, als ob es sich bei jeder

Anmeldung des Benutzers um das erste Mal handelt. Wenden Sie die in der folgenden Tabelle gezeigten Gruppenrichtlinieneinstellungen an, um die Anmeldeleistung für Benutzer mit obligatorischen Benutzerprofilen zu verbessern. (Die Tabelle zeigt, auf welche Betriebssystemversionen die einzelnen Richtlinieneinstellungen angewendet werden können.)

GRUPPENRICHTLINIENE INSTELLUNG	WINDOWS 10	WINDOWS SERVER 2016	WINDOWS8.1	WINDOWS SERVER 2012
Computer Konfiguration #a0 administrative Vorlagen #a1 System #a2 Logon **-#a3 anzeigen der ersten Anmeldungs Animation** = deaktiviert	✓	✓	✓	✓
Computer Konfiguration #a0 administrative Vorlagen #a1 Windows-Komponenten #a2 Suche #a3 **Allow Cortana** = disabled	✓	✓	✗	✗
Computer Konfiguration #a0 administrative Vorlagen #a1 Windows-Komponenten #a2 Cloud-Inhalt #a3 **Deaktivieren von Microsoft Consumer Experience** = aktiviert	✓	✗	✗	✗

NOTE

Die oben genannten Gruppenrichtlinieneinstellungen können in Windows 10 Professional Edition angewendet werden.

Verwandte Themen

- Verwalten von Windows 10-Optionen für Start Layout und Taskleiste
- Einschränken von Windows 10 auf spezifische Apps
- Windows-Blickpunkt auf dem Sperrbildschirm
- Konfigurieren von Geräten ohne MDM

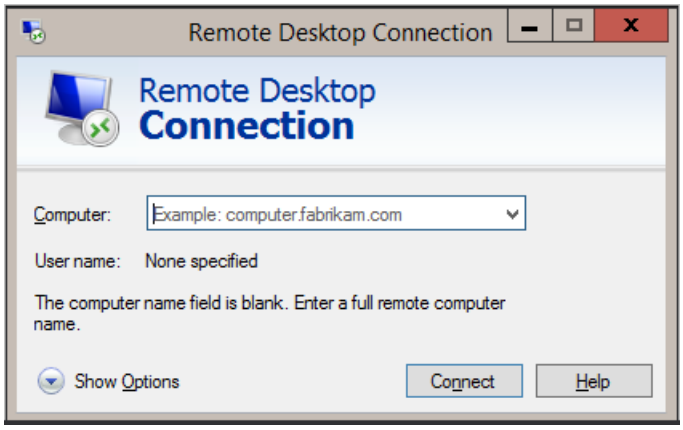
Verbinden mit einem PC, der Mitglied des Remote Azure Active Directory ist

27.02.2020 • 3 minutes to read

Gilt für

- Windows 10

Windows 10 unterstützt seit seiner Veröffentlichung Remoteverbindungen zu Mitgliedscomputern von Active Directory-Domänen. Ab Windows10, Version 1607, können Sie auch eine Verbindung zu einem Remotecomputer herstellen, der Mitglied einer Azure Active Directory (Azure AD)-Domäne ist.

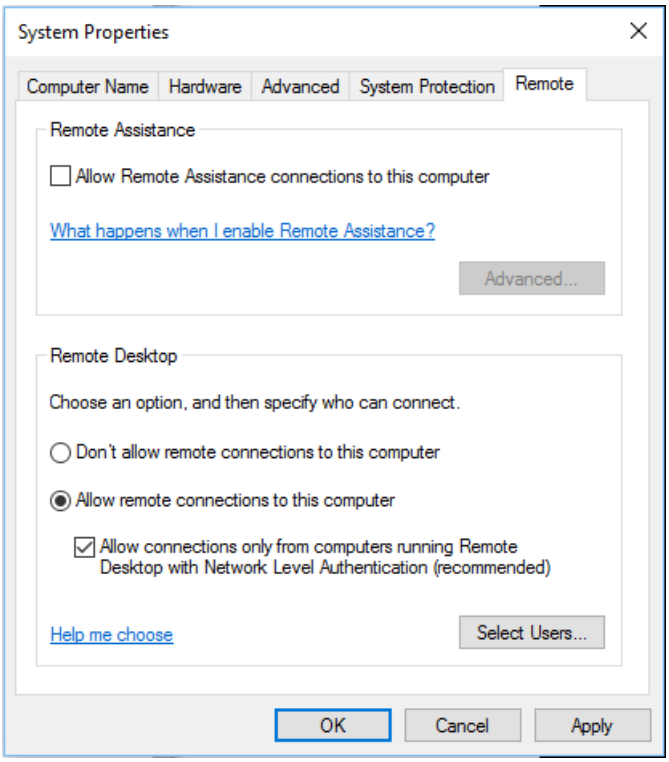


> **TIP**
> Ab Windows 10, Version 1809, können Sie die Biometrie verwenden, um sich bei einer Remotedesktopsitzung zu authentifizieren.

Einrichtung

- Auf beiden PCs (lokal und remote) muss Windows10 Version 1607 oder höher ausgeführt werden. Eine Remoteverbindung mit einem PC, der Mitglied des Azure AD ist, auf dem frühere Versionen von Windows10 ausgeführt werden, wird nicht unterstützt.
- Auf dem lokalen PC (von dem aus Sie eine Verbindung herstellen) muss entweder Azure AD beigetreten oder eine Hybrid Azure AD beigetreten sein. Eine Remote Verbindung mit einem Azure AD-Computer, der mit einem nicht verbundenen Gerät oder einem anderen Gerät als Windows 10 verbunden ist, wird nicht unterstützt. Stellen Sie sicher, dass Remote Credential Guard, ein neues Feature in Windows10, Version 1607, auf dem Client-PC deaktiviert ist, den Sie verwenden, um die Verbindung mit dem Remote-PC herzustellen.
- Gehen Sie auf dem PC, zu dem Sie eine Verbindung herstellen möchten, folgendermaßen vor:

  1. Öffnen Sie die Systemeigenschaften für den Remote-PC.
  2. Aktivieren Sie **Remoteverbindung mit diesem Computer zulassen** , und wählen Sie **Verbindungen nur von Computern zulassen, auf denen Remotedesktop mit Authentifizierung auf Netzwerkebene ausgeführt wird**.



3. Wenn der Benutzer, der den PC dem Azure AD hinzugefügt hat, der einzige ist, der eine Remoteverbindung herstellt, ist keine zusätzliche Konfiguration erforderlich. Um weiteren Benutzern die Verbindung mit dem PC zu erlauben, müssen Sie Remoteverbindungen für die lokale Gruppe **Authentifizierte Benutzer** zulassen. Klicken Sie auf **Benutzer auswählen**.

> **NOTE**
>
> Sie können einzelne Azure AD-Konten für Remoteverbindungen angeben, indem Sie den Benutzer mindestens einmal am Remotegerät anmelden lassen und dann das folgende PowerShell-Cmdlet ausführen:
>
> `net localgroup "Remote Desktop Users" /add "AzureAD\the-UPN-attribute-of-your-user"`, wobei *Vorname Nachname* der Name des Benutzerprofils in C:\Users\ ist, das auf der Grundlage des DisplayName-Attributs in Azure AD erstellt wird.
>
> Dieser Befehl funktioniert nur für AADJ-Geräte Benutzer, die bereits zu einer lokalen Gruppe (Administratoren) hinzugefügt wurden. Andernfalls wird mit diesem Befehl der folgende Fehler ausgelöst. Zum Beispiel:
> nur für Cloud-Benutzer: "Es gibt keinen solchen globalen Benutzer oder eine solche Gruppe: *Name*"
> für synchronisierten Benutzer: "Es gibt keinen solchen globalen Benutzer oder eine solche Gruppe: *Name*"
>
> In Windows10, Version 1709, muss der Benutzer nicht zuerst auf das Remotegerät anmelden.
>
> In Windows10, Version 1709, können Sie andere Azure AD-Benutzer zur **Administratoren**-Gruppe auf einem Gerät in **Einstellungen** hinzufügen und Remote-Anmeldeinformationen auf die **Administratoren** einschränken. Liegt ein Problem beim Remoteverbinden vor, stellen Sie sicher, dass beide Geräte mit Azure AD verbunden sind und dass TPM auf beiden Geräten ordnungsgemäß funktioniert.

4. Geben Sie **Authentifizierte Benutzer** ein, und klicken Sie dann auf **Namen überprüfen**. Wenn sich das Fenster **Name nicht gefunden** öffnet, klicken Sie auf **Speicherorte** , und wählen Sie „Dieser PC" aus.

> **TIP**
> Wenn Sie eine Verbindung mit dem Remotecomputer herstellen, geben Sie Ihren Kontonamen in `AzureAD UPN` folgendem Format ein:. Der lokale PC muss entweder Domänenmitglied oder Azure AD-Joined sein. Der lokale PC und der Remote-PC müssen sich im gleichen Azure AD-Mandanten befinden.

> **NOTE**
> Wenn Sie keine Verbindung mit der Remote Desktop Verbindung 6,0 herstellen können, müssen Sie die neuen Features von RDP 6,0 deaktivieren und wieder zu RDP 5,0 zurückkehren, indem Sie einige Änderungen in der RDP-Datei ändern. Einzelheiten finden Sie im Support Artikel.

Unterstützte Konfigurationen

In Organisationen, die Active Directory und Azure AD integriert haben, können Sie eine Verbindung von einem Hybrid-PC mit einem Azure AD-Join-PC herstellen, indem Sie Folgendes verwenden:

- Kennwort
- Smartcards
- Windows Hello for Business, wenn die Domäne vom Microsoft Endpoint Configuration Manager verwaltet wird

Bei Organisationen mit integriertem Active Directory und Azure AD können Sie folgendermaßen eine Verbindung von einem Azure AD-beigetretenen PC zu einem AD-beigetretenen PC herstellen, wenn der Azure AD-beigetretene PC in das Unternehmensnetzwerk eingebunden ist:

- Kennwort
- Smartcards
- Windows Hello for Business, wenn die Organisation über ein Abonnement für die mobile Geräteverwaltung (Mobile Device Management, MDM) verfügt.

Bei Organisationen mit integriertem Active Directory und Azure AD können Sie folgendermaßen eine Verbindung von einem Azure AD-beigetretenen PC zu einem anderen Azure AD-beigetretenen PC herstellen:

- Kennwort
- Smartcards
- Windows Hello for Business, mit oder ohne MDM-Abonnement.

Bei Organisationen, die nur Azure AD verwenden, können Sie folgendermaßen von einem Azure AD-beigetretenen PC zu einem anderen Azure AD-beigetretenen PC eine Verbindung herstellen:

- Kennwort
- Windows Hello for Business, mit oder ohne MDM-Abonnement.

> **NOTE**
> Wenn auf dem RDP-Client Windows Server 2016 oder Windows Server 2019 ausgeführt wird, um eine Verbindung mit Azure Active Directory-verbundenen Computern herstellen zu können, muss der RDP- Authentifizierungsanforderungen basierender Benutzer-zu-Benutzer (PKU2U) die Verwendung von Online Identitäten ermöglichen.

Verwandte Themen

Verwenden von Remotedesktop

Verknüpfen von Windows 10 Mobile mit Azure Active Directory

01.06.2019 • 10 minutes to read

Gilt für

- Windows 10 Mobile

Geräte mit Windows10 Mobile können Azure Active Directory (Azure AD) beitreten, wenn das Gerät während der Out-of-Box-Umgebung (OOBE) konfiguriert ist. In diesem Artikel werden die Überlegungen und Optionen für die Verwendung von Windows10 Mobile mit Azure AD in Ihrer Organisation beschrieben.

Gründe für die Teilnahme an Windows10 Mobile zu Azure AD

Wenn ein Gerät mit Windows10 Mobile mit Azure AD verbunden ist, kann das Gerät ausschließlich die Anmeldeinformationen Ihrer Organisation verwenden, und Sie können sicherstellen, dass sich Benutzer mit den Anmeldeanforderungen Ihrer Organisation anmelden. Die Teilnahme an einem mobilen Windows10-Gerät zu Azure Ad bietet viele der gleichen Vorteile wie das beitreten zu Desktopgeräten, wie beispielsweise:

- Einmaliges Anmelden (SSO) in Apps wie Mail, Word und OneDrive mithilfe von Ressourcen, die in Azure AD gesichert wurden.
- SSO in Microsoft-Edge-Browser mit einer mit Azure AD verbundenen Webanwendung, wie Office 365 Portal, Visual Studio und über 2500 Apps, die nicht von Microsoft stammen.
- SSO zu lokalen Ressourcen.
- Registrieren Sie sich automatisch bei Ihrem mobilen Geräteverwaltungsdienst (MDM).
- Aktivieren Sie die Einstellungen des Roamingbetriebs für Unternehmen. (Derzeit nicht unterstützt, aber geplant)
- Bereitstellen von Apps für Benutzer über den Microsoft Store für Unternehmen

Aktualisieren Sie aktuelle Geräte auf Windows10 Mobile?

Unter Windows Phone 8.1 gab es nur die Möglichkeit zur Verbindung des Geräts mit persönlichen Cloud-Diensten mithilfe eines Microsoft-Kontos für die Authentifizierung. Dafür war die Erstellung eines Microsoft-Kontos für Arbeitszwecke erforderlich. In Windows10 Mobile können Sie Geräte direkt an Azure AD anschließen, ohne ein persönliches Microsoft-Konto zu benötigen.

Wenn Sie über vorhandene Windows Phone 8,1-Geräte verfügen, müssen Sie zunächst wissen, ob die Geräte, die Sie haben, auf Windows10 Mobile aktualisiert werden können. Microsoft wird in Kürze weitere Informationen zur Verfügbarkeit von Upgrades veröffentlichen. Sobald weitere Informationen verfügbar sind, werden sie unter Abrufen von Windows 10 Mobile veröffentlicht. Premier Enterprise-Kunden, die ein Unternehmen benötigen, um das Upgrade von Windows10 Mobile zu verschieben, sollten sich an Ihren Technical Account Manager wenden, um zu verstehen, welche Optionen verfügbar sein können.

Vor dem Aktualisieren und Verknüpfen von Geräten mit Azure AD sollten Sie die aktuelle Datennutzung berücksichtigen. Die Art, wie Benutzer vorhandene Geräte nutzen und welche Daten lokal gespeichert werden, variiert für jeden Kunden. Werden SMS zur Arbeitszwecken verwendet und müssen sie gespeichert sowie nach dem Upgrade nutzbar sein? Gibt es Fotos, die lokal gespeichert werden oder mit einem Microsoft-Konto verknüpft

sind? Gibt es Geräte und App-Einstellungen, die beibehalten werden müssen? Sind Kontakte auf der SIM-Karte gespeichert, die einem Microsoft-Konto zugeordnet sind? Bevor Sie die Geräte mit Azure AD verknüpfen, müssen Sie sich über Methoden zur Aufzeichnung und Speicherung der Daten, die beibehalten werden sollen, informieren. Fotos, Musikdateien und Dokumente, die lokal auf dem Gerät gespeichert sind, können vom Gerät mit einer USB-Verbindung auf den PC kopiert werden.

Möchten Sie aktualisierte mobile Geräte mit Azure AD verbinden, müssen die Geräte zurückgesetzt werden, um die Willkommensseite des Geräte-Setups zu starten. Es ist nicht möglich, ein Gerät mit Azure AD zu verknüpfen und gleichzeitig bestehende Benutzerdaten beizubehalten. Dies ähnelt dem Ändern ein Geräts von persönlichem Besitz zu Unternehmensbesitz. Wenn ein Benutzer einer Unternehmensdomäne beitritt, muss er sich als Domänenbenutzer anmelden und ein neues Nutzerprofil verwenden. Ein neues Benutzerprofil bedeutet, dass bestehende Einstellungen, Apps oder Daten von vorherigen, persönlichen Profilen nicht beibehalten werden können.

Wenn Sie das Zurücksetzen des Geräts vermeiden möchten, sollten Sie Arbeitskonten hinzufügen, anstatt die Konten mit Azure AD zu verknüpfen.

Der Unterschied zwischen „Arbeitskonto hinzufügen" und „Azure AD verknüpfen"

Auch wenn die Azure AD-Mitgliedschaft auf Windows10 Mobile die beste Gesamterfahrung bietet, gibt es zwei Möglichkeiten, wie Sie ein hinzugefügtes Arbeitskonto verwenden können, anstatt das Gerät aufgrund organisatorischer Anforderungen zu Azure AD hinzuzufügen.

- Sie können die Windows-Willkommensseite mit der Option **Später anmelden** verlassen. Damit können Sie Windows10 Mobile mit einem verbundenen Azure AD-Konto oder einem Microsoft-Konto verwenden.
- Auf den Geräten können Sie ohne vorheriges Zurücksetzen weitere Zugriffsrechte für Azure AD-Backup-Ressourcen hinzufügen.

Keine dieser Methoden bietet jedoch SSO im Microsoft Store oder SSO für lokale Ressourcen, außerdem besteht keine Möglichkeit zur Synchronisierung von Einstellungen auf Grundlage des Azure AD-Kontos mit Roamingbetrieb für Unternehmen. Informationen zu Enterprise State Roaming in Azure AD.

Mit **Einstellungen** >; **Konten** > **Ihre E-Mail-Adresse und Konten** > **Geschäfts- oder Schulkonto hinzufügen** können Benutzer ihr Azure AD-Konto dem Gerät hinzufügen. Alternativ kann ein Arbeitskonto hinzugefügt werden, wenn der Benutzer sich für eine Anwendung wie Mail, Word usw. anmeldet. Wenn Sie in den Einstellungen die automatische Registrierung aktivieren, wird das Gerät automatisch im MDM registriert.

Ein zusätzliches Arbeitskonto bietet das gleiche SSO-Erlebnis bei Browser-Apps wie Office 365 (Office-Portal, Outlook im Web, Kalender, Kontakte, OneDrive), dem Azure AD-Profil, der App zur Änderung des Kennworts und Visual Studio. SSO ist für integrierte Anwendungen wie Mail, Kalender, Kontakte, OneDrive sowie Dateien, die auf OneDrive gehostet werden, verfügbar, d. h. Sie müssen kein Kennwort eingeben. In Office-Anwendungen wie Microsoft Word, Microsoft Excel usw. wählen Sie einfach das Azure AD-Konto aus; schon können Sie Dateien ohne Eingabe des Kennworts öffnen.

Vorbereiten für Windows10 Mobile

- **Azure AD-Konfiguration**

  Derzeit unterstützt die Azure AD-Verknüpfung nur die Selbstbereitstellung. Das bedeutet, dass die Anmeldeinformationen des Gerätenutzers während der ersten Einrichtung des Gerätes verwendet werden müssen. Wenn Ihr Mobilfunkanbieter Geräte in Ihrem Auftrag vorbereitet, wird dadurch die Möglichkeit, das Gerät mit Azure AD zu verbinden, beeinflusst. Viele IT-Administratoren möchten anfangs die Geräte für ihre Mitarbeiter selbst einrichten. Die Azure AD-Verbindung ist jedoch für Endanwender optimiert, was auch die Möglichkeit einer automatischen MDM-Einrichtung umfasst.

Standardmäßig ist Azure AD so eingerichtet, dass Geräte verbunden werden und Nutzer die Anmeldedaten ihres Unternehmens sowohl auf firmeneigenen als auch auf persönlichen Geräten nutzen können. Der Blogbeitrag Azure AD Join auf Windows 10-Geräten enthält weitere Informationen zur Überprüfung Ihrer Azure AD-Einstellungen. Sie können Azure AD so konfigurieren, dass alle Benutzer in Ihrer Organisation beitreten können, oder aber Sie haben die Möglichkeit, spezielle Azure AD-Gruppen auszuwählen.

- **Geräte-Setup**

  Ein Gerät mit Windows10 Mobile kann nur während OOBE an Azure AD teilnehmen. Neue Geräte von Mobilfunkanbietern befinden sich bei Auslieferung in diesem Status. Windows Phone 8,1-Geräte, die auf Windows10 Mobile aktualisiert werden, müssen zurückgesetzt werden, um für die Geräte Einrichtung wieder zu OOBE zu gelangen.

- **Mobile Geräteverwaltung**

  Für die Verwaltung von in Azure AD eingebundenen Geräten ist ein MDM-Dienst erforderlich. Sie können MDM nutzen, um Einstellungen und vom VPN oder WLAN verwendete Anwendungen und Zertifikate mithilfe von Push auf Geräte zu übertragen. Damit sich Geräte, die in Azure AD eingebunden sind, automatisch bei MDM registrieren, sind Lizenzen für Azure AD Premium oder Enterprise Mobility Suite (EMS) erforderlich. Weitere Informationen zum Einrichten des Azure AD-Mandanten zur automatischen Registrierung bei MDM.

- **Windows Hello**

  Standardmäßig ist die Erstellung eines Windows Hello (PIN) für Windows10 Mobile erforderlich und kann nicht deaktiviert werden. Sie können WindowsHello-Richtlinien mithilfe von Steuermechanismen in MDM (z. B. Intune) steuern. Weil das Gerät mithilfe von Anmeldeinformationen des Unternehmens eingebunden wurde, muss es über eine PIN zum Entsperren verfügen. Biometrische Daten wie Fingerabdruck oder Iriserkennung kann zur Authentifizierung verwendet werden. Zum Erstellen eines Windows Hello-Codes muss der Benutzer eine mehrstufige Authentifizierung durchführen, da es sich bei der PIN um eine starke Authentifizierungsanmeldeinformation handelt. Weitere Informationen zu Windows Hello für Azure AD

- **Bedingter Zugriff**

  Richtlinien für den bedingten Zugriff gelten auch für Windows10 Mobile. Mehrstufige Authentifizierung und Compliance-Regeln für Geräte können auf Benutzer und Ressourcen angewendet werden. Bevor der Zugriff auf Ressourcen erlaubt wird, ist erforderlich, dass der Benutzer oder das Gerät diese Anforderungen erfüllt. Richtlinien wie **Domänenbeitritt**, die herkömmliche Domänenbeitritte unterstützen, gelten nur für Desktop-PCs. Richtlinien, die abhängig von dem IP-Bereich sind, sind nur schwer auf einem Telefon umzusetzen, weil die IP-Adresse des Anbieters verwendet wird – es sei denn, der Benutzer ist mit einem WLAN- oder VPN-Netzwerk des Unternehmens verbunden.

- **Bekannte Probleme**

  - Die Apps für **Geräte-Backup und Wiederherstellung** sowie zum Synchronisieren von Fotos in OneDrive funktionieren nur mit dem Microsoft-Konto als Hauptkonto – diese Apps funktionieren nicht auf Geräten, die mit Azure AD verknüpft sind.

  - **Mein Handy finden** funktioniert, je nachdem, wie Sie Ihr Microsoft-Konto dem Gerät hinzufügen. Die Anwendung Cortana meldet sich beispielsweise so mit Ihrem Microsoft-Konto an, dass **Mein Handy finden** funktioniert. Cortana und OneNote funktionieren beide mit Azure AD-Konten, müssen jedoch zuerst mit einem Microsoft-Konto eingerichtet werden.

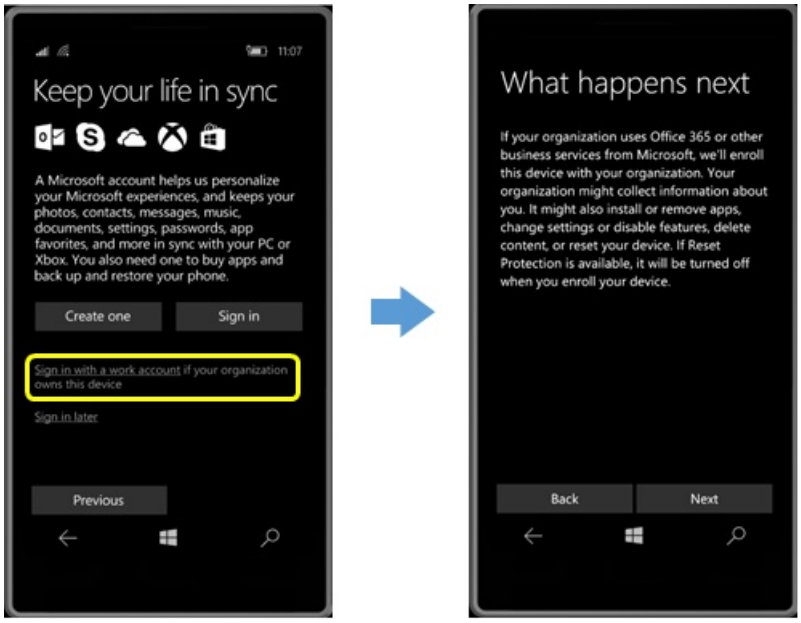
  - Bei OneNote muss sich der Benutzer mit einem Microsoft-Konto anmelden, muss aber mit dem Azure AD-Konto auch den Zugriff auf Notizbücher ermöglichen.

  - Wenn Ihre Organisation mit Azure AD arbeitet, benötigt der Verbindungsproxy Active Directory-

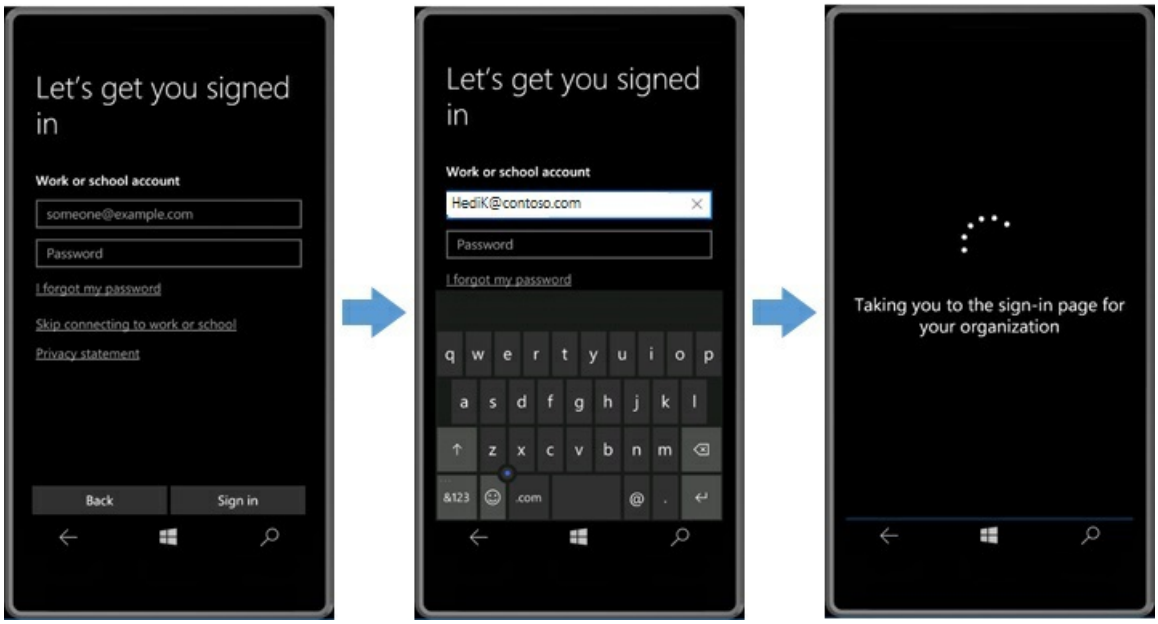
Verbunddienste (Active Directory Federation Services, ADFS) oder eine Drittpartei, die WS-Trust-Endpunkte genau wie ADFS unterstützt.

Beitreten zu Windows10 Mobile zu Azure AD

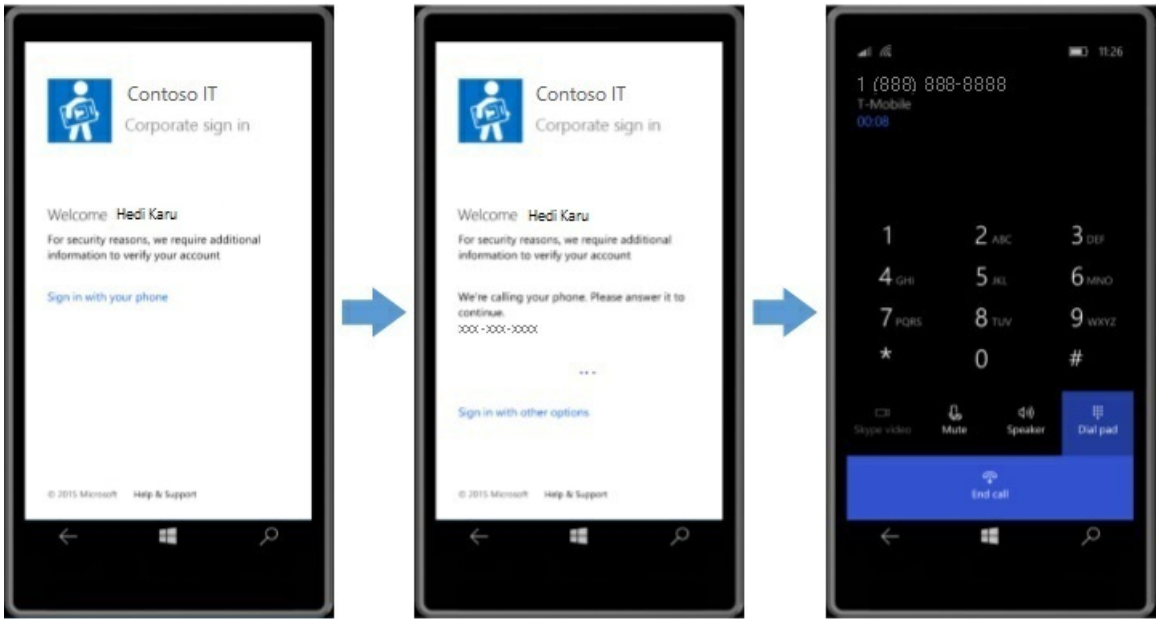
1. Wählen Sie unter **Behalten Sie den Überblick** auf der Windows-Willkommensseite die Option **Mit Arbeitskonto anmelden** aus, und tippen Sie dann auf **Weiter**.



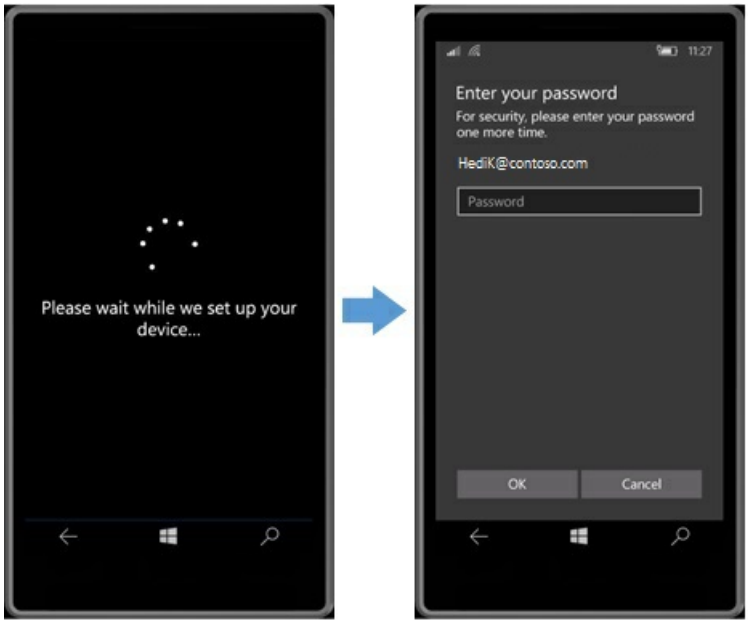
2. Geben Sie Ihr Azure AD-Konto ein. Wenn Ihr Azure AD-Konto ein Verbundkonto ist, werden Sie auf die Anmeldeseite Ihrer Organisation umgeleitet. Wenn dies nicht der Fall ist, geben Sie Ihr Kennwort hier ein.



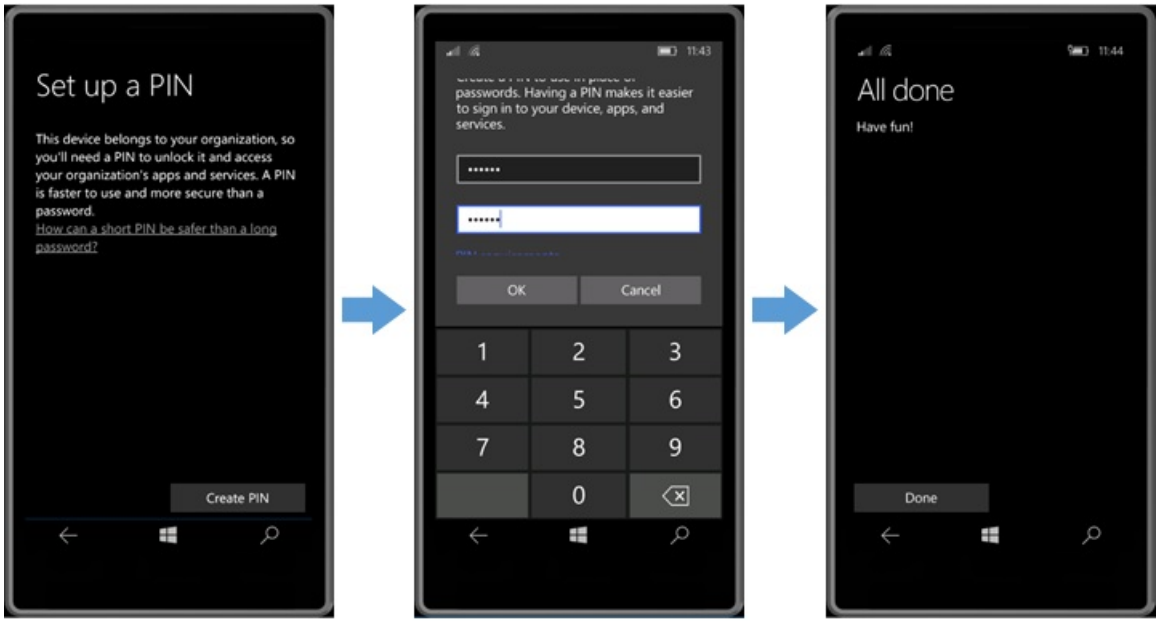
Wenn Sie auf die Anmeldeseite Ihrer Organisation weitergeleitet werden, müssen Sie u. U. einen zweiten Authentifizierungsfaktor angeben.



3. Nach Abschluss der Authentifizierung ist die Geräteregistrierung abgeschlossen. Verfügt Ihr MDM-Dienst über Nutzungsbedingungen, würden sie hier auch angezeigt werden. Verbundene Benutzer müssen erneut ein Kennwort zum Abschließen der Authentifizierung von Windows bereitstellen. Für Benutzer mit Kennwörtern, die in der Cloud verwaltet werden, wird diese Aufforderung nicht angezeigt. Für diese Verbundanmeldung muss Ihr Verbundserver einen aktiven WS-Trust-Endpunkt unterstützen.



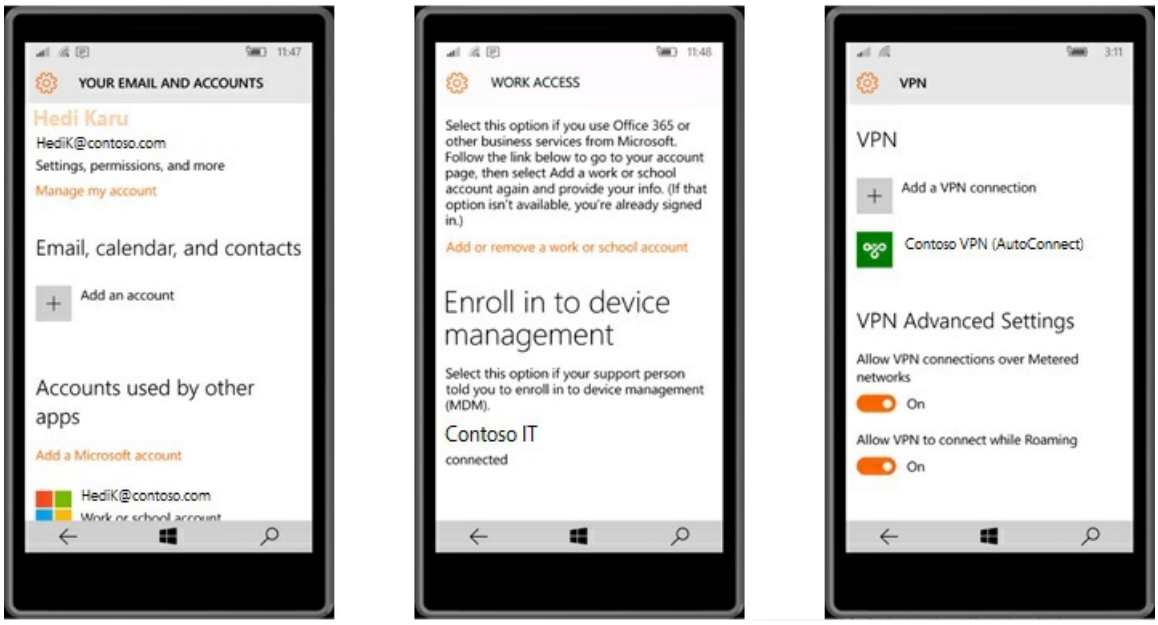
4. Richten Sie als Nächstes eine PIN ein.



HinweisWenn Sie mehr über die PIN-Anforderung erfahren möchten, lesen Sie warum eine PIN besser als ein Kennwort ist.

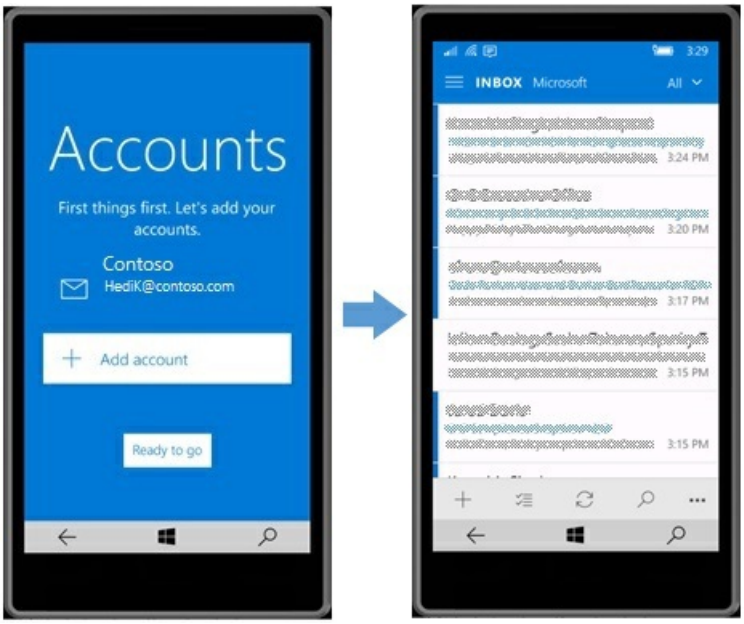
So überprüfen Sie den Azure AD-Beitritt

- Wechseln Sie zu **Einstellungen** > **Konten** > **Ihre E-Mail-Adresse und Konten**. Ihr Azure AD-Konto wird zuerst aufgeführt und ist weiterhin als Konto aufgelistet, das von anderen Apps verwendet wird. Wurde die automatische Registrierung bei MDM eingerichtet, sehen Sie unter **Einstellungen** > **Konten** > **Arbeitsplatzzugriff**, ob das Gerät ordnungsgemäß bei MDM registriert ist. Wenn MDM ein Zertifikat zur Nutzung durch ein VPN mithilfe von Push überträgt, wird unter **Einstellungen** > **Netzwerk & Drahtlos** > **VPN** die Möglichkeit einer VPN-Verbindung angegeben.

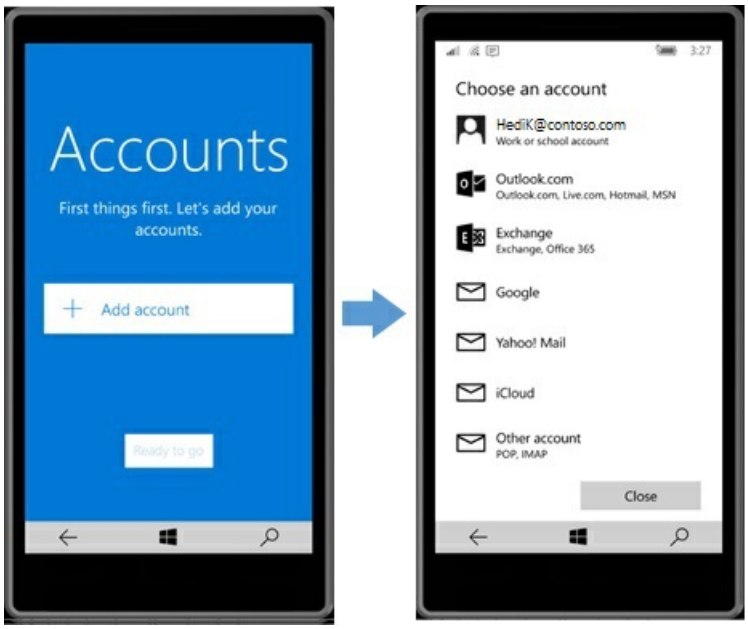


Einrichten von E-Mail und Kalender

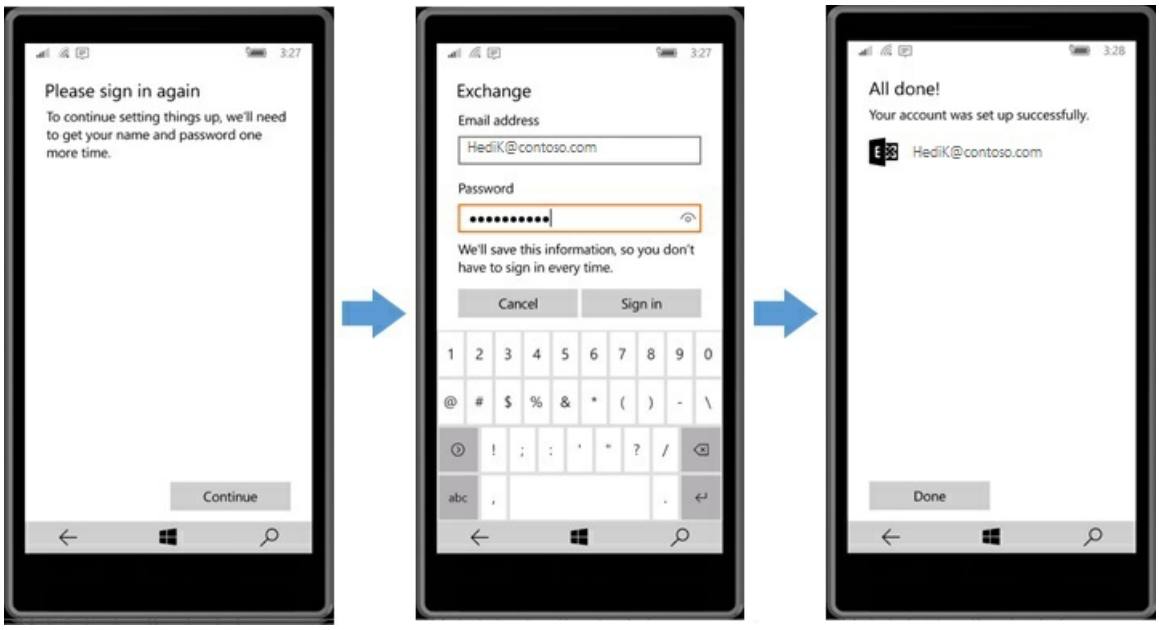
Das Einrichten von E-Mails auf Ihrem in Azure AD eingebundenen Gerät ist einfach. Nach Installation der **Mail** App gelangen Sie auf die **Konten**-Seite. Die E-Mail-Konten der meisten Benutzer werden in Office 365 gehostet, sodass die Synchronisierung automatisch gestartet wird. Tippen Sie einfach auf **Startklar**.



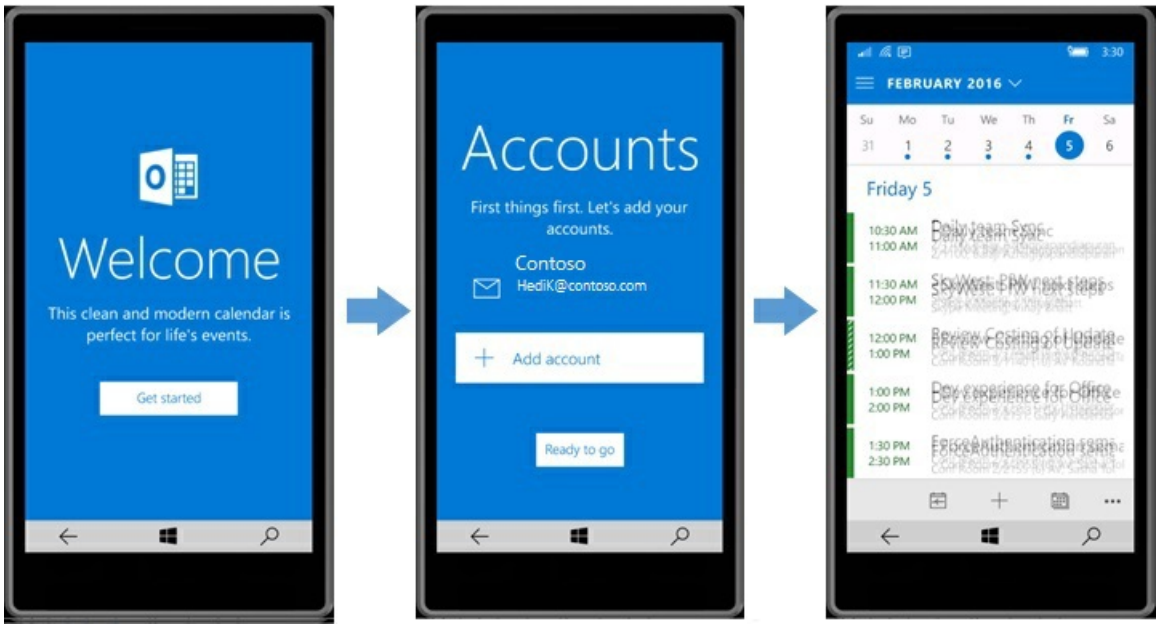
Wenn E-Mails lokal in Exchange gehostet werden, muss der Benutzer Anmeldeinformationen angeben, um unter Verwendung der Standardauthentifizierung eine Verbindung mit dem Exchange-Server herzustellen. Tippen Sie auf **Konto hinzufügen**, um die E-Mail-Konten zu sehen, die hinzugefügt werden können, einschließlich Ihres Azure AD-Kontos.



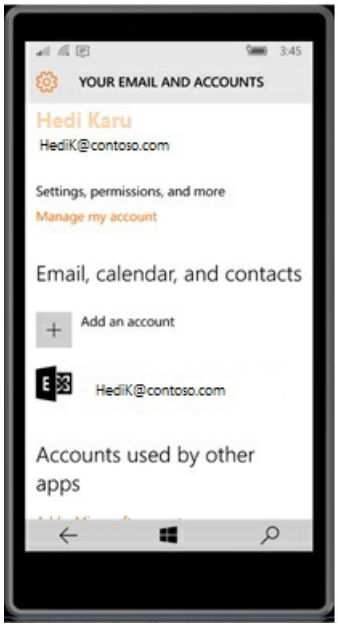
Nach der Auswahl eines Kontotyps geben Sie zum Abschluss der Installation Anmeldeinformationen für das Postfach an.



Die Installation ähnelt der Einrichtung der **Kalender** App. Öffnen Sie die App, damit Ihr Azure AD-Konto angezeigt wird – tippen Sie anschließend einfach auf **Startklar**.



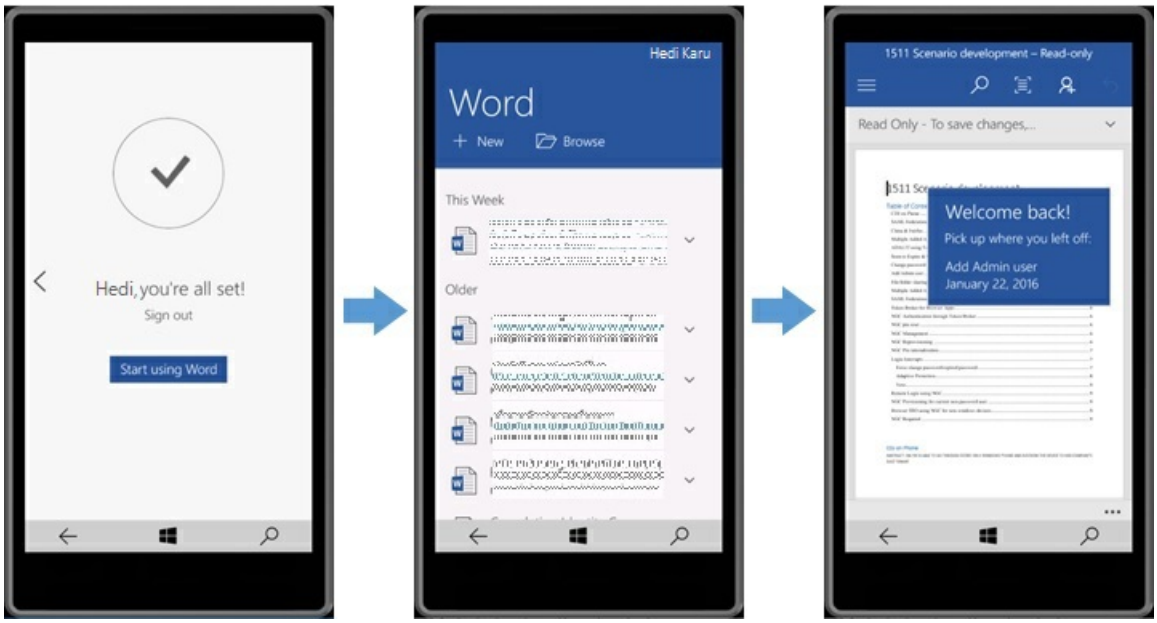
Kehren Sie zu **Einstellungen** > **Konten** > **Ihre E-Mail-Adresse und Konten** zurück, um das für **E-Mail, Kalender und Kontakte** aufgeführte Azure AD-Konto zu sehen.



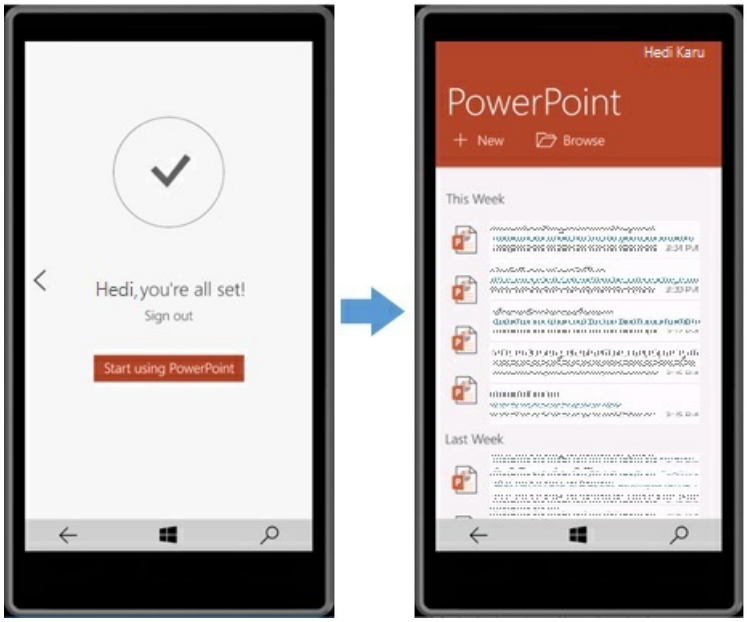
Verwenden von Office- und OneDrive-Apps

Office-Anwendungen wie Microsoft Word und Microsoft PowerPoint verbinden sich automatisch mit Ihrem Azure AD-Konto. Wenn Sie eine Office-App öffnen, sehen Sie einen Bildschirm, auf dem Sie zwischen einem Microsoft-Konto und einem Azure AD-Konto auswählen können. Während Office diesen Bildschirm anzeigt, werden Sie automatisch angemeldet. Haben Sie einige Sekunden Geduld und Office meldet Sie automatisch mit Ihrem Azure AD-Konto an.

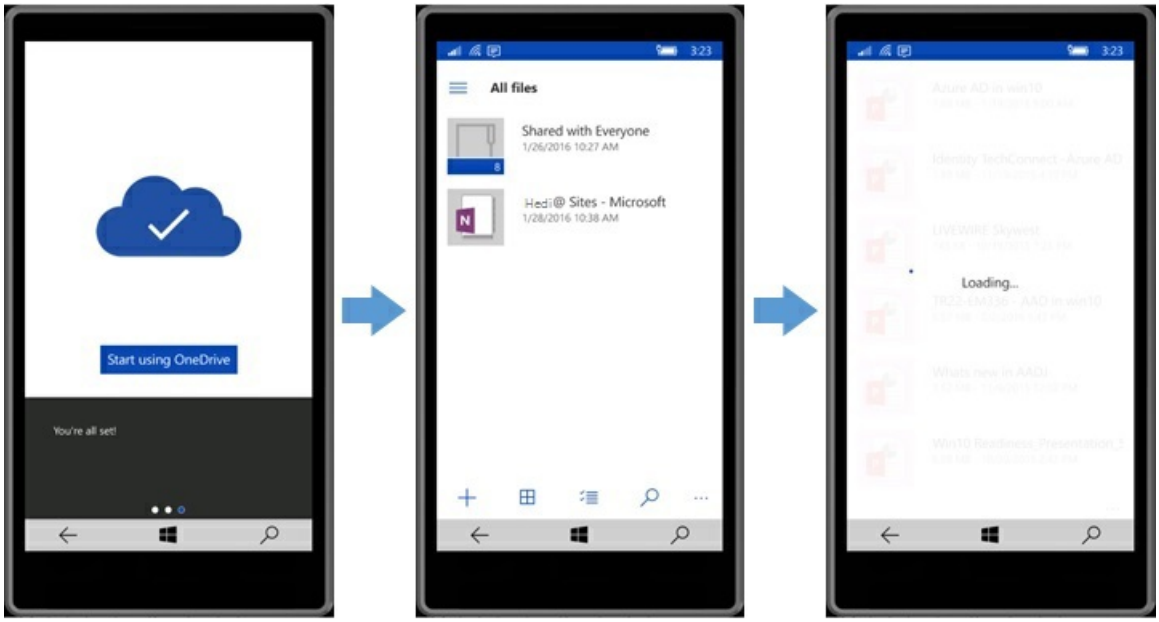
Microsoft Word zeigt automatisch die auf anderen Gerät zuletzt geöffneten Dokumente an. Beim Öffnen eines Dokuments können Sie direkt zu dem auf einem anderen Gerät zuletzt bearbeiteten Abschnitt wechseln.

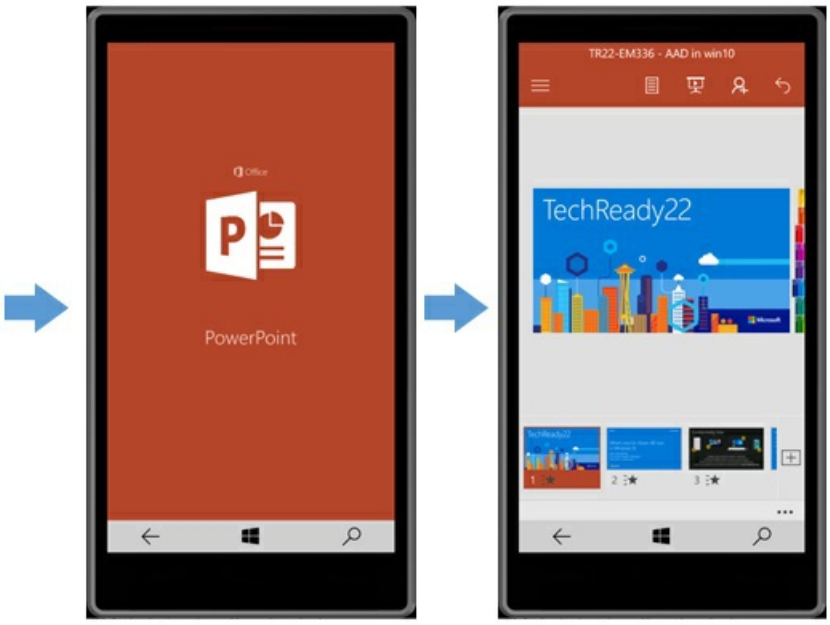


Microsoft PowerPoint zeigt die zuletzt geöffneten Foliengruppen an.



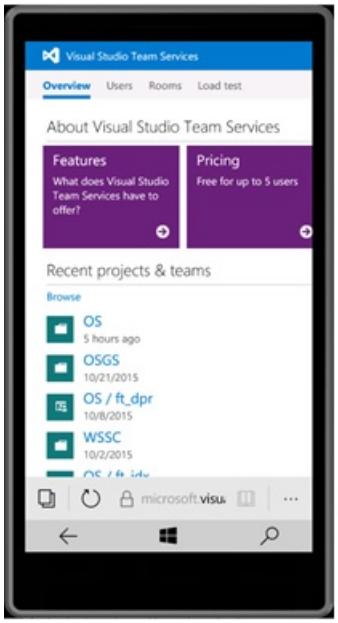
Die OneDrive-Anwendung verwendet auch SSO, zeigt Ihnen alle Ihre Dokumente an und ermöglicht es Ihnen, sie ohne weitere Authentifizierung zu öffnen.

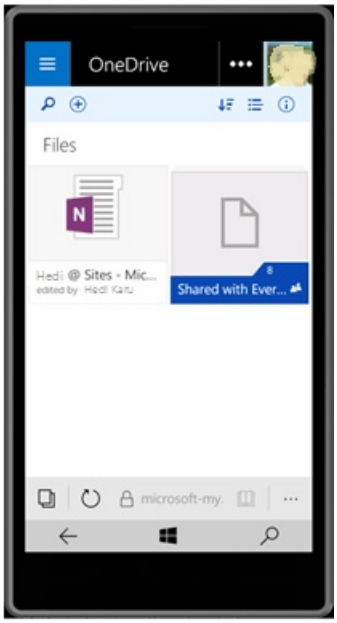




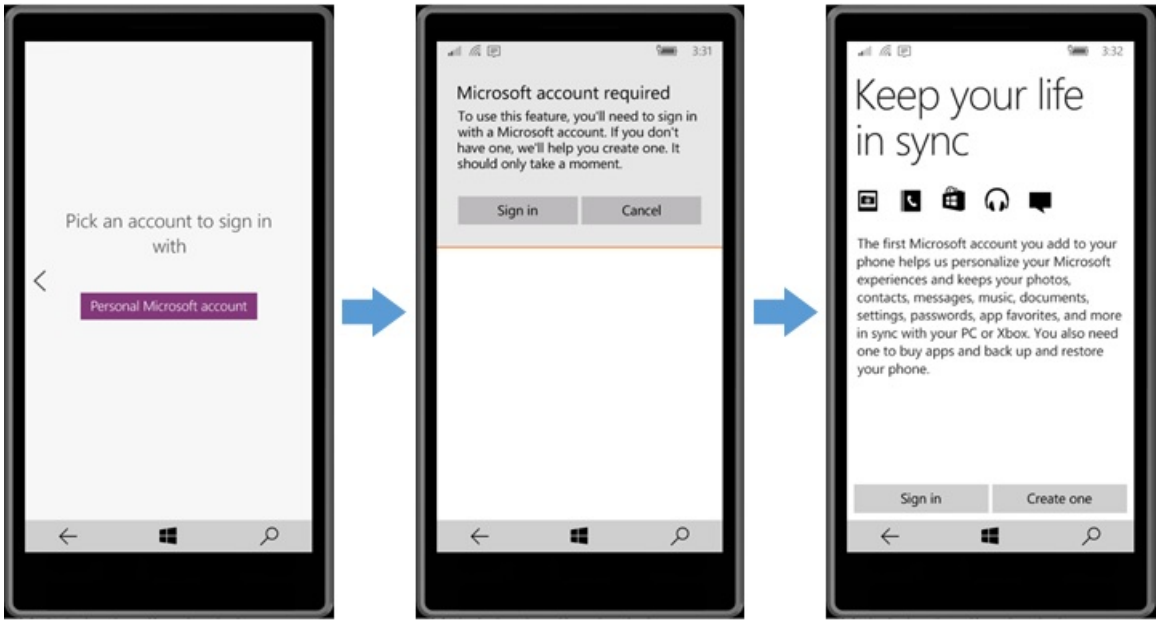
Zusätzlich zu SSO für Anwendungen können in Azure AD eingebundene Geräte auch SSO für

Browseranwendungen nutzen, die Azure AD vertrauen, z. B. Webanwendungen, Visual Studio, das Office 365-Portal und OneDrive for Business.

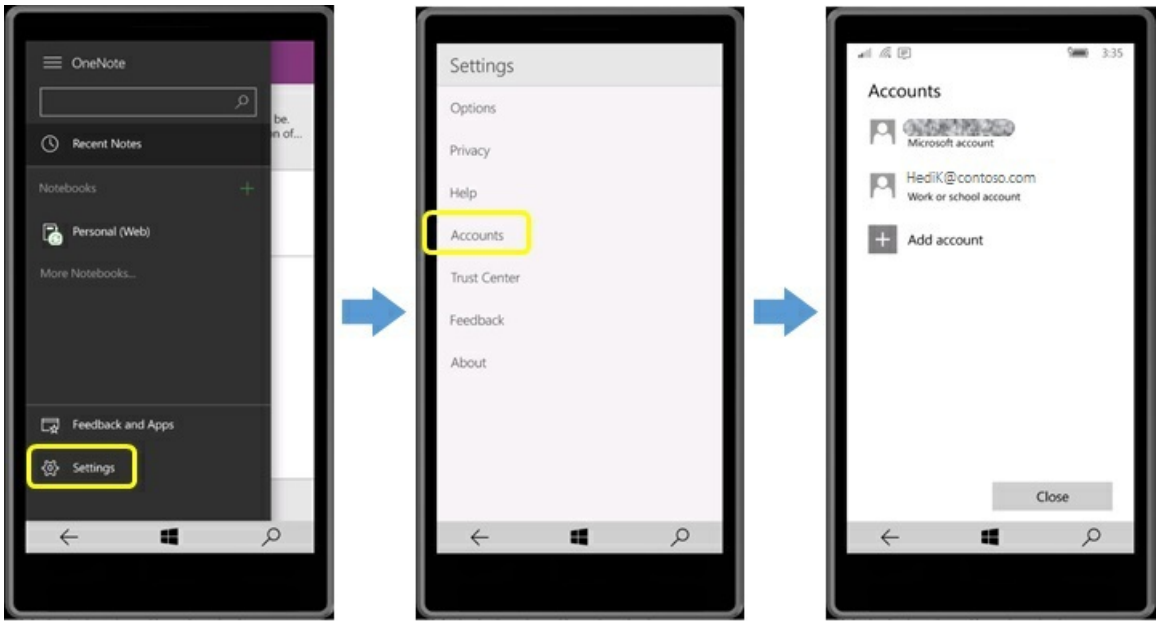




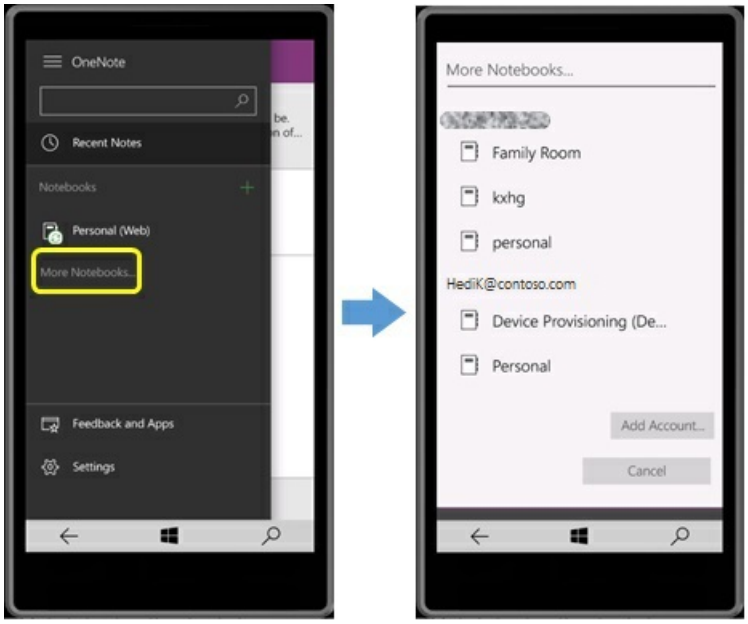
OneNote erfordert ein Microsoft-Konto, Sie können jedoch auch Ihr Azure AD-Konto verwenden.



Wechseln Sie nach der Anmeldung bei OneNote zu „Einstellungen > Konten“. Dort sehen Sie, dass Ihr Azure AD-Konto automatisch hinzugefügt wurde.

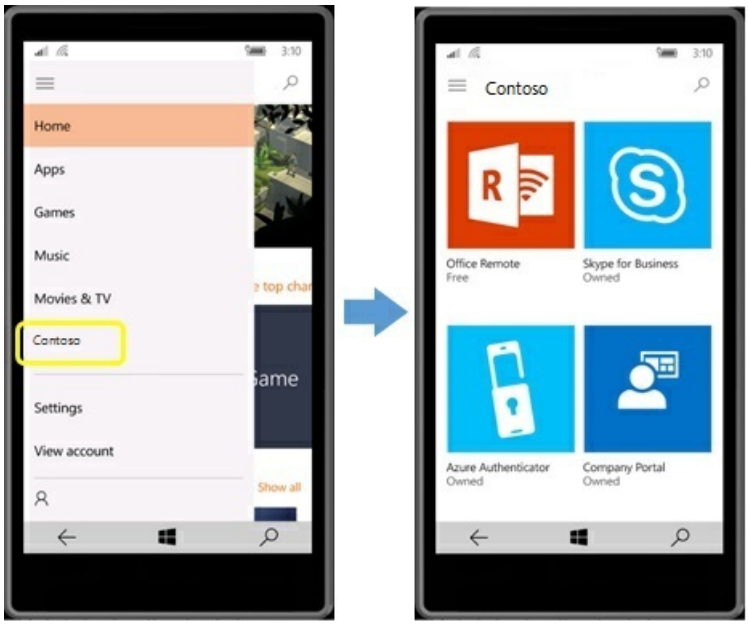


Um die Notizbücher anzuzeigen, auf die Ihr Azure AD-Konto zugreifen kann, tippen Sie auf **Weitere Notizbücher**, und wählen Sie das Notizbuch aus, das Sie öffnen möchten.



Verwenden des Microsoft Store für Unternehmen

In Microsoft Store für Unternehmen können Sie angeben, welche Anwendungen Ihren Benutzern in der Microsoft Store-App zur Verfügung stehen sollen. Diese Anwendungen werden auf einer Registerkarte mit dem Namen Ihres Unternehmens angezeigt. Anwendungen, die über das Portal des Microsoft Store für Unternehmen zugelassen wurden, können von Benutzern installiert werden.


3:10
Home
Apps
Games
Music
Movies & TV
Contoso
Settings
View account
Show all
3:10
Contoso
Office Remote
Free
Skype for Business
Owned
Azure Authenticator
Owned
Company Portal
Owned

Neue Richtlinien bei Windows 10

20.12.2019 • 15 minutes to read

Gilt für:

- Windows 10
- Windows 10 Mobile

Windows10 enthält die folgenden neuen Richtlinien für die Verwaltung. Vollständigen Satz von ADMX-Dateien mit administrativen Vorlagen für Windows 10 herunterladen.

Neue Gruppenrichtlinieneinstellungen in Windows10, Version 1809

Die folgenden Gruppenrichtlinieneinstellungen wurden in Windows 10, Version 1809, hinzugefügt:

Startmenü und Taskleiste

- Start-Menü und Taskbar\Force werden entweder in voller Bildschirmgröße oder in der Menügröße angezeigt
- Start-Menü und Taskbar\Remove "zuletzt hinzugefügt"-Liste aus dem Startmenü
- Menü "Start" und Taskbar\Remove "alle Programme" im Menü "Start"
- Startmenü und Taskbar\Remove-Liste "häufige Programme" im Startmenü

System

- System\Group Policy\Allow asynchrone Benutzergruppenrichtlinien Verarbeitung bei der Anmeldung über Remote Desktop Dienste
- System\Group Policy\Configure-Richtlinienverarbeitung
- System\Group Policy\Configure-Datenquellen, Richtlinienverarbeitung für Präferenz Erweiterungen
- System\Group Policy\Configure Devices, Richtlinienverarbeitung für Präferenz Erweiterungen
- System\Group Policy\Configure Drive Maps, Richtlinienverarbeitung für Präferenz Erweiterungen
- System\Group Policy\Configure-Richtlinie für die Richtlinienverarbeitung von Umgebungseinstellungen
- System\Group Policy\Configure files-Richtlinienverarbeitung für Präferenz Erweiterungen
- System\Group-Policy\Configure, Richtlinienverarbeitung für Einstellungserweiterungen
- System\Group Policy\Configure Folders, Richtlinienverarbeitung für Einstellungserweiterungen
- System\Group-Policy\Configure ini-Dateien, Richtlinienverarbeitung für Präferenz Erweiterungen
- System\Group Policy\Configure Internet Einstellungen, Richtlinienverarbeitung
- System\Group Policy\Configure-Richtlinienverarbeitung für lokale Benutzer und Gruppen
- System\Group Policy\Configure-Einstellungen für die Richtlinienverarbeitung für Netzwerkoptionen
- System\Group Policy\Configure Network Shares-Richtlinienverarbeitung für Präferenz Erweiterungen
- System\Group Policy\Configure-Einstellungen für die Richtlinienverarbeitung für Energieoptionen
- System\Group Policy\Configure Printer Preference Extension Policy processing
- System\Group Policy\Configure, Richtlinienverarbeitung für Präferenz Erweiterungen
- System\Group Policy\Configure-Richtlinienverarbeitung für Registrierungseinstellungen
- System\Group Policy\Configure Scheduled Tasks, Richtlinienverarbeitung für Einstellungserweiterungen
- System\Group Policy\Configure-Richtlinienverarbeitung für die Präferenz Erweiterung
- System\Group Policy\Configure-Tastenkombinationen für die Richtlinienverarbeitung
- System\Group Policy\Configure-Start Menü-Richtlinienverarbeitung
- System\Group Policy\Logging-und tracing\Configure-Anwendungseinstellungen, Protokollierung und

Ablaufverfolgung

- System\Group Policy\Logging-und tracing\Configure-Datenquellen-Einstellungen für Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging und tracing\Configure Devices-Einstellungen für Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging und tracing\Configure Drive Maps-Einstellungen für Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure-Umgebungseinstellungen, Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure-Datei Einstellungen, Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure-Ordneroptionen, Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure-Ordner-Einstellungen für Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure ini-Dateien, Einstellungen für Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging und tracing\Configure Internet Einstellungen, Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging und tracing\Configure lokale Benutzer und Gruppen-Präferenz Protokollierung und-Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure-Netzwerkoptionen, Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure-Netzwerkfreigaben, Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging und tracing\Configure-Einstellungen für die Energieoptionen-Protokollierung und-Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure-Druckereinstellungen für Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure-Einstellungen für die regionale Einstellungen-Protokollierung und Ablaufverfolgung
- Protokollierung und Ablaufverfolgung der Registrierungseinstellungen für System\Group Policy\Logging und tracing\Configure
- System\Group Policy\Logging-und tracing\Configure-Einstellungen für geplante Aufgaben, Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging und tracing\Configure Services-Einstellungen Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure-Tastenkombinationen, Protokollierung und Ablaufverfolgung
- System\Group Policy\Logging-und tracing\Configure-Startmenü-Einstellungen für Protokollierung und Ablaufverfolgung
- System\Kernel-DMA-Protection\Enumeration-Richtlinie für externe Geräte, die mit dem Kernel-DMA-Schutz unvereinbar sind
- System\OS Policies\Allow-Zwischenablage-Protokoll
- System\OS Policies\Allow-Zwischenablage Synchronisierung auf Geräten

Windows-Komponenten

- Windows Components\Data Collection and Preview Builds\Configure Microsoft 365 Update Readiness Upload Endpoint
- Windows-Components\Data Sammlung und Vorschau Builds\Disable Löschen von Diagnosedaten

- Windows Components\Data-Sammlung und Vorschau Builds\Disable Diagnostic Data Viewer
- Windows-Components\Delivery-Optimierung \ [reserviert für spätere Verwendung] Cache Server-Hostname
- Windows-Komponenten\Position und Sensoren\Windows-Positionssuche\Windows-Positionssuche deaktivieren
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkte/zulässige Snap-ins\DFS-Verwaltung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkter/zulässiger Snap-ins\File-Server Ressourcen-Manager
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkte/zulässige Snap-ins\Share-und Speicherverwaltung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ restricted/zulässiger Snap-ins\Storage-Manager für Sans
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ restricted/zulässig Snap-Ins\Erweiterungs-Snap-Ins Snap-ins\DFS-Verwaltungserweiterung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ restricted/zulässig Snap-Ins\Erweiterungs-Snap-Ins Snap-ins\Disk-Verwaltungserweiterung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-Ins\Erweiterungs-Snap-Ins Snap-ins\File Server Resource Manager-Erweiterung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ restricted/zulässig Snap-Ins\Erweiterungs-Snap-Ins Snap-ins\Share-und Speicher Verwaltungserweiterung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-Ins\Erweiterungs-Snap-Ins Snap-ins\Storage-Manager für Sans-Erweiterung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Group-Richtlinien Verwaltungs-Editor
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkter/zulässiger Snap-ins\Group Policy\Group Richtlinien-Starter-GPO-Editor
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung von Anwendungs-Snap-Ins
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ restricted/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Anwendungs Einstellungserweiterung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungen für die Systemsteuerung (Computer)
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ restricted/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungen für das Control Panel (Benutzer)
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "Datenquellen"
- Windows-Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ restricted/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Geräte-Einstellungserweiterung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "Laufwerk Karten"
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Umgebungs Einstellungserweiterung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Datei-Einstellungserweiterung

- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "Ordneroptionen"
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Ordner-Einstellungserweiterung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "INI-Dateien"
- Windows-Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung für Internet Einstellungen
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkte/zulässige Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "lokale Benutzer und Gruppen"
- Windows-Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "Netzwerkoptionen"
- Windows-Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "Netzwerkfreigaben"
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ restricted/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "Energieoptionen"
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Registerkarte "Einstellungen"
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Drucker-Einstellungserweiterung
- Windows-Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "regionale Einstellungen"
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Registrierungs Einstellungserweiterung
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ restricted/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung für geplante Aufgaben
- Windows-Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "Dienste"
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "Verknüpfungen"
- Windows Vorlagen\Windows-Komponenten\Microsoft-Verwaltungskonsole \ eingeschränkt/zulässig Snap-ins\Group Policy\Preference-Snap-in extensions\Permit Verwendung der Einstellungserweiterung "Startmenü"
- Windows Components\OOBE\Don 't Launch Datenschutzeinstellungen bei der Benutzeranmeldung
- Windows Components\OOBE\Don 't Launch Datenschutzeinstellungen bei der Benutzeranmeldung
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\Application Compatibility\Do nicht die IP-Adresse des Remote Desktop-Sitzungs Host Servers verwenden, wenn keine virtuelle IP-Adresse verfügbar ist
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\Application Compatibility\Select den Netzwerkadapter für die Remote Desktop-IP-Virtualisierung

verwenden

- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\Application Compatibility\Turn off Windows Installer RDS-Kompatibilität
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\Application Compatibility\Turn auf der Remote Desktop-IP-Virtualisierung
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\Connections\Allow Remote Start von nicht aufgelisteten Programmen
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\Connections\Turn off Fair-Share-CPU-Planung
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Geräte-und Ressourcen Redirection\Allow Zeitzonenumleitung
- Windows Remotedesktopdienste Desktop-Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Geräte-und Ressourcen Redirection\Do nicht zulassen Zwischenablageumleitung
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\Printer Redirection\Redirect nur den Standardclientdrucker
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\Printer Redirection\Redirect nur den Standardclientdrucker
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\RD Connection Broker\Use RD-Verbindungs Broker-Lastenausgleich
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Vorlagen\Windows-Komponenten\Remotedesktopdienste\Remotedesktop-Sitzungshost\Umgebung für Remotesitzung Environment\Allow Desktopkomposition für Remote Desktopsitzungen
- Windows Remotedesktopdienste Desktop-Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Vorlagen\Windows-Komponenten\Remotedesktopdienste\Remotedesktop-Sitzungshost\Umgebung für Remote Session Environment\Always Show Desktop on connection
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Vorlagen\Windows-Komponenten\Remotedesktopdienste\Remotedesktop-Sitzungshost\Umgebung für Remote Session Environment\Do nicht zulassen, dass die Schriftart glättet
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Vorlagen\Windows-Komponenten\Remotedesktopdienste\Remotedesktop-Sitzungshost\Umgebung für Remotesitzung Environment\Remove Remote Desktop Hintergrund
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\Session Zeit Limits\Set Zeitlimit für die Abmeldung von RemoteApp-Sitzungen
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Host\Session Zeit Limits\Set Zeitlimit für die Abmeldung von RemoteApp-Sitzungen
- Windows Vorlagen\Windows-Komponenten\Windows Defender-Antivirus\Configure-Erkennung für potenziell unerwünschte Anwendungen
- Windows Vorlagen\Windows-Komponenten\Windows Defender Antivirus\Scan\Configure niedrige CPU-Priorität für geplante Scans
- Windows Vorlagen\Windows-Komponenten\Windows Defender-Anwendung Guard\Allow Kamera-und Mikrofon Zugriff in Windows Defender Application Guard
- Windows Vorlagen\Windows-Komponenten\Windows Defender-Anwendung Guard\Allow, dass Benutzer Dateien Vertrauen, die in Windows Defender Application Guard geöffnet sind
- Windows Vorlagen\Windows-Komponenten\Windows Defender-Anwendung Guard\Allow Windows Defender Application Guard zur Verwendung von Stammzertifizierungsstellen auf dem Gerät des Benutzers
- Windows Vorlagen\Windows-Komponenten\Windows Defender-Anwendung Guard\Configure zusätzlicher Quellen für nicht vertrauenswürdige Dateien in Windows Defender Application Guard
- Windows Vorlagen\Windows-Komponenten\Windows Hello for Business\Use Windows Hello for Business-Zertifikate als Smartcard-Zertifikate

- Windows Vorlagen\Windows-Komponenten\Windows-Medien Player\Do nicht anzeigen der ersten Verwendung von Dialog Feldern
- Automatische Updates für Windows Vorlagen\Windows-Komponenten\Windows Media Player\Prevent
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Prevent CD-und DVD-Medien Informationsabruf
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Prevent Desktop Verknüpfungserstellung
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Prevent Medienfreigabe
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Prevent Music File Media Information Retrieval
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Prevent Schnellstartleiste-Verknüpfungserstellung
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Prevent Radio Sender Preset Retrieval
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Prevent Video glätten
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Networking\Configure http-Proxy
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Networking\Configure MMS-Proxy
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Networking\Configure-Netzwerkpufferung
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Networking\Configure RTSP-Proxy
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Networking\Hide Network (Registerkarte)
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Networking\Streaming Media Protocols
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Playback\Allow Bildschirmschoner
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\Playback\Prevent Codec herunterladen
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\User Interface\Do nicht Anchor anzeigen
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\User Interface\Hide-Registerkarte "Datenschutz"
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\User Interface\Hide-Registerkarte "Sicherheit"
- Windows Vorlagen\Windows-Komponenten\Windows Media Player\User Interface\Set und Lock Skin
- Windows Vorlagen\Windows-Komponenten\Windows Security\Account protection\Hide den Kontoschutz Bereich
- Windows Vorlagen\Windows-Komponenten\Windows Security\App und Browser protection\Hide APP und Browser Schutzbereich
- Windows Vorlagen\Windows-Komponenten\Windows Security\App und Browser protection\Prevent Benutzer vom Ändern von Einstellungen
- Windows Vorlagen\Windows-Komponenten\Windows Security\Device-Leistung und health\Hide der Geräteleistung und des Integritäts Bereichs
- Windows Vorlagen\Windows-Komponenten\Windows Security\Device security\Disable die Schaltfläche "TPM löschen"
- Windows Vorlagen\Windows-Komponenten\Windows Security\Device security\Hide den Bereich "Gerätesicherheit"
- Windows Vorlagen\Windows-Komponenten\Windows Security\Device security\Hide den sicheren Startbereich
- Windows Vorlagen\Windows-Komponenten\Windows Security\Device security\Hide der Seite "Sicherheitsprozessor (TPM)-Problembehandlung"
- Windows Vorlagen\Windows-Komponenten\Windows Security\Device security\Hide der TPM-Firmware-Update Empfehlung
- Windows Vorlagen\Windows-Komponenten\Windows Security\Enterprise Customization\Configure benutzerdefinierte Kontaktinformationen

- Windows Vorlagen\Windows-Komponenten\Windows Security\Enterprise Customization\Configure benutzerdefinierte Benachrichtigungen
- Windows Vorlagen\Windows-Komponenten\Windows Security\Enterprise Customization\Specify Kontakt Firmenname
- Windows Vorlagen\Windows-Komponenten\Windows Security\Enterprise Customization\Specify Kontakt-e-Mail-Adresse oder e-Mail-ID
- Windows Vorlagen\Windows-Komponenten\Windows Security\Enterprise Customization\Specify Kontakt Telefonnummer oder Skype-ID
- Windows Vorlagen\Windows-Komponenten\Windows Security\Enterprise Customization\Specify-Kontakt Website
- Windows Vorlagen\Windows-Komponenten\Windows Security\Family options\Hide den Bereich "Familienoptionen"
- Windows Vorlagen\Windows-Komponenten\Windows Security\Firewall und Netzwerk protection\Hide Firewall und Netzwerkschutz Bereich
- Windows Vorlagen\Windows-Komponenten\Windows Security\Notifications\Hide alle Benachrichtigungen
- Windows Vorlagen\Windows-Komponenten\Windows Security\Notifications\Hide nicht kritische Benachrichtigungen
- Windows Vorlagen\Windows-Komponenten\Windows Security\Systray\Hide Windows Security Systray
- Windows Vorlagen\Windows-Komponenten\Windows Security\Virus und Bedrohungs protection\Hide des Ransomware-Daten Wiederherstellungsbereichs
- Windows Vorlagen\Windows-Komponenten\Windows Security\Virus und Bedrohungs protection\Hide des Viren-und Bedrohungsschutz Bereichs
- Windows Vorlagen\Windows-Komponenten\Windows Update\Display-Optionen für Update Benachrichtigungen
- Windows Vorlagen\Windows-Komponenten\Windows Update\Remove Zugriff auf das Feature "Updates anhalten"

Systemsteuerung

- Steuern der Panel\Settings Seitensichtbarkeit
- Steuern von Panel\Regional und Sprache Options\Allow Benutzer zum Aktivieren von Online sprach Erkennungs Diensten

Netzwerk

- Network\Windows Connection Manager\Enable Windows to Soft-Trennen eines Computers von einem Netzwerk

Neue Gruppenrichtlinieneinstellungen in Windows10, Version 1803

Die folgenden Gruppenrichtlinieneinstellungen wurden in Windows 10, Version 1803, hinzugefügt:

System

- System\Credentials Delegation\Encryption Oracle-Wiederherstellung
- System\Group Policy\Phone-PC-Link auf diesem Gerät
- System\OS Policies\Allow Upload von Benutzeraktivitäten

Windows-Komponenten

- Windows Components\App Privacy\Let Windows-apps greifen auf ein Eye Tracker-Gerät zu
- Windows Components\Cloud Content\Turn off Windows Spotlight für Einstellungen
- Windows Components\Data-Sammlung und Vorschau Builds\Allow Gerätename, der in Windows-

Diagnosedaten gesendet werden soll

- Windows-Components\Data Sammlung und Vorschau Builds\Configure Telemetrie-Opt-in-Einstellung für Benutzeroberfläche
- Windows-Components\Data Sammlung und Vorschau Builds\Configure Telemetrie-Opt-in-Änderungsbenachrichtigungen
- Windows Components\Delivery Optimization\Maximum Hintergrund Download Bandbreite (Prozentsatz)
- Windows Components\Delivery Optimization\Maximum Foreground Download-Bandbreite (Prozentsatz)
- Windows Components\Delivery Optimization\Select der Quelle von Gruppen-IDs
- Windows Components\Delivery Optimization\Delay background Download from http (in Sekunden)
- Windows Components\Delivery Optimization\Delay Foreground Download from http (in Sekunden)
- Windows Components\Delivery Optimization\Select eine Methode zum Einschränken der Peer Auswahl
- Windows Components\Delivery Optimization\Set Geschäftszeiten, um die Bandbreite des Hintergrund Downloads zu begrenzen
- Windows Components\Delivery Optimization\Set Geschäftszeiten, um die Bandbreite des Vordergrund Downloads zu begrenzen
- Windows Components\IME\Turn auf Live-Aufkleber
- Windows Remotedesktopdienste Desktop-Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Geräte-und Ressourcen Redirection\Do nicht zulassen, dass die Videoaufnahme umgeleitet wird
- Windows Remotedesktopdienste Desktop Vorlagen Remotedesktop-Sitzungshost Desktopsitzung Vorlagen\Windows-Komponenten\Remotedesktopdienste\Remotedesktop-Sitzungshost\Umgebung für Remote Session Environment\Use Hardware-Grafikadapter für alle Remote Desktop Dienste-Sitzungen
- Windows Components\Search\Allow Cortana-Seite in OOBE auf einem Aad-Konto
- Windows Components\Store\Disable alle apps aus dem Microsoft Store
- Windows Components\Text Input\Allow Deinstallieren von sprach Features
- Windows Components\Text Input\Improve Freihand-und Eingabeerkennung
- Windows Vorlagen\Windows-Komponenten\Windows Defender Application Guard\Allow hardwarebeschleunigtes Rendering für Windows Defender Application Guard
- Windows Vorlagen\Windows-Komponenten\Windows Defender Security Center\Account protection\Hide den Kontoschutz Bereich
- Windows Vorlagen\Windows-Komponenten\Windows Defender Security Center\Device security\Hide den Bereich "Gerätesicherheit"
- Windows Vorlagen\Windows-Komponenten\Windows Defender Security Center\Device security\Hide the Security Processor (TPM) Troubleshooter-Seite
- Windows Vorlagen\Windows-Komponenten\Windows Defender Security Center\Device security\Hide den sicheren Startbereich
- Windows Vorlagen\Windows-Komponenten\Windows Defender-Sicherheits Center\Virus und Bedrohungs protection\Hide des Ransomware-Daten Wiederherstellungsbereichs

Neue Gruppenrichtlinieneinstellungen in Windows10, Version 1709

Die folgenden Einstellungen für Gruppenrichtlinien wurden in Windows10, Version 1709, hinzugefügt:

Systemsteuerung

- Systemsteuerung\Online-Tipps zulassen

Netzwerk

- Netzwerk\Netzwerkverbindungs-Statusanzeige\Globale DNS festlegen
- Netzwerk\WWAN-Dienst\WWAN UI-Einstellungen\UI-Sichtbarkeit des Mobilfunkzugriffs pro App festlegen
- Netzwerk\WWAN-Dienst\Datenverbindungszugriff\Zugriff der Windows-Apps auf Datenverbindungen

zulassen

System

- System\Integritätsnachweis für Geräte\Überwachung und Berichterstattung des Integritätsnachweis für Geräte
- System\OS-Richtlinien\Aktivitäts-Feed aktivieren
- System\OS-Richtlinien\Publizieren von Anwenderaktivitäten ermöglichen
- System\Energieverwaltung\Einstellungen der Energieeinschränkung\Energieeinschränkung ausschalten
- System\Speicherintegrität\Updates vom Datenträgerfehlermodell ermöglichen
- System\Trusted Platform Module-Dienste\System konfigurieren, um TPM zu reinigen, wenn es nicht bereit ist.

Windows-Komponenten

- Windows-Komponenten\App-Datenschutz\Windows-Apps mit nicht gekoppelten Geräten kommunizieren lassen
- Windows-Komponenten\Datensammlung und Vorabversionen\Beschränken Sie die erweiterte Diagnosedaten auf die Mindestanforderungen der Windows Analytics
- Windows-Komponenten\Handwriting\Standard-Andockmodus des Schreibbereichs
- Windows-Komponenten\Internet Explorer\Interneteinstellungen\Erweiterte Einstellungen\Durchsuchen\Die Schaltfläche (neben der Schaltfläche „Neue Registerkarte") ausblenden, über die Microsoft Edge geöffnet wird
- Windows-Komponenten\MDM\Automatische MDM-Registrierung mit AAD-Token
- Windows -Komponenten\Nachrichten\Message Service-Synchronisierung mit der Cloud ermöglichen
- Windows-Komponenten\Microsoft Edge\Die Bibliothek in Microsoft Edge immer anzeigen
- Windows-Komponenten\Microsoft Edge\Bereitstellungsfavoriten
- Windows-Komponenten\Microsoft Edge\Änderungen an den Favoriten in Microsoft Edge verhindern
- Windows-Komponenten\Microsoft FIDO-Authentifizierung\Verwendung von FIDO-Geräten zur Anmeldung verwenden
- Windows-Komponenten\OneDrive\OneDrive-Netzwerkverkehr davon abhalten, Netzwerkverkehr zu generieren, bis der Benutzers sich auf OneDrive anmeldet
- Windows-Komponenten\Mit Push installieren\Installationsdienst mit Push deaktivieren
- Windows-Komponenten\Suche\Cloud-Suche ermöglichen
- Windows-Komponenten\Windows Defender Application Guard\Datenpersistenz für Windows Defender Application Guard zulassen
- Windows-Komponenten\Windows Defender Application Guard\Überwachungsereignisse für Windows Defender Application Guard zulassen
- Windows-Komponenten\Windows Defender Antivirus\Windows Defender Exploit Guard\Netzwerkschutz\Benutzern und Apps den Zugriff auf gefährliche Websites verhindern
- Windows-Komponenten\Windows Defender Antivirus\Windows Defender Exploit Guard\Kontrollierter Ordnerzugriff\Kontrollierten Ordnerzugriff konfigurieren
- Windows-Komponenten\Windows Defender Antivirus\Windows Defender Exploit Guard\Attack Surface Reduction\Attack Surface Reduction-Regeln konfigurieren
- Windows-Komponenten\Windows Defender Antivirus\Windows Defender Exploit Guard\Attack Surface Reduction\Dateien und Pfade von Attack Surface Reduction-Regeln ausschließen
- Windows-Komponenten\Windows Defender Antivirus\Windows Defender Exploit Guard\Kontrollierter Ordnerzugriff\Erlaubte Apps konfigurieren
- Windows-Komponenten\Windows Defender Antivirus\Windows Defender Exploit Guard\Kontrollierter Ordnerzugriff\Geschützte Ordner konfigurieren
- Windows-Komponenten\Windows Defender Exploit Guard\Exploit-Schutz\Einen gemeinsamen Satz von Exploit-Schutzeinstellungen verwenden
- Windows-Komponenten\Windows Defender Security Center\Viren- & Bedrohungsschutz\Viren- &

Bedrohungsschutzbereich ausblenden
- Windows-Komponenten\Windows Defender Security Center\Firewall und Netzwerkschutz\Firewall und Netzwerkschutzbereich ausblenden
- Windows-Komponenten\Windows Defender Security Center\App- und Browser-Schutz\App- und Browser-Schutzbereich ausblenden
- Windows-Komponenten\Windows Defender Security Center\App- und Browser-Schutz\Benutzern das Ändern der Einstellungen nicht erlauben
- Windows-Komponenten\Windows Defender Security Center\Geräteleistung und Integrität\Geräteleistung und Integritätsbereich ausblenden
- Windows-Komponenten\Windows Defender Security Center\Familienoptionen\Familienoptionenbereich ausblenden
- Windows-Komponenten\Windows Defender Security Center\Benachrichtigungen\Alle Benachrichtigungen ausblenden
- Windows-Komponenten\Windows Defender Security Center\Benachrichtigungen\Alle nicht kritischen Benachrichtigungen ausblenden
- Windows-Komponenten\Windows Defender Security Center\Enterprise Customization\Benutzerdefinierte Benachrichtigungen ausblenden
- Windows-Komponenten\Windows Defender Security Center\Enterprise Customization\Benutzerdefinierte Kontaktinformationen ausblenden
- Windows-Komponenten\Windows Defender Security Center\Enterprise Customization\Kontaktname des Unternehmens ausblenden
- Windows-Komponenten\Windows Defender Security Center\Enterprise Customization\Kontakttelefonnummer oder Skype-ID ausblenden
- Windows-Komponenten\Windows Defender Security Center\Enterprise Customization\Kontakt-E-Mail-Adresse oder E-Mail-ID ausblenden
- Windows-Komponenten\Windows Defender Security Center\Enterprise Customization\Kontaktwebsite ausblenden
- Windows-Komponenten\Windows Hello for Business\Geräteentsperrungsfaktor konfigurieren
- Windows-Komponenten\Windows Hello for Business\Dynamischen Sperrfaktor konfigurieren
- Windows-Komponenten\Windows Hello for Business\Smartcard-Emulation ausschalten
- Windows-Komponenten\Windows Hello for Business\Aufzählung der emulierten Smartcard für alle Benutzer ermöglichen
- Windows-Komponenten\Windows Update\Herunterladen von Updates automatisch über getaktete Verbindungen ermöglichen
- Windows-Komponenten\Windows Update\Erlauben Sie nicht, das Rückstellungsrichtlinien für Updates in Windows Scans verursachen

Neue Gruppenrichtlinieneinstellungen in Windows10, Version 1703

Die folgenden Einstellungen für Gruppenrichtlinien wurden in Windows10, Version 1703, hinzugefügt:

Systemsteuerung

- Systemsteuerung\Programme hinzufügen oder entfernen\Standardkategorie für " Neue Programme hinzufügen" festlegen
- Systemsteuerung\Programme hinzufügen oder entfernen\Option " Ein Programm von CD oder Diskette hinzufügen" ausblenden
- Systemsteuerung\Personalisierung\Ändern des Bilds für den Sperr- und Anmeldebildschirm verhindern

Netzwerk

- Netzwerk\Intelligenter Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS)\Maximale Netzwerkbandbreite für BITS-Übertragungen im Hintergrund begrenzen
- Netzwerk\Intelligenter Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS)\BITS-Peercaching zulassen
- Netzwerk\Intelligenter Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS)\Alter der Dateien im BITS-Peercache begrenzen
- Netzwerk\Intelligenter Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS)\Größe des BITS-Peercaches beschränken
- Netzwerk\DNS-Client\NetBT-Abfragen nach vollqualifizierten Domänennamen zulassen
- Netzwerk\Netzwerkverbindungen\Zugriff auf Komponenteneigenschaften einer LAN-Verbindung nicht zulassen
- Netzwerk\Netzwerkverbindungen\Aktivieren/Deaktivieren einer LAN-Verbindung zulassen
- Netzwerk\Offlinedateien\Wirtschaftliche Anwendung der vom Administrator zugewiesenen Offlinedateien aktivieren
- Netzwerk\Offlinedateien\Modus für langsame Verbindungen konfigurieren
- Netzwerk\Offlinedateien\Transparentes Zwischenspeichern aktivieren
- Netzwerk\Microsoft Peer-zu-Peer-Netzwerkdienste\Peer Name Resolution-Protokoll\Lokale Siteclouds\Seedserver festlegen
- Netzwerk\Microsoft Peer-zu-Peer-Netzwerkdienste\Überprüfung der Kennwortstärke für Peergruppenfunktion deaktivieren

System

- System\App-V\Streaming\Ortanbieter
- System\App-V\Streaming\Zertifikatfilter für Client-SSL
- System\Delegierung von Anmeldeinformationen\Delegierung von Standardanmeldeinformationen mit reiner NTLM-Serverauthentifizierung zulassen
- System\STRG+ALT+ENTF (Optionen)\Kennwortänderung entfernen
- System\STRG+ALT+ENTF (Optionen)\Sperren des Computers entfernen
- System\STRG+ALT+ENTF (Optionen)\Task-Manager entfernen
- System\STRG+ALT+ENTF (Optionen)\Abmeldung entfernen
- System\Geräteinstallation\Keinen Windows-Fehlerbericht senden, wenn ein Standardtreiber für ein Gerät installiert ist
- System\Geräteinstallation\Verhindern, dass ein Fehlerbericht gesendet wird, wenn ein Gerätetreiber während der Installation zusätzliche Software anfordert
- System\Gebietsschemadienste\Außerkraftsetzungen lokaler Einstellungen durch Benutzer nicht zulassen
- System\Anmeldung\Herkömmliche Ausführungsliste nicht verarbeiten
- System\Anmeldung\Immer benutzerdefinierten Anmeldehintergrund verwenden
- System\Anmeldung\Netzwerkauswahl-UI nicht anzeigen
- System\Anmeldung\Benutzer darf keine Kontodetails auf dem Anmeldebildschirm anzeigen
- (System\Anmeldung\App-Benachrichtigungen auf dem Sperrbildschirm deaktivieren
- System\Benutzerprofile\Zeitüberschreitungswert für Dialogfelder festlegen
- System\Windows-NTP-Server aktivieren\Windows-Zeitdienst\Windows-NTP-Client aktivieren

Windows-Komponenten

- Windows-Komponenten\ActiveX-Installationsdienst\Genehmigte Installationsorte für ActiveX-Steuerelemente
- Windows-Komponenten\ActiveX-Installationsdienst\ActiveX-Installationsrichtlinie für Sites in vertrauenswürdigen Zonen erstellen
- Windows-Komponenten\Anwendungskompatibilität\Anwendungskompatibilitätsmodul deaktivieren

- Windows-Komponenten\Anwendungskompatibilität\Programmkompatibilitäts-Assistenten deaktivieren
- Windows-Komponenten\Anwendungskompatibilität\Problemaufzeichnung deaktivieren
- Windows-Komponenten\Anlagen-Manager\Antivirenprogramme beim Öffnen von Anlagen benachrichtigen
- Windows-Komponenten\Biometrie\Verwendung der Biometrie zulassen
- Windows-Komponenten\NetMeeting\Whiteboard deaktivieren
- Windows-Komponenten\Datensammlung und Vorabversionen\Organisations-ID konfigurieren
- Windows-Komponenten\Datei-Explorer\Menüleiste im Datei-Explorer anzeigen
- Windows-Komponenten\Dateiversionsverlauf\Dateiversionsverlauf deaktivieren
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Seite "Erweitert"\Animationen in Webseiten wiedergeben
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Zone vertrauenswürdiger Sites\Cross-Site Scripting-Filter aktivieren
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Internetzone\Cross-Site Scripting-Filter aktivieren
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Sperrung der Zone des Internets\ActiveX-Steuerelemente und Plug-Ins ausführen
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Sperrung der Zone des Internets\ActiveX-Steuerelemente ausführen, die als "sicher für Skripting" markiert sind
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Intranetzone\ActiveX-Steuerelemente und Plug-Ins ausführen
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Intranetzone\ActiveX-Steuerelemente ausführen, die als "sicher für Skripting" markiert sind
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Sperrung der Zone des Intranets\ActiveX-Steuerelemente und Plug-Ins ausführen
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Sperrung der Zone des Intranets\ActiveX-Steuerelemente ausführen, die als "sicher für Skripting" markiert sind
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Zone des lokalen Computers\ActiveX-Steuerelemente und Plug-Ins ausführen
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Zone des lokalen Computers\ActiveX-Steuerelemente ausführen, die als "sicher für Skripting" markiert sind
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Sperrung für Zone des lokalen Computers\ActiveX-Steuerelemente und Plug-Ins ausführen
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Sperrung für Zone des lokalen Computers\ActiveX-Steuerelemente ausführen, die als "sicher für Skripting" markiert sind
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Zone eingeschränkter Sites\ActiveX-Steuerelemente und Plug-Ins ausführen
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Zone eingeschränkter Sites\ActiveX-Steuerelemente ausführen, die als "sicher für Skripting" markiert sind
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Sperrung der Zone eingeschränkter Sites\ActiveX-Steuerelemente und Plug-Ins ausführen
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Sperrung der Zone eingeschränkter Sites\ActiveX-Steuerelemente ausführen, die als "sicher für Skripting" markiert sind
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Zone vertrauenswürdiger Sites\ActiveX-Steuerelemente und Plug-Ins ausführen
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Zone vertrauenswürdiger Sites\ActiveX-Steuerelemente ausführen, die als "sicher für Skripting" markiert sind
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Sperrung der Zone vertrauenswürdiger Sites\ActiveX-Steuerelemente und Plug-Ins ausführen
- Windows-Komponenten\Internet Explorer\Internetsystemsteuerung\Sicherheitsseite\Sperrung der Zone

vertrauenswürdiger Sites\ActiveX-Steuerelemente ausführen, die als "sicher für Skripting" markiert sind

- Windows-Komponenten\Internet Explorer\Schnellinfos\Schnellinfos auf die über eine Gruppenrichtlinie bereitgestellten Schnellinfos beschränken
- Windows-Komponenten\Internet Explorer\Kompatibilitätsansicht\Internet Explorer 7-Standards-Modus aktivieren
- Windows-Komponenten\Position und Sensoren\Windows-Positionssuche\Windows-Positionssuche deaktivieren
- Windows-Komponenten\Microsoft-Konto\Benutzerauthentifizierung von Microsoft-Konten aller Anwender blockieren
- Windows-Komponenten\Microsoft Edge\AutoAusfüllen konfigurieren
- Windows-Komponenten\Microsoft Edge\Entwicklungstools zulassen
- Windows-Komponenten\Microsoft Edge\DNT konfigurieren
- Windows-Komponenten\Microsoft Edge\InPrivate-Browsen zulassen
- Windows-Komponenten\Microsoft Edge\Kennwort-Manager konfigurieren
- Windows-Komponenten\Microsoft Edge\Popupblocker konfigurieren
- Windows-Komponenten\Microsoft Edge\Anpassung der Suchmaschine zulassen
- Windows-Komponenten\Microsoft Edge\Suchvorschläge in Adressleiste konfigurieren
- Windows-Komponenten\Microsoft Edge\Standardsuchmaschine festlegen
- Windows-Komponenten\Microsoft Edge\Zusätzliche Suchmaschinen konfigurieren
- Windows-Komponenten\Microsoft Edge\Enterprise Mode Site List konfigurieren
- Windows-Komponenten\Microsoft Edge\Verwendung der Localhost IP-Adresse für WebRTC verhindern
- Windows-Komponenten\Microsoft Edge\Startseiten konfigurieren
- Windows-Komponenten\Microsoft Edge\Sperrung von Startseiten deaktivieren
- Windows-Komponenten\Microsoft Edge\Umgehung der Windows Defender SmartScreen-Aufforderungen für Websites verhindern
- Windows-Komponenten\Microsoft Edge\Umgehung der Windows Defender SmartScreen-Aufforderungen für Dateien verhindern
- Windows-Komponenten\Microsoft Management Console\Eingeschränkte/Zugelassene Snap-Ins.Net Framework-Konfiguration
- Windows-Komponenten\Windows Installer\Verwenden des Neustart-Managers nicht zulassen
- Windows-Komponenten\Desktopgadgets\Entpacken und Installieren von nicht digital signierten Gadgets einschränken
- Windows-Komponenten\Desktopgadgets\Vom Benutzer installierte Desktopgadgets deaktivieren
- Windows-Komponenten\OneDrive\Verwendung von OneDrive für die Dateispeicherung verhindern
- Windows-Komponenten\OneDrive\Verwendung von OneDrive für die Dateispeicherung unter Windows 8.1 verhindern
- Windows-Komponenten\OneDrive\Synchronisierung von OneDrive-Dateien über getaktete Verbindungen verhindern
- Windows-Komponenten\OneDrive\Dokumente standardmäßig auf OneDrive speichern
- Windows-Komponenten\Smartcard\Zertifikate ohne Zertifikatattribut für erweiterte Schlüsselnutzung zulassen
- Windows-Komponenten\Smartcard\Zertifikatpropagierung von der Smartcard aktivieren
- Windows-Komponenten\Tablet-PC\Stift-UX-Verhalten\Stiftbewegungen verhindern
- Windows-Komponenten\BitLocker- Laufwerksverschlüsselung\Verschlüsselungsmethode und Verschlüsselungsstärke für Laufwerk auswählen (Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10 [Version 1507])
- Windows-Komponenten\Windows Defender Antivirus\Echtzeitschutz\Aktivieren der Verhaltensüberwachung
- Windows-Komponenten\Windows Defender Antivirus\Signaturaktualisierungen\Definieren der Dateifreigaben für das Herunterladen von Definitionsupdates

- Windows-Komponenten\Windows Defender Antivirus\Signaturaktualisierungen\Aktivieren von automatischen Scans nach Signaturupdates
- Windows-Komponenten\Datei-Explorer\Bestätigungsdialog beim Löschen von Dateien anzeigen
- Windows-Komponenten/Internet Explorer/Internetsystemsteuerung/Sicherheitsseite/Sperrung der Zone eingeschränkter Sites\OpenSearch-Abfragen im Datei-Explorer zulassen
- Windows-Komponenten\Windows Update\Zugriff auf alle Windows Update-Funktionen entfernen
- Windows-Komponenten\Windows Update\Automatische Updates konfigurieren
- Windows-Komponenten\Windows Update\Internen Pfad für den Microsoft Updatedienst angeben
- Windows-Komponenten\Windows Update\Suchhäufigkeit für automatische Updates
- Windows-Komponenten\Windows Update\Nichtadministratoren gestatten, Updatebenachrichtigungen zu erhalten
- Windows-Komponenten\Windows Update\Automatische Updates sofort installieren
- Windows-Komponenten\Windows Update\Empfohlene Updates über automatische Updates aktivieren
- Windows-Komponenten\Optionen für das Herunterfahren\Legacyschnittstelle für das Remoteherunterfahren deaktivieren

Eine Tabelle mit den Gruppenrichtlinieneinstellungen in Windows 10 und Windows Server 2016 finden Sie unter Referenz zu Gruppenrichtlinieneinstellungen für Windows und Windows Server.

Neue MDM-Richtlinien

Die Mobile Device Management (MDM) für Windows10 pro, Windows10 Enterprise, Windows10 Education und Windows10 Mobile umfasst Einstellungen von Windows Phone 8,1 sowie neue oder verbesserte Einstellungen für Windows10, wie beispielsweise:

- Defender (nur Windows10 pro, Windows10 Enterprise und Windows10 Education)
- Erweiterte Bluetooth-Richtlinien
- Passport und Hello
- Geräteupdate
- Nachweis über hardwarebasierte Geräteintegrität
- Kioskmodus, Startseite, Layout des Menüs „Start"
- Sicherheit
- VPN und WLAN-Verwaltung für Unternehmen
- Zertifikatverwaltung
- Windows-Tipps
- Erfahrungen von Verbrauchern, z.B. vorgeschlagene Apps in Start- und App-Kacheln, von Microsoft dynamisch ins standardmäßige Startmenü eingefügt.

Windows10, Version 1703, fügt eine Anzahl von Richtlinien für ADMX-Backup zu MDM hinzu.

Wenn Sie Microsoft InTune für MDM verwenden, können Sie benutzerdefinierte Richtlinien für die Bereitstellung offener Mobile Alliance-Einstellungen für Uniform Resource Identifier (OMA-URI) konfigurieren, die zum Steuern von Features in Windows10 verwendet werden können. Eine Liste der OMA-URI-Einstellungen finden Sie unter Benutzerdefinierte URI-Einstellungen für Windows 10-Geräte.

Keine neuen Exchange ActiveSync-Richtlinien. Weitere Informationen finden Sie in der technischen Referenz zum ActiveSync-Konfigurationsdienstanbieter.

Verwandte Themen

Referenz Kalkulationstabelle für Gruppenrichtlinieneinstellungen in Windows 1803

Verwalten von Unternehmensgeräten

Änderungen der Gruppenrichtlinieneinstellungen für das Menü „Start" in Windows 10

Windows 10 Mobile und MDM

Gruppenrichtlinieneinstellungen, die nur für Windows10 Enterprise und Windows10 Education gelten

01.06.2019 • 2 minutes to read

Betrifft

- Windows 10

Unter Windows 10, Version 1607, gelten die folgenden Gruppenrichtlinieneinstellungen nur für Windows 10 Enterprise und Windows 10 Education.

RICHTLINIENNAME	RICHTLINIENPFAD	KOMMENTARE
Configure Spotlight on lock screen	Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Cloud-Inhalte	Weitere Informationen finden Sie unter Windows-Blickpunkt auf dem Sperrbildschirm. Beachten Sie, dass die zusätzliche Richtlinie für **Cloud-Inhalte** namens **Do not suggest third-party content in Windows spotlight** für Windows 10 Pro gilt.
Features von Windows-Blickpunkt deaktivieren	Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Cloud-Inhalte	Weitere Informationen finden Sie unter Windows-Blickpunkt auf dem Sperrbildschirm.
Turn off Microsoft consumer features	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Cloud-Inhalte	Weitere Informationen finden Sie unter Windows-Blickpunkt auf dem Sperrbildschirm.
Sperrbildschirm nicht anzeigen	Computerkonfiguration > Administrative Vorlagen > Systemsteuerung > Personalisierung	Weitere Informationen finden Sie unter Windows-Blickpunkt auf dem Sperrbildschirm.
Kein STRG+ALT+ENTF erforderlich in Kombination mit **Anwendungsbenachrichtigungen auf gesperrtem Bildschirm deaktivieren**	Computerkonfiguration > Administrative Vorlagen > System > Anmeldung und Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen > Interaktive Anmeldung	Wenn diese beiden Richtlinien aktiviert sind, werden dadurch auch Sperrbildschirm-Apps (zugewiesener Zugriff) nur unter Windows 10 Enterprise und Windows 10 Education deaktiviert. Diese Richtlinieneinstellungen können auf Windows 10 Pro angewendet werden, Sperrbildschirm-Apps werden jedoch unter Windows 10 Pro nicht deaktiviert. **Wichtig:** Die Beschreibung für **Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich** im Gruppenrichtlinien-Editor gibt fälschlicherweise an, dass sie nur für Windows 10 Enterprise und Education gilt. Die Beschreibung wird in einer zukünftigen Version korrigiert.

RICHTLINIENNAME	RICHTLINIENPFAD	KOMMENTARE
Windows-Tipps nicht anzeigen	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Cloud-Inhalte	Weitere Informationen finden Sie unter Windows-Blickpunkt auf dem Sperrbildschirm.
Ein bestimmtes Standardbild für den Sperrbildschirm erzwingen	Computerkonfiguration > Administrative Vorlagen > Systemsteuerung > Personalisierung	Weitere Informationen finden Sie unter Windows-Blickpunkt auf dem Sperrbildschirm.
Startlayout	Benutzerkonfiguration\Administrative Vorlagen\Startmenü und Taskleiste	In Windows10, Version 1703, kann das benutzerdefinierte Start- und Taskleistenlayout auch auf Windows10 Pro angewendet werden. Weitere Informationen finden Sie unter Verwalten der Windows10-Startlayoutoptionen und -Richtlinien
Store-Anwendung deaktivieren	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Store > Turn off the Store application Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Store > Turn off the Store application	Weitere Informationen finden Sie im Knowledge Base-Artikel 3135657.
Nur privaten Store in der Microsoft Store-App anzeigen	Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Store > Only display the private store within the Microsoft Store app Benutzerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Store > Only display the private store within the Microsoft Store app	Weitere Informationen finden Sie unter Verwalten des Zugriffs auf den privaten Store.
Don't search the web or display web results	Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Suche\Don't search the web or display web results	Weitere Informationen finden Sie unter Integration von Cortana in Ihrem Unternehmen.

Verwalten der Einstellungs-App mit Gruppenrichtlinien

06.12.2019 • 2 minutes to read

Gilt für:

- Windows 10, Windows Server 2016

Sie können jetzt die Seiten, die in der Einstellungs-APP angezeigt werden, mithilfe von Gruppenrichtlinien verwalten. Auf diese Weise können Sie bestimmte Seiten von Benutzern ausblenden. Vor Windows 10, Version 1703, können Sie entweder alles in der Einstellungs-APP anzeigen oder vollständig ausblenden. Wenn Sie die Einstellungen der APP-Gruppenrichtlinien unter Windows Server 2016 verwenden möchten, installieren Sie Fix 4457127 oder ein höheres Kumulatives Update.

> **NOTE**
>
> Jeder Server, dessen Zugriff auf die Einstellungs-APP verwaltet werden soll, muss gepatcht werden.

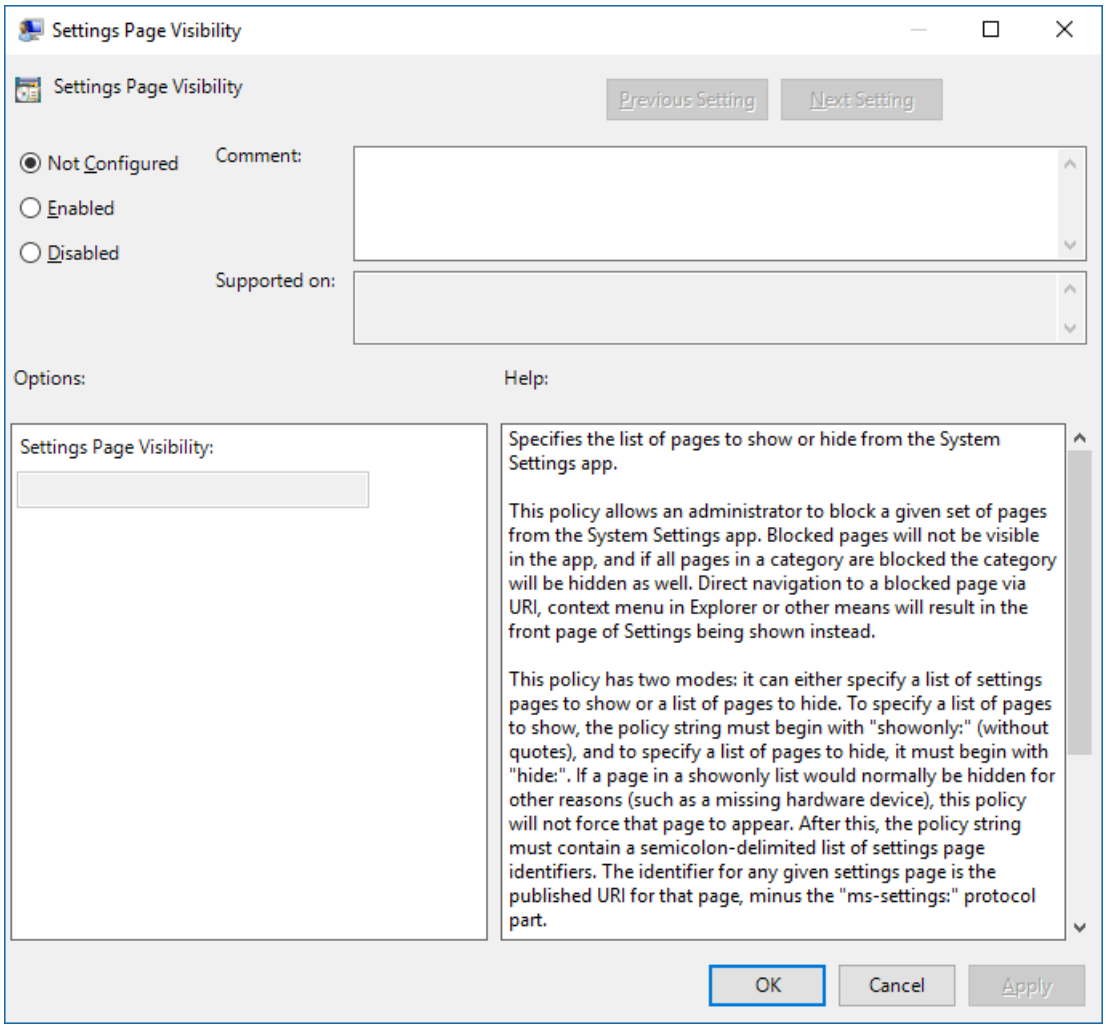
Wenn Sie die neuen Richtlinien zentral verwalten möchten, kopieren Sie die Datei "ControlPanel. ADMX" und "ControlPanel. ADML" in den zentralen Speicher , wenn Ihr Unternehmen einen oder den PolicyDefinitions-Ordner der Domänencontroller verwendet, die für die Gruppenrichtlinienverwaltung verwendet werden.

Diese Richtlinie steht je nach Version des Betriebssystems sowohl für Benutzer als auch für Computer zur Verfügung. Windows Server 2016 mit KB 4457127 wird sowohl für Benutzer-als auch für Computer Richtlinien verwendet. Windows 10, Version 1703, hat eine Computer Richtlinie für die Einstellungs-APP hinzugefügt. Windows 10, Version 1809, hat Benutzerrichtlinien für die Einstellungs-APP hinzugefügt.

Richtlinien Pfade:

**** > **Administrative**Vorlagen > für die Computer Konfiguration, Einstellungen für die**Seitensichtbarkeit**des**Control Panels** > .

Benutzerkonfiguration > -**Administrative Vorlagen** > : Einstellungen für die**Seitensichtbarkeit**des**Control Panels** > .



Konfigurieren der Gruppenrichtlinie

Die Gruppenrichtlinie kann auf eine von zwei Arten konfiguriert werden: Geben Sie eine Liste der Seiten an, die angezeigt werden, oder geben Sie eine Liste der Seiten an, die ausgeblendet werden sollen. Fügen Sie dazu entweder **ShowOnly:** oder **Hide:** gefolgt von einer durch Semikolons getrennten Liste von URIs auf der **Seite "Einstellungen" visiblity**. Eine vollständige Liste der URIs finden Sie im Abschnitt URI-Schemaverweis unter Starten der Windows-Einstellungs-APP.

> **NOTE**
> Wenn Sie den URI im Sichtbarkeits Textfeld der Einstellungsseite angeben, schließen Sie **MS-Settings:** in die Zeichenfolge nicht ein.

Einige Beispiele:

- Wenn Sie nur die Ethernet-und Proxy Seiten anzeigen möchten, setzen Sie das **Sichtbarkeits** Textfeld für die Einstellungen-App auf **ShowOnly: Network-Proxy; Netzwerk-Ethernet**.
- Um die Ethernet-und Proxy Seiten auszublenden, setzen Sie das **Sichtbarkeits** Textfeld für die Einstellungen-App auf **ausblenden: Netzwerk Proxy; Netzwerk-Ethernet**.

Welche Windows-Version wird ausgeführt?

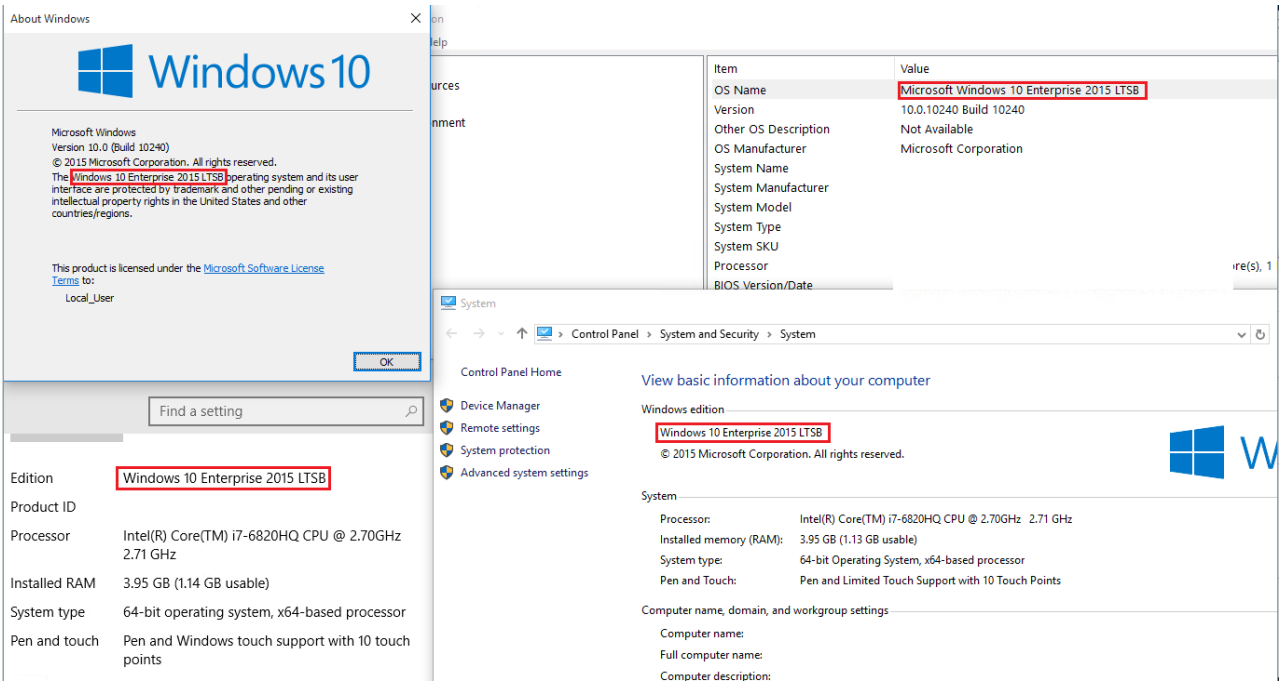
08.08.2019 • 2 minutes to read

Sie müssen wissen, welche Version von Windows 10 Sie ausführen, um festzustellen, ob Ihr Gerät für den lang Zeit Wartungs Kanal (LTSC, vormals LTSB) oder den halbjährlichen Kanal (SAC) registriert ist. Es gibt ein paar Möglichkeiten, dies herauszufinden. Jede Methode bietet einen anderen Satz von Details, daher ist es hilfreich, alle Informationen zu erfahren.

Systemeigenschaften

Klicken Sie auf **Start** > **Settings** > **System** #a0 klicken Sie auf **Info** von unten im Menü auf der linken Seite.

Sie sehen nun die Buildinformationen für **Edition**, **Version**und **Betriebssystem** . Etwas ähnliches:

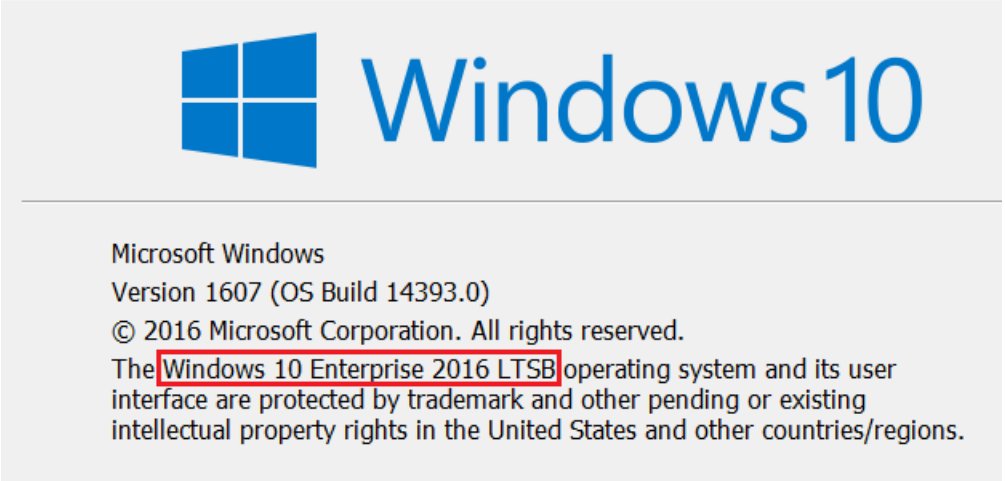


Verwenden der Stichwortsuche

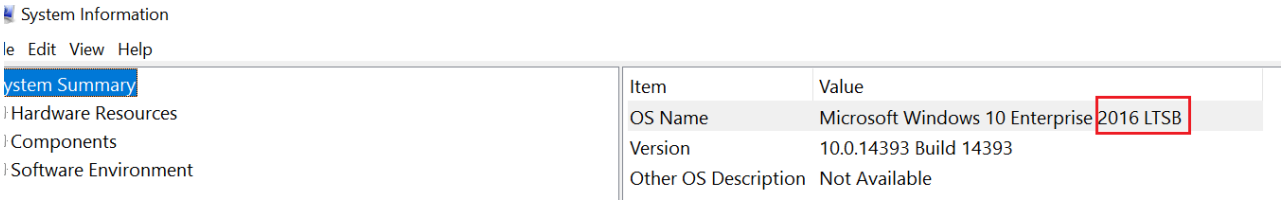
Sie können in der Suchleiste einfach Folgendes eingeben und die **Eingabe** Taste drücken, um die Versionsinformationen für Ihr Gerät anzuzeigen.

winver

About Windows

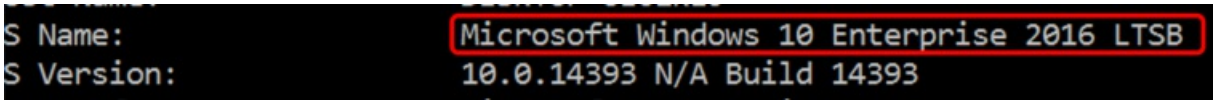


"msinfo" oder **"Msinfo32"** , um die **System Informationen**zu öffnen:



Verwenden der Eingabeaufforderung oder PowerShell

Geben Sie an der Eingabeaufforderung oder PowerShell-Schnittstelle **"System Info | findstr/b/c: "Betriebssystem Name"/b/c: "Betriebssystem Version"** , und drücken Sie dann die **Eingabe** Taste.



Geben Sie an der Eingabeaufforderung oder PowerShell **"slmgr/dlv"** ein, und drücken Sie dann die EINGABETASTE. Der Befehl /dlv zeigt die detaillierten Lizenzierungsinformationen an. Beachten Sie, dass in der Ausgabe "Unternehmen" angezeigt wird, wie in der folgenden Abbildung zu sehen ist:

Was bedeutet das alles?

Der Long-Term Servicing Channel ist nur in der Windows10 Enterprise LTSB-Edition verfügbar. Dieser Windows-Build enthält nicht viele in-Box-Anwendungen wie Microsoft Edge, Microsoft Store, Cortana (Sie verfügen über einige begrenzte Suchfunktionen), Microsoft Mail, Kalender, OneNote, Wetter, Nachrichten, Sport, Geld, Fotos, Kamera, Musik und Uhrzeit. Beachten Sie, dass das LTSC-Modell in erster Linie für spezielle Geräte gilt.

Im halbjährlichen Kanal können Sie Funktionsupdates einrichten, sobald Microsoft Sie freigibt. Dieser Service modal ist ideal für Pilotbereitstellungen und zum Testen von Windows 10-Funktionsupdates sowie für Benutzer wie Entwickler, die mit den neuesten Features sofort arbeiten müssen. Nachdem Sie die neueste Version getestet

haben, können Sie auswählen, wann Sie Sie in Ihrer Bereitstellung weit Ausrollen möchten.

Zurücksetzen von Windows 10 Mobile-Geräten

01.06.2019 • 2 minutes to read

Gilt für

- Windows 10 Mobile

Es gibt zwei Methoden zum Zurücksetzen eines mobilen Windows10-Geräts: Factory Reset und "Wipe and persist" zurücksetzen.

- **Zurück auf Werkseinstellungen** setzt den Zustand des Geräts auf den Zustand beim ersten Start zuzüglich aller Updatepakete zurück. Das Gerät wird nicht auf den ursprünglichen werksseitigen Zustand zurückgesetzt. Um das Gerät auf den ursprünglichen werksseitigen Zustand zurückzusetzen, müssen Sie mithilfe des Windows Device Recovery Tool einen Flash mit dem ursprünglichen werkseitigen Image ausführen. Die gesamte Bereitstellung, die vom Unternehmen auf das Gerät angewendet wurde, geht verloren und muss erneut angewendet werden, wenn erforderlich. Details dazu, was entfernt oder beibehalten wird, finden Sie unter Zurücksetzen mobiler Geräte.
- **Zurücksetzen und beibehalten** behält alle Bereitstellungen bei, die vor dem Zurücksetzen auf das Gerät angewendet wurden. Nach dem Zurücksetzen durch „Zurücksetzen und beibehalten" werden alle beibehaltenen Bereitstellungspakete automatisch auf das Gerät angewendet. Außerdem werden die Daten im freigegebenen Unternehmensspeicherordner „\Data\SharedData\Enterprise\Persistent" in diesem Ordner wiederhergestellt. Weitere Informationen zum freigegebenen Unternehmensspeicherordner finden Sie unter EnterpriseExtFileSystem-CSP.

Sie können die Zurücksetzung mit dem Dienst für die Verwaltung mobiler Geräte (MDM) auslösen. Alternativ kann ein Benutzer die Zurücksetzung in der Benutzeroberfläche oder durch die Verwendung von Hardwaretasten auslösen.

Zurücksetzen mithilfe von MDM

Der Befehl für die Remotezurücksetzung wird als XML-Bereitstellungsdatei an das Gerät gesendet. Da der RemoteWipe-Konfigurationsdienstanbieter (CSP) OMA DM und WAP verwendet, wird die Authentifizierung zwischen Client und Server und die Bereitstellung der XML-Bereitstellungsdatei als Bereitstellung behandelt. Der Befehl für die Remotezurücksetzung wird mittels der Funktion **ResetPhone** auf dem Gerät implementiert. Weitere Informationen zu den Daten, die durch den Befehl für die Remotezurücksetzung entfernt werden, finden Sie unter Zurücksetzen mobiler Geräte.

Verwenden Sie die folgende syncML, um eine Zurücksetzung auf die Werkseinstellungen durchzuführen und das Gerät auf den werksseitigen Zustand zurückzusetzen.

```
<SyncML xmlns="SYNCML:SYNCML1.2">
 <SyncBody>
  <Exec>
   <CmdID>3</CmdID>
   <Item>
    <Target><LocURI>./Vendor/MSFT/RemoteWipe/DoWipe</LocURI></Target>
   </Item>
  </Exec>
  <Final/>
 </SyncBody>
</SyncML>
```

Verwenden Sie die folgende syncML, um eine Zurücksetzung durch „Zurücksetzen und Beibehalten"

durchzuführen, die auf das Gerät vor der Zurücksetzung angewendete Bereitstellungen und lokale Datendateien beibehält.

```
<SyncML xmlns="SYNCML:SYNCML1.2">
    <SyncBody>
        <Exec>
            <CmdID>3</CmdID>
            <Item>
                 <Target><LocURI>./Vendor/MSFT/RemoteWipe/DoWipePersistProvisionedData</LocURI></Target>
            </Item>
        </Exec>
        <Final/>
 </SyncBody>
</SyncML>
```

Zurücksetzen mittels der Benutzeroberfläche

1. Wechseln Sie auf Ihrem mobilen Gerät zu **Einstellungen** > **System** > **zum** > **Zurücksetzen des Telefons** .

2. Wenn Sie auf **Handy zurücksetzen**tippen, wird im Dialogfeld die Option **Auch bereitgestellten Inhalt entfernen** angezeigt, wenn:

   - mindestens ein Bereitstellungspaket angewendet wurde, oder
   - eine Datei im freigegebenen Unternehmensspeicherordner „\Data\SharedData\Enterprise\Persistent“ vorhanden ist.

   Wenn die Option **Auch bereitgestellten Inhalt entfernen** ausgewählt ist, wird die Zurücksetzung als reguläre Zurücksetzung auf die Werkseinstellungen ausgeführt. Wenn die Option nicht aktiviert ist, erfolgt die Zurücksetzung als „Zurücksetzen und Beibehalten“.

Zurücksetzen mittels Hardwaretasten

Wenn Ihr Telefon nicht mehr reagiert und Sie nicht zu **Einstellungen**navigieren können, können Sie das Telefon möglicherweise mithilfe von Hardwaretasten zurücksetzen. Die Zurücksetzung mithilfe von Hardwaretasten ermöglicht Ihnen nicht, bereitgestellte Inhalte beizubehalten. Auf Lumia-Telefonen (und einigen anderen Telefonen) müssen Sie die folgenden Schritte ausführen, um das Telefon zurückzusetzen:

1. Halten Sie die Tasten **Leiser** und **Ein/Aus** gleichzeitig gedrückt, bis Sie eine Vibration spüren (ungefähr 10 bis 15 Sekunden).

2. Wenn Sie die Vibration spüren, lassen Sie die Tasten los und drücken anschließend sofort die Taste **Leiser** . Halten Sie diese Taste gedrückt, bis ein großes Ausrufezeichen angezeigt wird.

3. Wenn das Ausrufezeichen angezeigt wird, drücken Sie die folgenden vier Tasten in dieser Reihenfolge: **Lauter**, **Leiser**, **Ein/Aus**, **Leiser**. Ihr Telefon sollte nun zurückgesetzt und neu gestartet werden. (Die Zurücksetzung kann eine Weile dauern.)

Verwalten von Windows10 in Ihrer Organisation – Übergang zum modernen Management

27.02.2020 • 9 minutes to read

Die Verwendung persönlicher Geräte für die Arbeit sowie Mitarbeiter, die nicht im Büro arbeiten, können die Geräteverwaltung im Unternehmen verändern. Bestimmte Organisationsbereiche sind unter Umständen auf besonders präzise Steuerungsmöglichkeiten für Geräte angewiesen, während in anderen womöglich eine weniger komplexe, szenariobasierte Verwaltung vorzuziehen ist, die besser in ein modernes Arbeitsumfeld passt. Windows10 bietet die Flexibilität, um auf diese sich ändernden Anforderungen zu reagieren, und kann problemlos in einer gemischten Umgebung bereitgestellt werden. Sie können den Prozentsatz von Windows10-Geräten nach und nach erhöhen und sich dabei an die normalen Upgradezeitpläne Ihrer Organisation halten.

Ihre Organisation hat vielleicht die Verwendung von Windows10-Geräten und ein Downgrade auf Windows7 in Erwägung gezogen, bis der formale Upgradeprozess vorbereitet wurde. Durch dieses Vorgehen werden aufgrund der Standardisierung zwar scheinbar Kosten gespart, die Einsparungen sind jedoch höher, wenn Sie das Downgrade vermeiden und direkt von den Kostenminderungen profitieren, die Windows 10 ermöglicht. Da Windows10-Geräte mit den gleichen Prozessen und Technologien wie andere ältere Windows-Versionen verwaltet werden können, ist eine Koexistenz von Versionen ganz einfach.

Ihre Organisation kann verschiedene Betriebssysteme in einer Vielzahl von Gerätetypen unterstützen und diese über einen gemeinsamen Satz von Tools wie Microsoft Endpoint Configuration Manager, Microsoft InTune oder anderen Produkten von Drittanbietern verwalten. Dank dieser „kontrollierten Vielfalt" profitieren Ihre Benutzer von den Produktivitätsoptimierungen ihrer neuen Windows 10-Geräte (einschließlich umfassender Unterstützung von Touch- und Freihandeingabe), ohne dass Sie dafür Kompromisse bei der Sicherheit und Verwaltbarkeit eingehen müssten. So können Sie und Ihre Organisation noch schneller von Windows10 profitieren.

Dieses sechsminütige Video zeigt, wie Benutzer ein neues Mobilgerät mitbringen, ihre personalisierten Einstellungen verwenden und in wenigen Minuten in einer verwalteten Umgebung arbeiten können, ohne sich ins Firmennetz integrieren zu müssen. Außerdem wird veranschaulicht, wie IT-Administratoren durch Richtlinien und Konfigurationen sicherstellen können, dass die Geräte regelkonform verwendet werden.

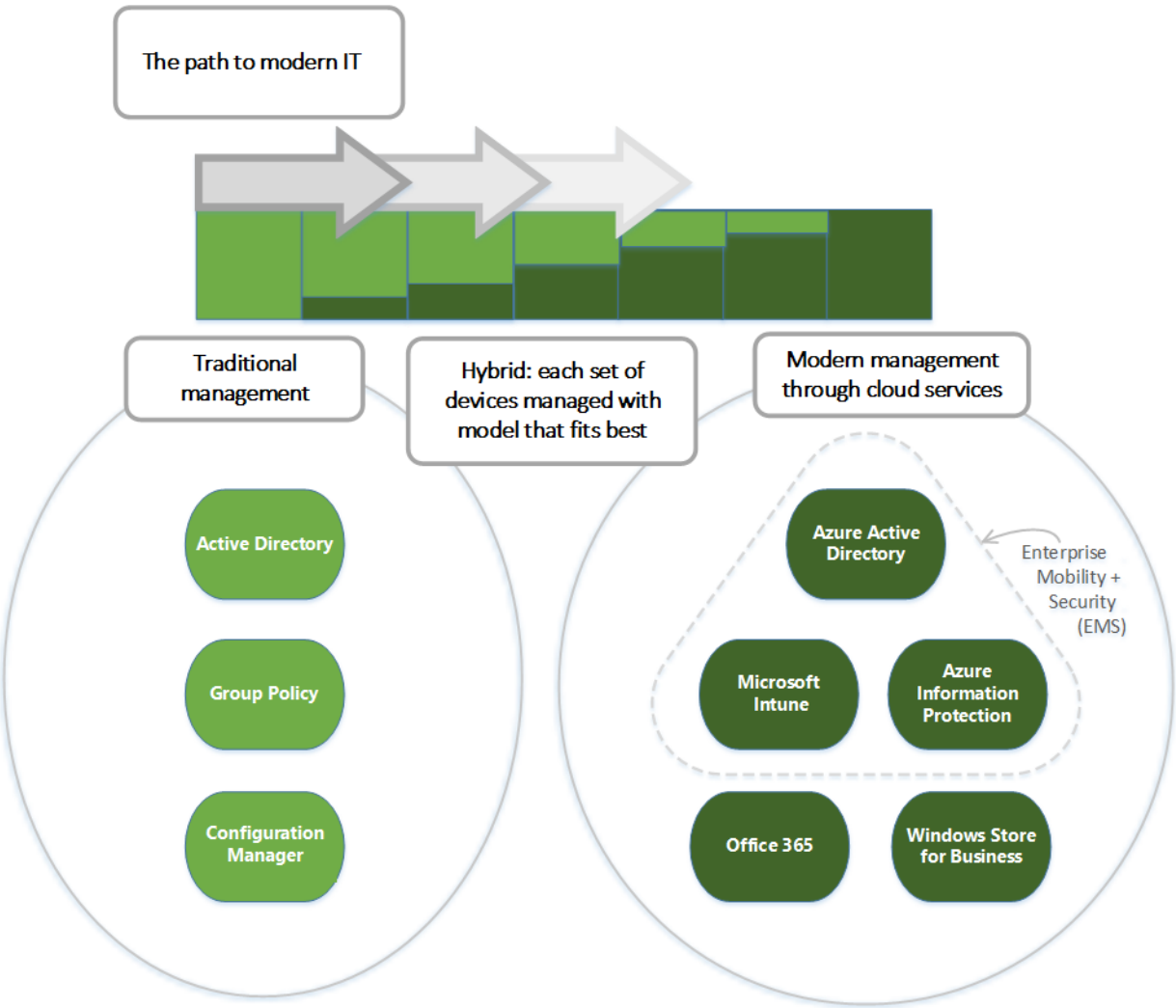
> **NOTE**
>
> In diesem Video wird der Konfigurationsvorgang mithilfe des klassischen Azure-Portals veranschaulicht, das im Ruhestand ist. Kunden sollten das neue Azure-Portal verwenden. Hier erfahren Sie, wie mithilfe des neuen Azure-Portals Aufgaben ausführen, die Sie vorher im klassischen Azure-Portal ausgeführt haben.

Dieses Thema enthält Anleitungen für Strategien zur Bereitstellung und Verwaltung von Windows10, einschließlich der Bereitstellung von Windows10 in einer gemischten Umgebung. In diesem Thema werden Verwaltungsoptionen sowie die vier Phasen des Gerätelebenszyklus behandelt:

- Bereitstellung
- Identität und Authentifizierung
- Konfiguration
- Aktualisierung und Wartung

Überprüfen der Verwaltungsoptionen in Windows10

Windows10 bietet eine Reihe von Verwaltungsoptionen, wie im folgenden Diagramm dargestellt:



Wie im Diagramm angegeben, bietet Microsoft weiterhin Unterstützung für tiefe Verwaltbarkeit und Sicherheit durch Technologien wie Gruppenrichtlinien, Active Directory und Microsoft Configuration Manager. Microsoft verfolgt darüber hinaus einen Ansatz zur einfacheren modernen Verwaltung, bei dem Mobilgeräte und Clouddienste immer mehr an Bedeutung gewinnen. In diesem Rahmen werden cloudbasierte Geräteverwaltungslösungen wie Microsoft Enterprise Mobility + Security (EMS) verwendet. Künftige Windows-Innovationen, die über Windows as a Service bereitgestellt werden, werden durch Clouddienste wie Microsoft Intune, Azure Active Directory, Azure Information Protection, Office 365 und den Microsoft Store für Unternehmen ergänzt.

Bereitstellung

Windows10 kann zwar weiterhin auf herkömmliche Weise bereitgestellt werden, bietet aber auch ein sofort einsatzbereites Verwaltungsmodell. Halten Sie sich an folgende Punkte, um aus neuen Geräten vollständig konfigurierte und verwaltete Geräte zu machen:

- Vermeiden Sie das reimaging mithilfe der dynamischen Bereitstellung, die von einem cloudbasierten Geräte Verwaltungsdienst wie Microsoft Autopilot oder Microsoft InTuneaktiviert ist.
- Erstellen Sie eigenständige Bereitstellungspakete, die mit dem Windows-Designer für die Imageerstellung und -konfiguration (Windows Imaging and Configuration Designer, ICD) erstellt werden.
- Verwenden Sie herkömmliche Bildgebungstechniken wie das Bereitstellen von benutzerdefinierten Bildern mithilfe von Microsoft Endpoint Configuration Manager.

Ihnen stehen mehrere Optionen für das Upgrade auf Windows 10 zur Verfügung. Bei vorhandenen Geräten mit Windows7 oder Windows8.1 können Sie den vorhandenen stabilen Upgradeprozess zur schnellen und zuverlässigen Migration zu Windows10 nutzen und dabei alle vorhandenen Apps, Daten und Einstellungen automatisch beibehalten. Dies kann deutlich niedrigere Bereitstellungskosten und eine höhere Produktivität bedeuten, da Endbenutzer umgehend produktiv arbeiten können – alle Elemente befinden sich an der gleichen Stelle wie zuvor. Selbstverständlich können Sie auch die herkömmliche Wipe-and-Load-Methode verwenden und dabei die gleichen Tools nutzen wie derzeit unter Windows7.

Identität und Authentifizierung

Windows10 und Dienste wie Azure Active Directory bieten neue Möglichkeiten für cloudbasierte Identität, Authentifizierung und Verwaltung. Sie können Benutzern erlauben, **ihr eigenes Gerät mitzubringen (Bring Your Own Device, BYOD)** oder **ein eigenes Gerät auszuwählen (Choose Your Own Device, CYOD)**. Für Letzteres können Sie eine Auswahl zur Verfügung stellen, aus der Benutzer wählen können. Gleichzeitig kümmern Sie sich möglicherweise um die Verwaltung von PCs und Tablets, die aufgrund von bestimmten Anwendungen oder Ressourcen, die darauf verwendet werden, in die Domäne eingebunden sein müssen.

Benutzer- und Geräteverwaltung können etwa in die folgenden zwei Kategorien unterteilt werden:

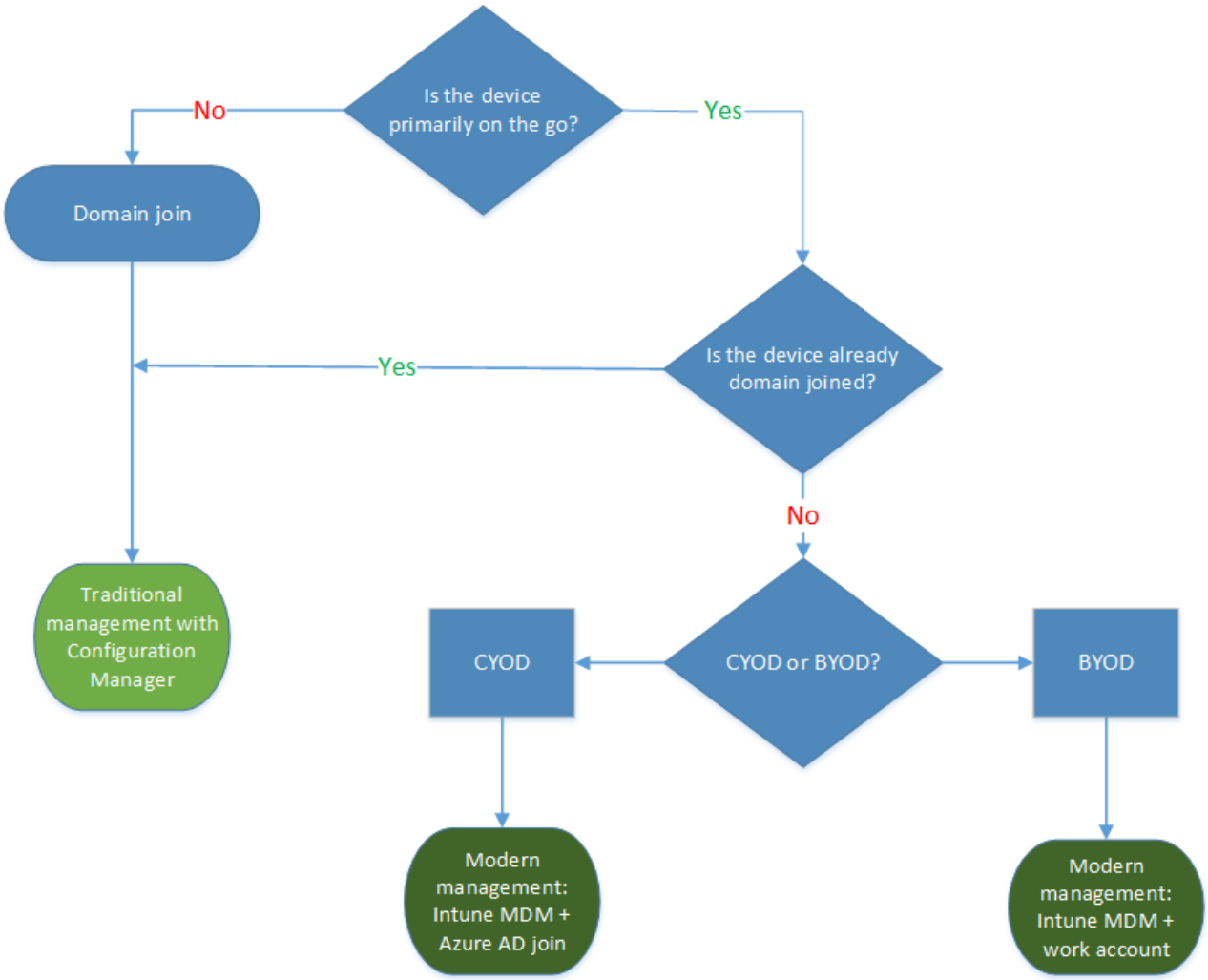
- **Unternehmensgeräte (CYOD) oder persönliche Geräte (BYOD), die von mobilen Benutzern für SaaS-Apps wie Office365 verwendet werden.** Unter Windows 10 können Ihre Mitarbeiter ihre Geräte selbst bereitstellen:
  - Bei Unternehmensgeräten können sie den Unternehmenszugriff mit Azure AD Join einrichten. Wenn Sie den Mitarbeitern Azure AD Join mit der automatischen Intune-MDM-Registrierung anbieten, können sie direkt in der Cloud *in nur einem Schritt* die Verwaltung ihrer Geräte durch das Unternehmen einrichten.
    Azure AD Join ist zudem eine hervorragende Lösung für Aushilfspersonal, vorübergehende Partner oder andere Teilzeitmitarbeiter. Ihre Konten können getrennt von der lokalen AD-Domäne gehalten werden, sie können aber dennoch auf erforderliche Unternehmensressourcen zugreifen.
  - Darüber hinaus können Mitarbeiter für persönliche Geräte die neue, vereinfachte BYOD-Umgebung nutzen, um ihr Geschäftskonto zu Windows hinzuzufügen und anschließend über das Gerät auf Arbeitsressourcen zuzugreifen.
- **In die Domäne eingebundene PCs und Tablets, die für herkömmliche Anwendungen und den Zugriff auf wichtige Ressourcen verwendet werden.** Dabei kann es sich um herkömmliche Anwendungen und Ressourcen, für die die Authentifizierung erforderlich ist, und um den Zugriff auf hochsensible oder vertrauliche lokale Ressourcen handeln. Unter Windows10 verfügen Sie über eine lokale Active Directory-Domäne, die in Azure AD integriert ist. Wenn Mitarbeitergeräte hinzugefügt werden, werden sie automatisch bei Azure AD registriert. Dies ermöglicht Folgendes:
  - Ortsunabhängiges einmaliges Anmelden bei cloudbasierten und lokalen Ressourcen
  - Unternehmens-Roaming von Einstellungen
  - Bedingter Zugriff auf Unternehmensressourcen basierend auf der Integrität oder Konfiguration des Geräts
  - Windows Hello for Business
  - Windows Hello

  Mit dem Configuration Manager- Client oder der Gruppenrichtlinie können auch weiterhin Domänen verbundene PCs und Tablets verwaltet werden.

Weitere Informationen dazu, wie Windows10 und AzureAD den Zugriff auf Arbeitsressourcen bei verschiedenen

Geräten und Szenarien optimieren, finden Sie unter Verwenden von Windows10-Geräten an Ihrem Arbeitsplatz.

Bei der Überprüfung der Rollen in Ihrer Organisation können Sie mithilfe des folgenden generalisierten Entscheidungsbaums Benutzer oder Geräte ermitteln, die in die Domäne eingebunden werden müssen. Ziehen Sie die Migration der verbleibenden Benutzer zu Azure AD in Betracht.



Einstellungen und Konfiguration

Ihre Konfigurationsanforderungen werden durch mehrere Faktoren bestimmt. Zu diesen zählen u.a. die erforderliche Verwaltungsstufe, die verwalteten Geräte und Daten und Ihre Branchenanforderungen. Mitarbeiter sind häufig beunruhigt, dass die IT-Abteilung strikte Richtlinien auf ihre persönlichen Geräte anwendet, möchten aber dennoch Zugriff auf Unternehmens-E-Mails und -Dokumente. Dank Windows10 können Sie einen einheitlichen Satz von Konfigurationen auf PCs, Tablets und Telefone über die allgemeine MDM-Ebene erstellen.

MDM: Mit MDM verfügen Sie über eine Möglichkeit, Einstellungen zu konfigurieren, mit denen Sie Ihre Verwaltungsaufgaben ausführen können, ohne jede mögliche Einstellung verfügbar zu machen. (Im Gegensatz dazu machen die Gruppenrichtlinien differenzierte Einstellungen verfügbar, die Sie einzeln steuern.) Ein Vorteil von MDM besteht darin, dass Sie über einfachere und effizientere Tools allgemeinere Einstellungen für Datenschutz-, Sicherheits- und Anwendungsverwaltung anwenden können. MDM ermöglicht Ihnen auch das Ziel, mit dem Internet verbundene Geräte für die Verwaltung von Richtlinien zu verwenden, ohne GP zu verwenden, das lokale Domänen verbundene Geräte erfordert. Daher ist MDM die beste Wahl für Geräte, die ständig unterwegs verwendet werden.

Gruppenrichtlinie und **Microsoft Endpoint Configuration Manager**: Ihre Organisation muss möglicherweise weiterhin Domänen verbundene Computer auf einer granularen Ebene wie die konfigurierbaren 1.500-Gruppenrichtlinieneinstellungen von Internet Explorer verwalten. In diesem Fall sind Gruppenrichtlinien und Configuration Manager weiterhin hervorragende Verwaltungsoptionen:

- Gruppenrichtlinien eignen sich optimal dazu, mit Windows-basierten Tools in die Domäne eingebundene Windows-PCs und -Tablets genauer zu konfigurieren, die mit dem Unternehmensnetzwerk verbunden sind. Microsoft fügt mit jeder neuen Version von Windows Gruppenrichtlinieneinstellungen hinzu.
- Configuration Manager bleibt die empfohlene Lösung für Konfigurationen mit höherer Granularität für eine stabile Softwarebereitstellung, für Windows-Updates und Betriebssystembereitstellungen.

Aktualisierung und Wartung

Mit Windows as a Service muss Ihre IT-Abteilung nicht mehr bei jeder neuen Windows-Version komplexe Imageerstellungsprozesse (Wipe and Load) ausführen. Bei Current Branch (CB) oder Current Branch for Business (CBB) erhalten Geräte die aktuellen Feature- und Qualitätsupdates über einfache (meist automatische) Patchvorgänge. Weitere Informationen finden Sie unter Szenarien für die Bereitstellung von Windows 10.

MDM mit Intune stellt Tools für die Anwendung von Windows-Updates auf Clientcomputern in Ihrer Organisation bereit. ConfigurationManager ermöglicht umfangreiche Verwaltungs-und Nachverfolgungsfunktionen dieser Updates, einschließlich Wartungsfenstern und automatischen Bereitstellungsregeln.

Nächste Schritte

Es gibt eine Vielzahl von Schritten, mit denen Sie die Modernisierung der Geräteverwaltung in Ihrer Organisation anstoßen können:

Bewerten Sie die derzeitigen Verwaltungsverfahren, und suchen Sie nach Investitionen, die Sie heute vornehmen können. Welche aktuellen Verfahren müssen gleich bleiben, welche können geändert werden? Genauer gesagt: Welche Elemente der herkömmlichen Verwaltung müssen Sie beibehalten, und in welchen Bereichen können Sie Modernisierungen vornehmen? Unabhängig davon, ob Sie die benutzerdefinierte Imageerstellung minimal halten, die Einstellungsverwaltung neu auswerten oder Authentifizierung und Compliance überdenken – die Vorteile spüren Sie unter Umständen sofort. Sie können das MDM-Migrationsanalyse Tool (FMAT) verwenden, um zu ermitteln, welche Gruppenrichtlinien für einen Zielbenutzer/-Computer festgelegt sind, und Sie mit der Liste der verfügbaren MDM-Richtlinien zu Querverweisen.

Bewerten Sie die verschiedenen Anwendungsfälle und Verwaltungsanforderungen in Ihrer Umgebung. Gibt es Gerätegruppen, die von einer schlankeren und einfacheren Verwaltung profitieren könnten? BYOD-Geräte sind beispielsweise prädestiniert für die cloudbasierte Verwaltung. Benutzer oder Geräte, die stärker regulierte Daten verarbeiten, benötigen unter Umständen eine lokale Active Directory-Domäne für die Authentifizierung. Dank Configuration Manager und EMS können Sie moderne Verwaltungsszenarien phasenweise implementieren. Dabei können Sie verschiedene Geräte auf genau die Weise einbinden, die am besten zu den Anforderungen Ihres Unternehmens passt.

Sehen Sie sich die Entscheidungsbäume in diesem Artikel an. Dank der verschiedenen Optionen in Windows10, Configuration Manager und Enterprise Mobility + Security können Sie Imageerstellung, Authentifizierung, Einstellungen und Verwaltungstools für alle Szenarien verwalten.

Gehen Sie in kleinen Schritten vor. Sie müssen nicht über Nacht auf moderne Geräteverwaltung umstellen. Neue Betriebssysteme und Geräte können zusätzlich zu älteren Systemen und Geräten verwendet werden. Dank dieser „kontrollierten Vielfalt" profitieren Ihre Benutzer von den Produktivitätsoptimierungen neuer Windows 10-Geräte, während Sie weiterhin ältere Geräte gemäß Ihren Anforderungen an Sicherheit und Verwaltbarkeit verwalten. Ab Windows 10, Version 1803, wurde die neue Richtlinie MDMWinsOverGP hinzugefügt, damit MDM-Richtlinien Vorrang vor GP haben, wenn sowohl GP als auch die entsprechenden MDM-Richtlinien auf dem Gerät eingestellt sind. Sie können mit der Implementierung von MDM-Richtlinien beginnen, während Sie Ihre GP-Umgebung beibehalten. Hier finden Sie eine Liste der MDM-Richtlinien mit äquivalenten GP- Richtlinien, die von GP unterstützt werden .

Optimieren Sie vorhandene Investitionen. Nutzen Sie bei der Umstellung von der herkömmlichen lokalen

Verwaltung auf eine moderne cloudbasierte Verwaltung die flexible Hybridarchitektur von Configuration Manager und Intune. Ab Configuration Manager 1710 können Sie mit der gemeinsamen Verwaltung Windows 10-Geräte gleichzeitig mithilfe von Configuration Manager und InTune verwalten. Weitere Informationen finden Sie in den folgenden Themen:

- Gemeinsames Management für Windows 10-Geräte
- Vorbereiten von Windows 10-Geräten für die gemeinsame Verwaltung
- Wechseln der Arbeitsauslastung von Configuration Manager auf InTune
- Dashboard für die gemeinsame Verwaltung in Configuration Manager

Verwandte Themen

- Was ist InTune?
- Windows 10-Richtlinien-CSP
- Windows 10-Konfigurationsdienst Anbieter

Bereitstellungs- und Verwaltungshandbuch für Windows10 Mobile

01.02.2020 • 67 minutes to read

Betrifft:

- Windows10 Mobile, Version 1511 und Windows 10 Mobile, Version 1607

Dieses Handbuch unterstützt IT-Experten beim Planen und Bereitstellen von Windows10 Mobile-Geräten.

Mitarbeiter verlassen sich bei ihren täglichen Arbeitsaufgaben zunehmend auf Smartphones. Allerdings stellen diese Geräte eine besondere Herausforderung hinsichtlich Verwaltung und Sicherheit dar. Ob es darum geht, unternehmenseigene Geräte bereitzustellen oder Mitarbeitern die Nutzung eigener Geräte zu gewähren – die IT muss schnell mobile Geräte und Apps bereitstellen und verwalten, um die Geschäftsziele zu erreichen. Außerdem muss sichergestellt sein, dass die Apps und Daten auf diesen mobilen Geräten vor Internetkriminalität und Verlust geschützt sind. Windows10 Mobile unterstützt Organisationen mit stabilen, flexiblen und integrierten Technologien zur Verwaltung mobiler Geräte und Apps bei der Bewältigung dieser Herausforderungen. Windows10 unterstützt eine End-to-End-Lebenszyklusverwaltung für Geräte. Dadurch haben Unternehmen die Kontrolle über ihre Geräte, Daten und Apps. Mithilfe einer umfassenden Verwaltungslösung für Mobilgeräte können die Geräte problemlos in die Standardmethoden für Lebenszyklen integriert werden – von der Registrierung, Konfiguration und Anwendungsverwaltung über Wartung und Überwachung bis hin zur Ausmusterung.

Inhalt dieses Artikels

- Bereitstellen
- Konfigurieren
- Apps
- Verwalten
- Ausmustern

Bereitstellen

Windows10 Mobile verfügt über einen integrierten Geräteverwaltungsclient zur Bereitstellung, Konfiguration, Verwaltung und Unterstützung von Smartphones. Dieser Client ist in allen Editionen des Windows10-Betriebssystems enthalten, einschließlich Desktop, Mobile und Internet der Dinge (IoT). Er bietet eine zentrale Benutzeroberfläche zur Verwaltung sämtlicher Windows10-Geräte mithilfe der Lösungen der mobilen Geräteverwaltung (MDM). Da der MDM-Client in die Identitätsverwaltung integriert ist, wird der Aufwand zum Verwalten von Geräten während des Lebenszyklus erheblich reduziert. Windows 10 enthält umfassende MDM-Funktionen, die von Microsoft-Verwaltungslösungen wie Microsoft InTune oder Microsoft Endpoint Configuration Manager sowie zahlreiche MDM-Lösungen von Drittanbietern verwaltet werden können. Es ist nicht erforderlich, eine zusätzliche, benutzerdefinierte MDM-App zu installieren, um Geräte zu registrieren und diese unter MDM-Kontrolle zu bringen. Alle MDM-Systemanbieter verfügen über gleichberechtigten Zugriff auf die Geräteverwaltungs-APIs (Application Programming Interfaces) von Windows10 Mobile. Dadurch können IT-Organisationen selbst das System wählen, das am ehesten zu ihren Verwaltungsanforderungen passt, ob Microsoft Intune oder ein MDM-Produkt eines Drittanbieters. Weitere Informationen zu den Geräteverwaltungs-APIs von Windows 10 Mobile finden Sie unter mobile Geräteverwaltung.

Bereitstellungsszenarien

Gilt für: unternehmenseigene und persönliche Geräte

Der integrierte MDM-Client ist für alle Editionen des Windows10-Betriebssystems üblich, einschließlich Desktop, Handy und Internet der Dinge (viel). Der Client bietet eine einzige Schnittstelle, über die Sie jedes Gerät verwalten können, das Windows10 ausführt. Der Client hat zwei wichtige Funktionen: Geräteregistrierung bei einem MDM System und Geräteverwaltung.

Organisationen müssen bei der Bereitstellung von Geräten in der Regel zwei Szenarien berücksichtigen: Bring Your Own Device (BYOD), also das Mitbringen eigener Geräte, und das Auswählen unternehmenseigener Geräte (Choose Your Own Device, CYOD). In beiden Fällen muss das Gerät in einem MDM-System registriert werden, in dem es dann mit den entsprechenden Einstellungen für die jeweilige Organisation und den jeweiligen Mitarbeiter konfiguriert wird. Mit den Geräteverwaltungsfunktionen von Windows10 Mobile werden sowohl persönliche Geräte in BYOD-Szenarien als auch unternehmenseigene Geräte in CYOD-Szenarien unterstützt. Das Betriebssystem bietet einen flexiblen Ansatz für die Registrierung von Geräten bei Verzeichnisdiensten und MDM-Systemen. IT-Organisationen können umfassende Gerätekonfigurationsprofile basierend auf ihren geschäftlichen Anforderungen bereitstellen, um mobile Geschäftsdaten zu verwalten und zu schützen. Apps können problemlos auf persönlichen oder unternehmenseigenen Geräten bereitgestellt werden, entweder über den Microsoft Store für Unternehmen oder über ein unternehmenseigenes MDM-System, das hinsichtlich öffentlicher Apps mit dem Microsoft Store für Unternehmen zusammenarbeiten kann. Bei Auswahl der Verwaltungsstrategie und der Kontrollen, die Ihre Organisation anwenden sollte, ist es wichtig zu wissen, wem das Gerät gehört und wofür der Mitarbeiter es verwendet. Bereitstellungsprozesse und Konfigurationsrichtlinien können je nach dem variieren, ob persönliche Geräte, unternehmenseigene Geräte oder Kombinationen aus den beiden bereitgestellt werden sollen.

Bei **persönlichen Geräten** müssen Unternehmen in der Lage sein, unternehmenseigene zum Apps und Daten auf dem Gerät zu verwalten, ohne die Möglichkeiten zur Personalisierung des Geräts nach den individuellen Anforderungen des Mitarbeiters zu beeinträchtigen. Das Gerät gehört dem Mitarbeiter, und dank Unternehmensrichtlinien kann er es für geschäftliche und private Zwecke nutzen. Eigene Apps kann er nach Belieben hinzufügen. Die größte Herausforderung bei persönlichen Geräten besteht darin, wie Organisationen die Offenlegung von Unternehmensdaten verhindern können, während persönliche Daten weiterhin privat und unter der alleinigen Kontrolle des Mitarbeiters bleiben. Dazu muss das Gerät in der Lage sein, eine Trennung von Apps und Daten durch eine strikte Kontrolle des geschäftlichen und persönlichen Datenverkehrs zu unterstützen.

Bei **unternehmenseigenen Geräten** erhalten Organisationen deutlich mehr Kontrolle. Die IT kann eine ausgewählte Liste unterstützter Gerätemodelle an Mitarbeiter ausgeben oder Geräte direkt erwerben und vorkonfigurieren. Da sich die Geräte im Besitz des Unternehmens befinden, kann beschränkt werden, inwieweit Mitarbeiter diese Geräte personalisieren können. Bedenken hinsichtlich Sicherheit und Datenschutz können leichter berücksichtigt werden, da das Gerät vollständig der bestehenden Unternehmensrichtlinie unterliegt.

Geräteregistrierung

Gilt für: unternehmenseigene und persönliche Geräte

Bei der Registrierung von persönlichen und unternehmenseigenen Geräten bei MDM-Systemen werden unterschiedliche Methoden verwendet. Das verantwortliche Team sollte diese Unterschiede bei der Entscheidung, welcher Ansatz für mobile Mitarbeiter in Ihrer Organisation am besten geeignet ist, berücksichtigen.

Überlegungen zur Initialisierung und Registrierung von Geräten

	Persönliche Geräte	Unternehmensgeräte
Besitz	Mitarbeiter	Organisation

Geräteinitialisierung Auf der Windows-Willkommensseite wird der Mitarbeiter beim ersten Start des Geräts aufgefordert, dem Gerät eine Cloud-Identität hinzuzufügen.	Die Hauptidentität auf dem Gerät ist persönliche Identität. Persönliche Geräte werden mit einem Microsoft-Konto (MSA) unter Verwendung einer persönlichen E-Mail-Adresse initiiert.	Die Hauptidentität auf dem Gerät ist eine Organisationsidentität. Unternehmenseigene Geräte werden mit einem Organisationskonto (konto@unternehmensdomäne.erw) initialisiert. Die Initialisierung eines Geräts mit einem Unternehmenskonto ist einzigartig in Windows10. Keine andere mobile Plattform bietet derzeit diese Funktion. Die Standardoption ist die Verwendung einer Azure Active Directory-Organisationsidentität. Beim Überspringen der Kontoeinrichtung in OOBE wird ein lokales Konto erstellt. Die einzige Möglichkeit zum späteren Hinzufügen eines Cloudkontos besteht darin, ein Microsoft-Konto hinzuzufügen, sodass dieses Gerät in einem Bereitstellungsszenario für persönliche Geräte verwendet wird. Andernfalls muss das Gerät zurückgesetzt werden.
Geräteregistrierung Durch das Registrieren von Geräten in einem MDM-System können Unternehmensdaten gesteuert und geschützt werden, während Mitarbeiter weiterhin produktiv arbeiten können.	Die Geräteregistrierung kann vom Mitarbeiter initiiert werden. Dieser kann dem Windows10 Mobile-Gerät ein Azure-Konto als sekundäres Konto hinzufügen. Für den Fall, dass das MDM-System bei Ihrem AzureAD registriert ist, wird das Gerät automatisch im MDM-System registriert, sobald der Benutzer ein Azure AD-Konto als sekundäres Konto hinzufügt (MSA + AAD + MDM). Wenn in Ihrer Organisation kein AzureAD vorhanden ist, wird das Gerät des Mitarbeiters automatisch im MDM-System Ihrer Organisation registriert (MSA + MDM). Die MDM-Registrierung kann auch mit einem Bereitstellungspaket initiiert werden. Dank dieser Option kann die IT eine benutzerfreundliche Self-Service-Registrierung persönlicher Geräte anbieten. Die Bereitstellung wird momentan nur für die reine MDM-Registrierung (MSA + MDM) unterstützt.	Der Benutzer initiiert die MDM-Registrierung, indem er das Gerät der Azure AD-Instanz seiner Organisation hinzufügt. Das Gerät wird automatisch im MDM-System registriert, sobald das Gerät im AzureAD registriert wird. Dazu muss das MDM-System bei Ihrem AzureAD registriert sein (AAD + MDM).

Empfehlung: Microsoft empfiehlt die AzureAD-Registrierung und automatische MDM-Registrierung für unternehmenseigene Geräte (AAD+MDM) und persönliche Geräte (MSA+AAD+MDM). Dazu ist Azure AD Premium erforderlich.

Identitätsverwaltung

Gilt für: unternehmenseigene und persönliche Geräte

Mitarbeiter können ein Gerät nur mit einem einzigen Konto initialisieren. Daher muss Ihre Organisation unbedingt steuern, welches Konto zuerst aktiviert wird. Die Wahl des Kontos bestimmt, wer das Gerät kontrolliert und welche Verwaltungsfunktionen Ihnen zur Verfügung stehen.

> **Hinweis:** Warum muss der Benutzer dem Gerät auf der Windows-Willkommensseite ein Konto hinzufügen?

> Windows10 Mobile-Geräte werden nur von einem einzigen Benutzer verwendet. Die Benutzerkonten bieten Zugriff auf eine Vielzahl von Standard-Cloud-Diensten, die die Produktivität und den Komfort des Smartphones für den Benutzer erhöhen. Zu den Diensten zählen unter anderem Store zum Herunterladen von Apps, Groove für Musik und Unterhaltung und Xbox für Spiele. Sowohl ein MSA- als auch ein Azure AD-Konto bieten Zugriff auf diese Dienste.

In der folgenden Tabelle wird die Auswirkung der Identitätsauswahl auf die Geräteverwaltungseigenschaften in Szenarien mit persönlichen und unternehmenseigenen Geräten erläutert.

Überlegungen zur Identitätsauswahl bei der Geräteverwaltung

	Persönliche Identität	**Unternehmensidentität**
Erstes Konto auf dem Gerät	Microsoft-Konto	Azure AD-Konto
Benutzerfreundlichkeit der Registrierung	Mitarbeiter verwenden ihr Microsoft-Konto zum Aktivieren des Geräts. Anschließend registrieren sie ihr Gerät mithilfe ihres Azure AD-Kontos (Identität der Organisation) bei Azure AD und registrieren das Gerät außerdem bei der MDM-Lösung des Unternehmens (MSA+AAD+MDM).	Mitarbeiter registrieren das Gerät mithilfe ihres Azure AD-Kontos bei Azure AD. Die Registrierung bei der MDM-Lösung der Organisation erfolgt automatisch (AAD+MDM – erfordert AzureAD Premium).
Verwaltung von Anmeldeinformationen	Mitarbeiter melden sich am Gerät mit Anmeldeinformationen eines Microsoft-Kontos an. Benutzer können sich bei Geräten nicht mit Azure AD-Anmeldeinformationen anmelden. Dies gilt auch, wenn sie die Anmeldeinformationen nach der ursprünglichen Aktivierung mit einem Microsoft-Konto hinzufügen.	Mitarbeiter melden sich am Gerät mit Azure AD-Anmeldeinformationen an. Die IT kann das Hinzufügen einer persönlichen Identität wie z.B. eines Microsoft- oder Google-Kontos blockieren. Die IT steuert ohne Einschränkungen alle Gerätezugriffsrichtlinien.
Möglichkeit zur Blockierung der Verwendung einer persönlichen Identität auf dem Gerät	Nein	Ja
Verwendung von Benutzereinstellungen und Daten über mehrere Windows-Geräte hinweg	Benutzer- und App-Einstellungen stehen dank Roaming über OneDrive auf allen Geräten zur Verfügung, die mit der gleichen persönlichen Identität aktiviert wurden.	Wenn das Gerät mit einem Microsoft-Konto aktiviert und dann ein Azure AD-Konto hinzugefügt wird, können Benutzer- und App-Einstellungen geräteübergreifend verwendet werden. Wenn Sie Ihr Microsoft-Konto einem zu Azure AD hinzugefügten Gerät hinzufügen, ist dies nicht der Fall. Microsoft plant das Unternehmens-Roaming für eine zukünftige Version.

Grad der Kontrolle	Organisationen können die meisten der verfügbaren restriktiven Richtlinien auf Geräte anwenden und das Microsoft-Konto deaktivieren. Sie können verhindern, dass Benutzer Vollzugriff auf ihre Geräte erlangen, indem sie deren Registrierung bei der MDM-Lösung der Organisation aufheben oder das Gerät zurücksetzen. Rechtliche Einschränkungen können gelten. Weitere Informationen erhalten Sie bei Ihrer Rechtsabteilung.	Organisationen können auf Geräten beliebige restriktive Richtlinien anwenden, um diese an Unternehmensstandards und Kompatibilitätsbestimmungen anzupassen. Außerdem können sie verhindern, dass der Benutzer die Registrierung des Geräts beim Unternehmen aufhebt.
Informationsschutz	Sie können zwar Richtlinien zum Schutz und zur Kontrolle von unternehmenseigenen Apps und Daten auf den Geräten anwenden und so dem Verlust von geistigem Eigentum vorbeugen, den Mitarbeitern jedoch weiterhin uneingeschränkte Kontrolle über persönliche Aktivitäten wie das Herunterladen und Installieren von Apps und Spielen gewähren.	Unternehmen können die private Nutzung von Geräten blockieren. Durch die Initialisierung von Geräten mit einer Unternehmensidentität haben Organisationen uneingeschränkte Kontrolle über die Geräte und können eine Personalisierung der Geräte verhindern.
App-Einkäufe	Mitarbeiter können mit einer persönlichen Kreditkarte Apps aus dem Store erwerben und installieren.	Mitarbeiter können Apps aus dem Microsoft Store für Unternehmen installieren. Mitarbeiter können ohne das Hinzufügen eines Microsoft-Kontos keine Apps aus dem Store installieren oder erwerben.

> **Hinweis:** Im Zusammenhang mit Windows-as-a-Service wird sich die Differenzierung der MDM-Funktionen zukünftig ändern.

Optionen für die Infrastruktur

Gilt für: unternehmenseigene und persönliche Geräte

In Szenarien der persönlichen und der unternehmenseigenen Bereitstellung stellt ein MDM-System die grundlegende Infrastruktur dar, die zum Bereitstellen und Verwalten von Windows10 Mobile-Geräten erforderlich ist. Ein Azure AD Premium-Abonnement wird als Identitätsanbieter empfohlen und ist erforderlich, um bestimmte Funktionen zu unterstützen. Windows10 Mobile ermöglicht eine reine cloudbasierte Infrastruktur oder eine Hybrid-Infrastruktur, bei der die Azure AD-Identitätsverwaltung mit einem lokalen Verwaltungssystem kombiniert wird, um Geräte zu verwalten. Microsoft unterstützt jetzt auch eine rein lokale Lösung zum Verwalten von Windows10 Mobile-Geräten mit Configuration Manager.

Azure Active Directory Azure AD ist ein cloudbasierter Verzeichnisdienst zur Identitäts- und Zugriffsverwaltung. Dank der Möglichkeit zur Integration in bereits vorhandene lokale Verzeichnisse lässt sich eine Hybrid-Identitätslösung realisieren. Organisationen, die Microsoft Office365 oder Intune verwenden, nutzen bereits AzureAD, das drei Editionen umfasst: Free, Basic und Premium (siehe Azure Active Directory-Editionen). Die AzureAD-Geräteregistrierung wird von allen Editionen unterstützt. Für die automatische MDM-Registrierung und den bedingten, gerätestatusbasierten Zugriff wird jedoch die Premium Edition benötigt.

Mobile Geräteverwaltung Microsoft Intune, Teil von Enterprise Mobility + Security, ist ein cloudbasiertes MDM-System zur Verwaltung von Remotegeräten. Die Identitätsverwaltung von Intune basiert ebenso wie die Identitätsverwaltung von Office365 auf Azure AD. Dadurch können die Mitarbeiter bei der Geräteregistrierung in Intune die gleichen Anmeldeinformationen verwenden wie bei der Anmeldung bei Office365. Intune unterstützt auch Geräte mit anderen Betriebssystemen wie iOS und Android und stellt somit eine umfassende MDM-Lösung

dar. Mehrere MDM-Systeme unterstützen Windows10, und die meisten unterstützen Bereitstellungsszenarien für persönliche und unternehmenseigene Geräte. Windows10 Mobile wird momentan von folgenden MDM-Anbietern unterstützt: AirWatch, Citrix, MobileIron, SOTI, Blackberry und weitere. Die meisten branchenführenden MDM-Anbieter unterstützen bereits die Integration in AzureAD. Die MDM-Anbieter mit Azure AD-Unterstützung finden Sie im Azure Marketplace. Wenn Azure AD in Ihrer Organisation nicht verwendet wird, muss der Benutzer bei OOBE ein Microsoft-Konto verwenden, bevor das Gerät bei der MDM-Lösung mithilfe eines Unternehmenskontos registriert wird.

> **Hinweis:** Anstelle eines umfangreichen MDM-Systems kann für die Verwaltung mobiler Geräte auch Exchange ActiveSync (EAS) verwendet werden. Diese Option wird in diesem Handbuch jedoch nicht behandelt. EAS ist in Microsoft Exchange Server2010 und höheren Versionen sowie in Office365 verfügbar. Darüber hinaus wurde Office365 von Microsoft kürzlich um Intune-basierte MDM-Funktionen erweitert. Von MDM für Office365 werden nur mobile Geräte unterstützt (also etwa Geräte unter Windows10 Mobile, iOS oder Android). MDM für Office365 bietet einen Teil der Verwaltungsfunktionen von Intune. Hierzu zählen die Remotezurücksetzung eines Geräts, die Blockierung des Zugriffs eines Geräts auf ExchangeServer-E-Mails sowie die Konfiguration von Geräterichtlinien (etwa für Kennungsanforderungen). Weitere Informationen zu den Funktionen von MDM für Office 365 finden Sie unter Übersicht der mobilen Geräteverwaltung für Office 365.

Clouddienste Auf Mobilgeräten mit Windows10 Mobile können Benutzer problemlos Verbindungen zu Clouddiensten herstellen, die Benutzerbenachrichtigungen bereitstellen und Diagnose- sowie Nutzungsdaten sammeln. Mit Windows 10 Mobile können Organisationen steuern, wie diese Clouddienste von Geräten genutzt werden.

Windows-Pushbenachrichtigungsdienst Mithilfe des Windows-Pushbenachrichtigungsdiensts können Softwareentwickler über ihre Clouddienste Popup-, Kachel- und Signalupdates sowie unformatierte Updates senden. Damit steht ein Mechanismus zur energieeffizienten und verlässlichen Updatebereitstellung für Benutzer zur Verfügung. Pushbenachrichtigungen können allerdings die Akkulaufzeit beeinträchtigen. Daher schränkt der Stromsparmodus von Windows10 Mobile Hintergrundaktivitäten auf den Geräten ein, um die Akkulaufzeit zu verlängern. Benutzer können den Stromsparmodus so konfigurieren, dass er automatisch aktiviert wird, wenn der Akkustand einen bestimmten Schwellenwert unterschreitet. Im Stromsparmodus deaktiviert Windows10 Mobile den Empfang von Pushbenachrichtigungen, um Energie zu sparen. Für dieses Verhalten gibt es jedoch eine Ausnahme. Unter Windows10 Mobile kann der Stromsparmodus mithilfe der Einstellung „Immer zugelassen" (in der Einstellungs-App) so konfiguriert werden, dass Apps auch bei aktiviertem Stromsparmodus Pushbenachrichtigungen empfangen. Diese Liste kann von Benutzern manuell konfiguriert werden, oder die IT kann das URI-Schema für den Stromsparmodus in Windows10 Mobile konfigurieren (ms-settings:batterysaver-settings).

Weitere Informationen zum Integritätsnachweis unter Windows 10 Mobile finden Sie im Sicherheitshandbuch für Windows 10 Mobile.

Windows Update for Business Microsoft hat Windows Update for Business entwickelt, um IT-Administratoren weitere Verwaltungsfunktionen rund um Windows Update bereitzustellen, wie beispielsweise die Möglichkeit, Updates für Gruppen von Geräten bereitzustellen oder Wartungszeitfenster für die Installation von Updates festzulegen.

Microsoft Store für Unternehmen Der Microsoft Store für Unternehmen ist der zentrale Ort, an dem IT-Administratoren Apps für Windows10-Geräte suchen, erwerben, verwalten und verteilen können. Dazu gehören sowohl interne branchenspezifische Apps als auch kommerziell erhältliche Drittanbieter-Apps.

Konfigurieren

MDM-Administratoren können Richtlinieneinstellungen auf jedem persönlichen und unternehmenseigenen Gerät, das in einem MDM-System registriert ist, definieren und implementieren. Die verwendeten

Konfigurationseinstellungen sind abhängig vom Bereitstellungsszenario. Dabei bieten unternehmenseigene Geräte die umfassendsten Kontrollmöglichkeiten für die IT.

> **Hinweis:** Dieses Handbuch unterstützt IT-Experten dabei, die Verwaltungsoptionen für das Windows10 Mobile-Betriebssystem zu verstehen. In der Dokumentation zu Ihrem MDM-System finden Sie Informationen darüber, wie diese Richtlinien von Ihrem MDM-Anbieter aktiviert werden. Nicht alle MDM-Systeme unterstützen jede in diesem Handbuch beschriebene Einstellung. Einige unterstützen benutzerdefinierte Richtlinien über OMA-URI-XML-Dateien. Weitere Informationen finden Sie unter Microsoft Intune-Unterstützung für benutzerdefinierte Richtlinien. Namenskonventionen können zwischen MDM-Anbietern ebenfalls variieren.

Kontoprofil

Gilt für: unternehmenseigene Geräte

Das Erzwingen von Kontenbeschränkungen für Mitarbeiter auf einem unternehmenseigenen Gerät ist wichtig für das Verhindern von Datenlecks und den Datenschutz. Durch die Beschränkung des Geräts auf ein einziges Konto, das von der Organisation kontrolliert wird, kann das Risiko von Datenlecks verringert werden. Sie können Mitarbeitern jedoch erlauben, ein persönliches Microsoft-Konto oder sonstige private E-Mail-Konten hinzuzufügen.

- **Microsoft-Konto zulassen** Gibt an, ob Benutzer dem Gerät ein Microsoft-Konto hinzufügen und dieses Konto zur Authentifizierung bei Clouddiensten verwenden dürfen, z.B. für das Erwerben von Apps im Microsoft Store, auf Xbox oder in Groove.
- **Manuelles Hinzufügen von Nicht-Microsoft-Konten zulassen** Gibt an, ob Benutzer E-Mail-Konten hinzufügen dürfen, bei denen es sich nicht um Microsoft-Konten handelt.

E-Mail-Konten

Gilt für: unternehmenseigene und persönliche Geräte

E-Mails, der zugehörige Kalender und Kontakte sind die primären Apps, die Benutzer auf ihren Smartphones aufrufen. Deren ordnungsgemäße Konfiguration ist entscheidend für den Erfolg jedes Mobilitätsprogramms. Bei Bereitstellungsszenarien für persönliche und unternehmenseigene Geräte werden diese E-Mail-Kontoeinstellungen direkt nach der Registrierung bereitgestellt. Mithilfe Ihres unternehmenseigenen MDM-Systems können Sie E-Mail-Kontoprofile für Ihr Unternehmen definieren, diese auf Geräten bereitstellen sowie Richtlinien für den Posteingang verwalten.

- Die meisten unternehmenseigenen E-Mail-Systeme nutzen **Exchange ActiveSync (EAS)**. Weitere Informationen zum Konfigurieren von EAS-E-Mail-Profilen finden Sie unter ActiveSync CSP.
- **Simple Mail Transfer Protocol (SMTP)**-E-Mail-Konten können ebenfalls mit Ihrem MDM-System konfiguriert werden. Ausführlichere Informationen zur Konfiguration von SMTP-E-Mail-Profilen finden Sie unter Email CSP. Die Erstellung eines SMTP-E-Mail-Profils wird von Microsoft Intune derzeit nicht unterstützt.

Einschränkungen für die Gerätesperre

Gilt für: unternehmenseigene und persönliche Geräte

Es ist allgemein üblich, Geräte mit Unternehmensinformationen durch eine Kennung zu schützen, wenn diese nicht verwendet werden. Als bewährte Methode empfiehlt Microsoft die Implementierung einer Richtlinie für die Gerätesperre von Windows10 Mobile-Geräten, um Apps und Daten zu schützen. Sie können ein komplexes Kennwort oder eine numerische PIN zum Sperren von Geräten verwenden. Windows Hello wurde mit Windows10 eingeführt und ermöglicht die Verwendung einer PIN, eines Begleitgeräts (z.B. Microsoft Band) oder biometrischer Daten, um Ihre Identität zum Entsperren von Windows10 Mobile-Geräten zu überprüfen.

> **Hinweis:** Bei der Erstauslieferung waren Microsoft Passport und Windows Hello in Windows10 enthalten, die zusammen für eine mehrstufige Authentifizierung sorgten. Für eine einfachere Bereitstellung und höhere Wartungsfreundlichkeit hat Microsoft diese Technologien in einer zentralen Lösung mit dem Namen Windows

> Hello vereint. Kunden, die diese Technologien bereits eingesetzt haben, werden keine Änderungen in Bezug auf die Funktionalität feststellen. Kunden, die Windows Hello noch evaluieren müssen, werden eine einfachere Bereitstellung beobachten, die auf vereinfachte Richtlinien, Dokumentation und Semantik zurückzuführen ist. Für die Verwendung von Windows Hello mit biometrischen Daten ist spezielle Hardware erforderlich, etwa ein Fingerabdruckleser, ein beleuchteter IR-Sensor oder sonstige biometrische Sensoren. Für den hardwarebasierten Schutz der Anmeldeinformationen von Windows Hello ist TPM1.2 oder höher erforderlich. Ist kein TPM vorhanden oder konfiguriert, wird ein softwarebasierter Schutz der Anmeldeinformationen/Schlüssel verwendet. Begleitgeräte müssen über Bluetooth mit Windows10-PCs gekoppelt werden. Für die Verwendung eines Windows Hello-Begleitgeräts, das ein Roaming der Anmeldeinformationen von Windows Hello ermöglicht, muss der Benutzer mit der Pro- oder Enterprise-Edition auf dem Windows10-PC angemeldet sein.

Die meisten Richtlinien zur Einschränkung der Gerätesperre über ActiveSync und MDM sind seit Windows Phone7 verfügbar und können auch für Windows10 Mobile noch verwendet werden. Wenn Sie Windows10-Geräte in einem Bereitstellungsszenario für persönliche Geräte bereitstellen, gelten diese Einstellungen.

- **Device Password Enabled** Gibt an, ob Benutzer ein Kennwort für die Gerätesperre verwenden müssen.
- **Allow Simple Device Password** Gibt an, ob Benutzer ein einfaches Kennwort (z.B. „1111“ oder „1234“) verwenden dürfen.
- **Alphanumeric Device Password Required** Gibt an, ob Benutzer ein alphanumerisches Kennwort verwenden müssen. Wenn entsprechend konfiguriert, fordert Windows den Benutzer mit einer vollständigen Gerätetastatur zur Eingabe eines komplexen Kennworts auf. Andernfalls kann der Benutzer über die Tastatur eine numerische PIN eingeben.
- **Min Device Password Complex Characters** Die Anzahl von Kennwortelementtypen (d.h. Groß- und Kleinbuchstaben, Zahlen oder Satzzeichen), die zum Erstellen sicherer Kennwörter erforderlich sind
- **Device Password History** Die Anzahl von Kennwörtern, die von Windows10 Mobile im Kennwortverlauf gespeichert werden. (Kennwörter aus dem Verlauf können nicht zur Erstellung neuer Kennwörter verwendet werden.)
- **Min Device Password Length** Die Mindestanzahl von Zeichen für die Erstellung neuer Kennwörter
- **Max Inactivity Time Device Lock** Die maximale Inaktivitätsdauer (in Minuten), nach der Geräte gesperrt werden und ein Kennwort für die Entsperrung erforderlich ist
- **Allow Idle Return Without Password** Gibt an, ob sich Benutzer erneut authentifizieren müssen, wenn ihre Geräte vor Erreichen der Inaktivitätszeit aus einem Standbymodus reaktiviert werden.
- **Max Device Password Failed Attempts** Gibt die maximal zulässige Anzahl nicht erfolgreicher Authentifizierungsversuche an, nach denen ein Gerät zurückgesetzt wird. (Mit dem Wert „0“ wird die Gerätezurücksetzung deaktiviert.)
- **Screen Timeout While Locked** Die Anzahl von Minuten bis zum Sperrbildschirm-Timeout. (Diese Richtlinie wirkt sich auf die Energieverwaltung des Geräts aus.)
- **Allow Screen Timeout While Locked User Configuration** Gibt an, ob Benutzer das Bildschirmtimeout manuell konfigurieren können, während der Sperrbildschirm des Geräts aktiv ist. (Wenn Sie diese Einstellung deaktivieren, wird die Einstellung **Screen Timeout While Locked** von Windows10 Mobile ignoriert.)

Wenn Sie Geräte mit dem Szenario für unternehmenseigene Geräte bereitstellen, sind die Einstellungen in Verbindung mit Windows Hello für die Konfiguration der Gerätesperre wichtig. Microsoft hat für alle Benutzer die Anforderung festgelegt, im Rahmen des Beitritts zu Azure AD eine numerische Kennung zu erstellen. Durch diesen Richtlinienstandard müssen Benutzer eine vierstellige Kennung auswählen. Diese kann jedoch mit einem AAD-registrierten MDM-System für die von Ihrer Organisation gewünschte Komplexität konfiguriert werden. Wenn Sie Azure AD mit einem automatischen MDM-Registrierungsmechanismus verwenden, werden diese Richtlinieneinstellungen automatisch während der Geräteregistrierung angewendet.

Sie werden feststellen, dass einige der Einstellungen sehr ähnlich sind, insbesondere jene in Verbindung mit Mindestlänge, Verlauf, Ablauf und Komplexität der Kennung. Wenn Sie die Richtlinie an mehreren Orten festlegen,

werden beide Richtlinien angewendet, wobei die strikteste Richtlinie beibehalten wird. Unter PassportForWork CSP, DeviceLock CSP (Windows Phone8.1) und Policy CSP finden Sie ausführlichere Informationen.

Ändern der Einstellungen verhindern

Gilt für: unternehmenseigene Geräte

In der Regel dürfen Mitarbeiter bestimmte Einstellungen auf persönlichen Geräten ändern, die Sie auf unternehmenseigenen Geräten möglicherweise sperren würden. Mitarbeiter können bestimmte Einstellungen des Smartphones über die Einstellungs-Applets interaktiv anpassen. Mithilfe von MDM können Sie einschränken, welche Einstellungen Benutzer ändern können.

- **Allow Your Account** Gibt an, ob Benutzer im Einstellungsbereich „Ihre E-Mail-Adresse und Konten" die Kontokonfiguration ändern dürfen.
- **Allow VPN** Ermöglicht dem Benutzer die Änderung von VPN-Einstellungen.
- **Allow Data Sense** Ermöglicht dem Benutzer die Änderung von Data Sense-Einstellungen.
- **Allow Date Time** Ermöglicht dem Benutzer die Änderung von Einstellungen zu Datum und Uhrzeit.
- **Allow Edit Device Name** Ermöglicht dem Benutzer die Änderung des Gerätenamens.
- **Allow Speech Model Update** Gibt an, ob das Gerät Updates für die Spracherkennungs- und Sprachsynthesemodelle erhält (zur Verbesserung der Genauigkeit und Leistung).

Hardwareeinschränkungen

Gilt für: unternehmenseigene Geräte

Geräte unter Windows10 Mobile sind mit neuester Technologie ausgestattet. Hierzu zählen beliebte Hardwarefeatures wie Kameras, GPS-Sensoren, Mikrofone, Lautsprecher, NFC-Funkmodule, Speicherkartensteckplätze, USB-Schnittstellen, Bluetooth-Schnittstellen, Mobilfunkmodule und WLAN. Die Verfügbarkeit dieser Features kann mit Hardwareeinschränkungen gesteuert werden.

Nachfolgend sind die MDM-Einstellungen aufgeführt, die Windows10 Mobile im Zusammenhang mit der Konfiguration von Hardwareeinschränkungen unterstützt.

> **Hinweis:** Einige diese Hardwareeinschränkungen sorgen für Konnektivität und tragen zum Datenschutz bei.

- **NFC zulassen:** Gibt an, ob das NFC-Funkmodul aktiviert ist.
- **USB-Verbindung zulassen:** Gibt an, ob die USB-Verbindung aktiviert ist. (Diese Einstellung hat keine Auswirkung auf die USB-Ladefunktion.)
- **Bluetooth zulassen:** Gibt an, ob Benutzer auf ihren Geräten das Bluetooth-Funkmodul aktivieren und verwenden können.
- **Werbung per Bluetooth zulassen:** Gibt an, ob das Gerät als Quelle für Bluetooth-Ankündigungen fungieren und für andere Geräte sichtbar sein kann.
- **Sichtbaren Bluetoothmodus zulassen:** Gibt an, ob das Gerät nach anderen Geräten (wie etwa Headsets) suchen kann.
- **Allow Bluetooth pre-pairing** Gibt an, ob bestimmte gebündelte Bluetooth-Peripheriegeräte automatisch mit dem Hostgerät gekoppelt werden.
- **Bluetooth Services Allowed List:** Die Liste mit Bluetooth-Diensten und -Profilen, mit denen das Gerät eine Verbindung herstellen kann
- **Set Bluetooth Local Device Name:** Der Name des lokalen Bluetooth-Geräts
- **Kamera zulassen:** Gibt an, ob die Kamera aktiviert ist.
- **Allow Storage Card:** Gibt an, ob der Speicherkartensteckplatz aktiviert ist.
- **Sprachaufzeichnung zulassen:** Gibt an, ob der Benutzer das Mikrofon für Sprachaufzeichnungen verwenden darf.
- **Allow Location:** Gibt an, ob das Gerät den GPS-Sensor oder andere Standortermittlungsmethoden

verwenden kann, um Anwendungen Standortinformationen zur Verfügung zu stellen.

Zertifikate

Gilt für: unternehmenseigene und persönliche Geräte

Zertifikate helfen, die Sicherheit zu verbessern, indem Sie Kontoauthentifizierung, Wi-Fi-Authentifizierung, VPN-Verschlüsselung und SSL-Verschlüsselung von Webinhalten bereitstellen. Benutzer können Zertifikate auf Geräten zwar auch manuell verwalten, es empfiehlt sich jedoch, die Zertifikate während ihres gesamten Lebenszyklus (von der Registrierung über die Verlängerung bis hin zur Sperrung) über Ihr MDM-System zu verwalten. Um Zertifikate manuell zu installieren, können Sie sie auf der Microsoft Edge-Website veröffentlichen oder direkt per E-Mail senden. Letzteres eignet sich ideal für Testzwecke. Mit SCEP- und MDM-Systemen ist die Zertifikatverwaltung vollständig transparent und erfordert keinerlei Benutzereingriff. Dies kommt der Benutzerproduktivität zugute und verringert die Anzahl von Supportanfragen. Ihr MDM-System kann diese Zertifikate automatisch in den Zertifikatspeichern des Geräts bereitstellen, nachdem Sie das Gerät registrieren (sofern das MDM-System SCEP (Simple Certificate Enrollment Protocol) oder PFX (Personal Information Exchange unterstützt). Der MDM-Server kann per SCEP registrierte Clientzertifikate (einschließlich der von Benutzern installierten Zertifikate) auch abfragen und löschen oder eine neue Registrierungsanforderung auslösen, bevor das aktuelle Zertifikat abläuft. Neben der SCEP-Zertifikatverwaltung unterstützt Windows 10 Mobile auch die Bereitstellung von PFX-Zertifikaten. Die nachfolgende Tabelle enthält die Einstellungen für die Bereitstellung von PFX-Zertifikaten unter Windows10 Mobile. Ausführlichere Informationen zur Verwaltung von MDM-Zertifikaten finden Sie unter Client Certificate Install CSP und Installieren digitaler Zertifikate unter Windows10 Mobile. Verwenden Sie die Einstellung Manuelle Stammzertifikat Installation zulassen, um zu verhindern, dass Benutzerstamm-und Zwischenzertifizierungsstellen Zertifikate absichtlich oder versehentlich manuell installieren.

> **Hinweis:** Zertifikatbezogene Probleme auf Geräten mit Windows10 Mobile können mithilfe der kostenlosen Zertifikate-App aus dem Microsoft Store diagnostiziert werden. Diese App für Windows10 Mobile ermöglicht Folgendes:
>
> - Anzeigen einer Zusammenfassung aller persönlichen Zertifikate
> - Anzeigen der Details einzelner Zertifikate
> - Anzeigen der verwendeten Zertifikate für die VPN-, WLAN- und E-Mail-Authentifizierung
> - Ermitteln möglicherweise abgelaufener Zertifikate
> - Überprüfen des Zertifikatpfads und Vergewissern, dass Sie über die korrekten Zertifikate von Zwischen- und Stamm-ZS verfügen
> - Anzeigen der im TPM des Geräts gespeicherten Zertifikatschlüssel

WLAN-Profile

Gilt für: unternehmenseigene und persönliche Geräte

WLAN-Verbindungen werden bei mobilen Geräten mindestens ebenso intensiv genutzt wie die Datenverbindung. Die meisten WLAN-Netzwerke von Unternehmen erfordern Zertifikate und andere komplexe Informationen, um den Zugriff einzuschränken und zu schützen. Diese erweiterten WLAN-Informationen sind für typische Benutzer schwierig zu konfigurieren, doch MDM-Systeme können diese WLAN-Profile ohne Benutzereingriff vollständig konfigurieren. Sie können mehrere WLAN-Profile in Ihrem MDM-System erstellen. Die folgende Tabelle enthält die WLAN-Verbindungsprofileinstellungen von Windows10 Mobile, die von Administratoren konfiguriert werden können.

- **SSID** Der Name der Wi-Fi-Netzwerkdienst Satz-ID für die Groß-/Kleinschreibung
- **Sicherheitstyp** Die Art der Sicherheit, die das WLAN-Netzwerk verwendet; Dies kann einer der folgenden Authentifizierungstypen sein:
  - Open 802.11
  - Shared 802.11

  - WPA-Enterprise 802.11
  - WPA-Personal 802.11
  - WPA2-Enterprise 802.11
  - WPA2-Personal 802.11
- **Authentication encryption** Die Art der von der Authentifizierung verwendeten Verschlüsselung. Mögliche Verschlüsselungsmethoden:
  - None (no encryption)
  - Wired Equivalent Privacy
  - Temporal Key Integrity Protocol
  - Advanced Encryption Standard (AES)
- **Extensible Authentication Protocol Transport Layer Security (EAP-TLS)** EAP-TLS kann von den Sicherheitstypen „WPA-Enterprise 802.11“ und „WPA2-Enterprise 802.11“ mit Zertifikaten zur Authentifizierung verwendet werden.
- **Protected Extensible Authentication Protocol with Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2)** PEAP-MSCHAPv2 kann von den Sicherheitstypen „WPA-Enterprise 802.11“ und „WPA2-Enterprise 802.11“ mit einer Kombination aus Benutzername und Kennwort zur Authentifizierung verwendet werden.
- **Gemeinsam verwendeter Schlüssel** Von den Sicherheitstypen „WPA-Personal 802.11“ und „WPA2-Personal 802.11“ kann ein gemeinsam verwendeter Schlüssel zur Authentifizierung verwendet werden.
- **Proxy** Die Konfiguration eines beliebigen Netzwerk Proxys, der für die WLAN-Verbindung erforderlich ist (um den Proxy Server anzugeben, verwenden Sie den vollqualifizierten Domänennamen [FQDN], Internet Protocol Version 4 [IPv4]-Adresse, IP Version 6 [IPv6]-Adresse oder IPvFuture-Adresse).
- **Deaktivieren der Internet Verbindungsüberprüfung** Ob die WLAN-Verbindung auf Internet Konnektivität überprüft werden soll
- **Proxy auto-configuration URL** Eine URL, die die Proxy-Autokonfigurationsdatei angibt
- **Enable Web Proxy Auto-Discovery Protocol (WPAD)** Gibt an, ob WPAD aktiviert ist.

Darüber hinaus können Sie einige WLAN-Einstellungen für das gesamte Gerät festlegen.

- **Automatische Verbindung mit WLAN-Hotspots zulassen** Ob das Gerät automatisch erkennt und eine Verbindung zu WLAN-Netzwerken hergestellt wird
- **Manuelle WLAN-Konfiguration zulassen** Gibt an, ob der Benutzer die WLAN-Einstellungen manuell konfigurieren kann.
- **WLAN zulassen** Gibt an, ob die WLAN-Hardware aktiviert ist.
- **Internetfreigabe zulassen** Mit dieser Einstellung wird die Internetfreigabe zugelassen oder untersagt.
- **WLAN Scan Mode** Gibt an, wie aktiv das Gerät nach WLAN-Netzwerken sucht.

Ausführlichere Informationen zu WLAN-Verbindungsprofileinstellungen finden Sie unter Wi-Fi CSP und Policy CSP.

APN-Profile

Gilt für: unternehmenseigene Geräte

Ein APN (Access Point Name) definiert Netzwerkpfade für Datenverbindungen. Üblicherweise wird für ein Gerät in Zusammenarbeit mit einem Mobilfunkanbieter lediglich ein einzelner APN definiert. Sie können jedoch auch mehrere APNs definieren, falls Ihr Unternehmen mehrere Mobilfunkanbieter verwendet. Ein APN stellt eine private Verbindung mit dem Unternehmensnetzwerk bereit, die anderen Unternehmen im Netz des Mobilfunkanbieters nicht zur Verfügung steht. APN-Profile können in MDM-Systemen definiert und bereitgestellt werden, um die Datenverbindung für Windows 10 Mobile zu konfigurieren. Geräte unter Windows 10 Mobile können immer nur ein APN-Profil besitzen. Die folgende Tabelle enthält die MDM-Einstellungen für APN-Profile, die von Windows10 Mobile unterstützt werden.

- **APN name** Der APN-Name
- *IP connection type* Der IP-Verbindungstyp. Mögliche Werte:
  - IPv4 only
  - IPv6 only
  - IPv4 and IPv6 concurrently
  - IPv6 with IPv4 provided by 46xlat
- **LTE attached** Gibt an, ob der APN als Teil eines LTE-Attach angefügt werden soll.
- **APN class ID** Der GUID, der die APN-Klasse gegenüber dem Modem definiert
- **APN authentication type** Der APN-Authentifizierungstyp. Mögliche Werte:
  - Keine
  - Auto
  - PAP
  - CHAP
  - MSChapv2
- **Benutzername** Das Benutzerkonto, wenn Benutzer als APN-Authentifizierungstyp die Option „PAP" (Password Authentication Protocol), „CHAP" oder „MSCHAPv2" auswählen
- **Kennwort** Das Kennwort für das unter „Benutzername" angegebene Benutzerkonto
- **Integrated circuit card ID** Der dem Mobilfunkverbindungsprofil zugeordnete ICCID (Integrated Circuit Card Identifier)
- **Always on** Gibt an, ob der Verbindungs-Manager bei Verfügbarkeit automatisch eine Verbindung zum APN herstellt.
- **Connection enabled** Gibt an, ob die APN-Verbindung aktiv ist.
- **Allow user control** Lässt zu, dass Benutzer Verbindungen zu anderen APNs neben dem APN des Unternehmens herstellen.
- **Hide view** Gibt an, ob die Mobilfunk-UX dem Benutzer das Anzeigen der APNs des Unternehmens gewährt.

Weitere Informationen zu den APN-Einstellungen finden Sie unter APN CSP.

Proxy

Gilt für: unternehmenseigene Geräte

Nachfolgend sind die Windows10 Mobile-Einstellungen zum Verwalten der APN-Proxyeinstellungen für die Geräteverbindung von Windows10 Mobile aufgeführt.

- **Verbindungsname** Gibt den Namen der Verbindung an, mit der der Proxy verknüpft ist (der APN-Name einer konfigurierten Verbindung).
- **Bypass Local** Gibt an, ob der Proxy umgangen werden soll, wenn das Gerät auf lokale Hosts zugreift.
- **Aktivieren** Gibt an, ob der Proxy aktiviert ist.
- **Ausnahme** Gibt eine durch Semikolons getrennte Liste externer Hosts an, die den Proxy umgehen sollen, wenn auf sie zugegriffen wird.
- **Benutzername** Gibt den Benutzernamen für die Verbindung zum Proxy an.
- **Kennwort** Gibt das Kennwort für die Verbindung zum Proxy an.
- **Server** Gibt den Namen des Proxyservers an.
- **Proxy connection type** Der Proxy-Verbindungstyp. Unterstützte Optionen: Null Proxy, HTTP, WAP, SOCKS4
- **Port** Die Portnummer der Proxyverbindung

Weitere Informationen zu Proxyeinstellungen finden Sie unter CM_ProxyEntries CSP.

VPN

Gilt für: unternehmenseigene und persönliche Geräte

Organisationen verwenden häufig ein VPN, um den Zugriff auf Apps und Ressourcen im Intranet des Unternehmens zu steuern. Neben den systemeigenen Microsoft-VPNs PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) und IKEv2 (Internet Key Exchange Protocol Version2) unterstützt Windows10 Mobile auch SSL-VPN-Verbindungen, die ein herunterladbares Plug-In aus dem Microsoft Store erfordern und von der Auswahl des VPN-Anbieters abhängig sind. Diese Plug-Ins funktionieren wie Apps und können mit Ihrem MDM-System direkt aus dem Microsoft Store installiert werden (siehe App-Verwaltung).

Sie können mehrere VPN-Verbindungsprofile erstellen und anschließend auf verwalteten Geräten unter Windows10 Mobile bereitstellen. Zum Erstellen eines VPN-Profils mit den systemeigenen VPN-Protokollen von Windows10 Mobile (z.B. IKEv2, PPTP oder L2TP) können Sie die folgenden Einstellungen verwenden:

- **VPN Servers** Der VPN-Server für das VPN-Profil
- **Routing policy type** Die Art der vom VPN-Profil verwendeten Routingrichtlinie. Mögliche Werte:
  - Split tunnel. Nur der für das Intranet bestimmte Netzwerkdatenverkehr wird über die VPN-Verbindung gesendet.
  - Force tunnel. Der gesamte Datenverkehr wird über die VPN-Verbindung gesendet.
- **Tunneling protocol type** Das Tunneling-Protokoll für VPN-Profile, die systemeigene VPN-Protokolle von Windows10 Mobile verwenden. Mögliche Werte: PPTP, L2TP, IKEv2, Automatisch
- **User authentication method** Die Benutzerauthentifizierungsmethode für die VPN-Verbindung. Mögliche Werte: EAP oder MSChapv2. (Der Wert „MSChapv2" wird von Windows10 Mobile für IKEv2-basierte VPN-Verbindungen nicht unterstützt.)
- **Machine certificate** Das für IKEv2-basierte VPN-Verbindungen verwendete Computerzertifikat.
- **EAP configuration** Um VPN-Benutzern ein einmaliges Anmelden mithilfe von Zertifikatauthentifizierung zu ermöglichen, muss eine XML-Datei für die EAP-Konfiguration (Extensible Authentication Protocol) erstellt und in das VPN-Profil eingebunden werden.
- **L2tpPsk** Der vorinstallierte Schlüssel für eine L2TP-Verbindung
- **Cryptography Suite** Aktiviert die Auswahl der Attribute für die kryptografische Suite, die für IPsec-Tunneling verwendet werden.

> **Hinweis:** Ein Profil für einmaliges Anmelden mit einer XML-Datei für die EAP-Konfiguration lässt sich am einfachsten mit dem Rasphone-Tool auf einem Windows10-PC erstellen. Nach der Ausführung von rasphone.exe führt Sie der Konfigurations-Assistent durch die erforderlichen Schritte. Weitere Informationen zum Erstellen des XML-BLOBs für die EAP-Konfiguration finden Sie im Artikel zur EAP-Konfiguration. Sie können das resultierende XML-BLOB im MDM-System verwenden, um das VPN-Profil auf dem Windows10 Mobile-Smartphone zu erstellen. Wenn Sie über mehrere Zertifikate auf den Geräten verfügen, sollten Sie Filterbedingungen für die automatische Zertifikatauswahl konfigurieren, damit Mitarbeiter nicht bei jeder Aktivierung einer VPN-Verbindung ein Authentifizierungszertifikat auswählen müssen. In diesem Artikel finden Sie weitere Details. Windows10 für PCs und Windows10 Mobile verfügen über den gleichen VPN-Client.

Mit Microsoft Store-basierten VPN-Plug-Ins für die VPN-Verbindung können Sie ein VPN-Plug-In-Profil mit den folgenden Attributen erstellen:

- **VPN-Server** Eine durch Kommas getrennte Liste mit VPN-Servern. Die Server können als URL, als vollqualifizierter Hostname oder als IP-Adresse angegeben werden.
- **Benutzerdefinierte Konfiguration** Ein HTML-codiertes XML-BLOB für SSL-VPN-Plug-In-spezifische Konfigurationsinformationen (wie etwa Authentifizierungsinformationen), die der Plug-In-Anbieter benötigt
- **Microsoft Store VPN plugin family name** Gibt den Microsoft Store-Paketfamiliennamen für das Microsoft Store-basierte VPN-Plug-In an.

Darüber hinaus können Sie pro VPN-Profil Folgendes angeben:

- **App-Triggerliste** Sie können jedem VPN-Profil eine App-Triggerliste hinzufügen. Die in der Liste angegebene

App löst automatisch das VPN-Profil für die Intranetverbindung aus. Wenn mehrere VPN-Profile für verschiedene Apps erforderlich sind, wird vom Betriebssystem automatisch die VPN-Verbindung hergestellt, wenn der Benutzer zwischen den Apps wechselt. Es kann jeweils nur eine VPN-Verbindung aktiv sein. Sollte die VPN-Verbindung getrennt werden, wird sie von Windows 10 Mobile automatisch und ohne Benutzereingriff wiederhergestellt.

- **Route List** Eine Liste mit Routen, die der Routingtabelle für die VPN-Schnittstelle hinzugefügt werden sollen. Diese ist erforderlich für Fälle von getrenntem Tunneln, bei denen die VPN-Server-Site basierend auf der der Schnittstelle zugewiesenen IP-Adresse mehr Subnetze umfasst als das Standardsubnetz.
- **Domänennamen-Informationsliste** NRPT-Regeln (Name Resolution Policy Table – Richtlinientabelle für die Namensauflösung) für das VPN-Profil
- **Traffic Filter List** Gibt eine Liste mit Regeln an. Nur Datenverkehr, der diesen Regeln entspricht, kann über die VPN-Schnittstelle gesendet werden.
- **DNS-Suffixe** Eine durch Kommas getrennte Liste mit DNS-Suffixen für die VPN-Verbindung. Alle DNS-Suffixe in dieser Liste werden automatisch der Suffix-Suchliste hinzugefügt.
- **Proxy** Jegliche nach der Herstellung der VPN-Verbindung erforderliche Proxyunterstützung, einschließlich Name des Proxyservers sowie URL für die automatische Proxykonfiguration. Gibt die URL für den automatischen Abruf von Proxyservereinstellungen an.
- **Always on connection** Windows10 Mobile bietet ein ständig aktives VPN, sodass eine VPN-Verbindung automatisch gestartet werden kann, sobald sich ein Benutzer anmeldet. Die VPN-Verbindung bleibt bestehen, bis sie vom Benutzer manuell getrennt wird.
- **Remember credentials** Gibt an, ob Anmeldeinformationen von der VPN-Verbindung zwischengespeichert werden.
- **Trusted network detection** Eine durch Kommas getrennte Liste mit vertrauenswürdigen Netzwerken, die dafür sorgt, dass keine VPN-Verbindung hergestellt wird, wenn direkt auf das Intranet zugegriffen werden kann (WLAN)
- **Enterprise Data Protection Mode ID** Unternehmens-ID. Ein optionales Feld, mit dem zugelassen werden kann, dass das VPN automatisch anhand einer App ausgelöst wird, die mit einer Windows Information Protection-Richtlinie festgelegt wird.
- **Gerätekompatibilität** Mit dieser Einstellung können Azure AD-basierter bedingter Zugriff auf das VPN eingerichtet und einmaliges Anmelden mit einem anderen Zertifikat als dem VPN-Authentifizierungszertifikat für die Kerberos-Authentifizierung im Fall von Gerätekompatibilität zugelassen werden.
- **Lock Down VPN profile** Ein Sperrmodus-VPN-Profil weist folgende Merkmale auf:
  - Es ist ständig aktiv.
  - Es kann nicht getrennt werden.
  - Wenn das VPN-Profil nicht verbunden ist, hat der Benutzer keinen Netzwerkzugriff.
  - Keine anderen VPN-Profile können verbunden oder geändert werden.
- **ProfileXML** Für den Fall, dass Ihr MDM-System nicht alle VPN-Einstellungen unterstützt, die Sie konfigurieren möchten, können Sie eine XML-Datei zum Definieren des VPN-Profils erstellen, das auf alle erforderlichen Felder angewendet werden soll.

Weitere Informationen zu VPN-Profilen finden Sie unter VPNv2 CSP

Einige geräteweite Einstellungen für die Verwaltung von VPN-Verbindungen können Ihnen bei der Verwaltung von VPNs über Datenverbindungen helfen. Dadurch reduzieren sich wiederum die Kosten im Zusammenhang mit Roaming- oder Datentarifgebühren.

- **Allow VPN** Gibt an, ob Benutzer die VPN-Einstellungen ändern können.
- **VPN über Mobilfunk zulassen** Gibt an, ob Benutzer VPN-Verbindungen über Mobilfunknetze herstellen können.
- **Allow VPN Over Cellular when Roaming** Gibt an, ob Benutzer während des Roamings VPN-Verbindungen über Mobilfunknetze herstellen können.

Speicherverwaltung

Gilt für: unternehmenseigene und persönliche Geräte

Der Schutz der Apps und Daten auf einem Gerät ist ein zentraler Aspekt der Gerätesicherheit. Eine Methode zum Schutz Ihrer Apps und Daten ist die Verschlüsselung des internen Gerätespeichers. Die Geräteverschlüsselung in Windows 10 Mobile trägt dazu bei, Unternehmensdaten vor unbefugtem Zugriff zu schützen, auch wenn ein nicht autorisierter Benutzer den physischen Besitz des Geräts besitzt.

Windows10 Mobile ermöglicht außerdem die Installation von Apps auf einer SD-Karte. Das Betriebssystem speichert Apps auf einer speziell für diesen Zweck vorgesehenen Partition. Dieses Feature ist immer aktiv, daher muss hierzu nicht erst eine Richtlinie festgelegt werden.

Die SD-Karte wird eindeutig mit einem Gerät gekoppelt. Die Apps und Daten auf der verschlüsselten Partition sind für kein anderes Gerät sichtbar. Auf der unverschlüsselten Partition gespeicherte Daten (etwa Musik oder Fotos) stehen dagegen auch anderen Geräten zur Verfügung. Dadurch erhalten Benutzer die Flexibilität, eine SD-Karte zu verwenden, während vertrauliche Apps und Daten weiterhin geschützt bleiben.

Sie können die Einstellung **Allow Storage Card** deaktivieren, wenn Sie Benutzern die Verwendung von SD-Karten vollständig untersagen möchten. Wenn Sie den Speicher nicht verschlüsseln möchten, können Sie Ihre unternehmenseigenen Apps und Daten mithilfe der Einstellungen „Restrict app data to the system volume" und „Restrict apps to the system volume" schützen. Diese Einstellungen sorgen dafür, dass Benutzer Ihre Apps und Daten nicht auf SD-Karten kopieren können.

Nachfolgend sind die MDM-Speicherverwaltungseinstellungen von Windows10 Mobile aufgeführt.

- **Allow Storage Card:** Gibt an, ob die Verwendung von Speicherkarten für die Datenspeicherung zulässig ist.
- **Require Device Encryption** Gibt an, ob der interne Speicher verschlüsselt wird. (Die Verschlüsselung eines Geräts kann nicht durch eine Richtlinie deaktiviert werden.)
- **Verschlüsselungsmethode** Gibt die BitLocker-Laufwerkverschlüsselungsmethode und die Verschlüsselungsstärke an. Mögliche Werte:
  - AES-Cipher Block Chaining (CBC) 128-bit
  - AES-CBC 256-bit
  - XEX-based tweaked-codebook mode with cipher text stealing (XTS)–AES (XTS-AES) 128-bit (Standardeinstellung)
  - XTS-AES-256-bit
- **Allow Federal Information Processing Standard (FIPS) algorithm policy** Gibt an, ob das Gerät die FIPS-Algorithmusrichtlinie zulässt.
- **SSL-Verschlüsselungssammlungen** Gibt eine Liste mit den zulässigen kryptografischen Verschlüsselungsalgorithmen für SSL-Verbindungen an.
- **Restrict app data to the system volume** Gibt an, ob App-Daten auf das Systemlaufwerk beschränkt werden.
- **Restrict apps to the system volume** Gibt an, ob Apps auf das Systemlaufwerk beschränkt werden.

Apps

Gilt für: unternehmenseigene und persönliche Geräte

Die Benutzerproduktivität auf mobilen Geräten wird oft durch Apps ermöglicht.

Mithilfe der Universellen Windows-Plattform (UWP) für Windows-Apps ermöglicht Windows10 das Entwickeln von Apps, die nahtlos geräteübergreifend funktionieren. UWP führt die Anwendungsplattform für alle Geräte mit Windows10 zusammen, sodass Apps ohne Änderungen auf allen Editionen von Windows10 ausgeführt werden können. Dadurch sparen Entwickler Zeit und Ressourcen, sodass Apps schneller und effizienter für mobile Benutzer bereitgestellt werden können. Durch das Modell „Write Once Run Anywhere" (WORA, Einmal schreiben, überall ausführen) wird auch die Produktivität der Benutzer gefördert, indem ein konsistentes und vertrautes App-

Verhalten auf jedem Gerätetyp bereitgestellt wird.

Für die Kompatibilität mit vorhandenen Apps können Apps für Windows Phone8.1 weiterhin auf Windows10 Mobile-Geräten ausgeführt werden. Dadurch wird die Migration auf die aktuelle Plattform erleichtert. Microsoft empfiehlt, Ihre Apps nach UWP zu migrieren, um alle Vorteile von Windows10 Mobile nutzen zu können. Darüber hinaus wurden Brücken zum leichten und schnellen Aktualisieren vorhandener Apps für Windows Phone8.1 (Silverlight) und iOS auf UWP entwickelt.

Auch das Lizenzieren und Erwerben von UWP-Apps über den Microsoft Store für Unternehmen sowie deren Bereitstellung auf Mitarbeitergeräten mithilfe des Microsoft Store oder eines MDM-Systems, das mit dem Microsoft Store für Unternehmen integriert werden kann, hat Microsoft für Organisationen vereinfacht. Mobile Mitarbeiter müssen mit Apps ausgestattet werden. Dabei muss jedoch auf effiziente Weise sichergestellt werden, dass diese Apps die Unternehmensrichtlinien für Datensicherheit erfüllen.

Weitere Informationen zu universellen Windows-Apps finden Sie in der Anleitung für Apps für die Universelle Windows-Plattform (UWP) sowie unter Quick Start Challenge: Universal Windows Apps in Visual Studio. Lesen Sie außerdem Portieren von Apps auf Windows10.

Microsoft Store für Unternehmen: Beschaffen der richtigen App

Gilt für: unternehmenseigene und persönliche Geräte

Der erste Schritt bei der App-Verwaltung besteht darin, Apps auszuwählen, die Ihre Benutzer benötigen. Sie können Ihre eigenen Apps entwickeln oder Apps aus dem Microsoft Store beziehen. Bei Windows Phone8.1 wurde ein Microsoft-Konto benötigt, um Apps aus dem Microsoft Store zu erwerben und zu installieren. Mit dem Microsoft Store für Unternehmen bietet Microsoft Organisationen die Möglichkeit, Apps für Mitarbeiter aus einem privaten Store zu beziehen, ohne dass ein Microsoft-Konto auf Windows10-Geräten benötigt wird.

Der Microsoft Store für Unternehmen ist ein Webportal, über das IT-Administratoren Apps für Windows10-Geräte suchen, erwerben, verwalten und verteilen können.

Bei Azure AD authentifizierte Manager haben Zugriff auf Funktionen und Einstellungen des Microsoft Store für Unternehmen, und Store-Manager können eine private Kategorie von Apps erstellen, die nur ihrer Organisation zur Verfügung stehen. (Hier erhalten Sie weitere Informationen dazu, welche speziellen Azure AD-Konten Zugriff auf den Microsoft Store für Unternehmen haben.) Über den Microsoft Store für Unternehmen können Organisationen App-Lizenzen für ihre Organisation erwerben und ihren Mitarbeitern Apps zur Verfügung stellen. Neben kommerziell verfügbaren Apps können Ihre Entwickler auf Nachfrage branchenspezifische Apps im Microsoft Store für Unternehmen veröffentlichen. Darüber hinaus können Abonnements für den Microsoft Store für Unternehmen in MDM-Systeme integriert werden, sodass Apps aus dem Microsoft Store für Unternehmen mit dem MDM-System verteilt und verwaltet werden können.

Der Microsoft Store für Unternehmen unterstützt die App-Verteilung unter zwei Lizenzierungsmodellen: online und offline.

Das Online-Modell (vom Store verwaltet) ist die empfohlene Methode. Dabei werden sowohl Verwaltungsszenarien für persönliche Geräte als auch für unternehmenseigene Geräte unterstützt. Um Online-Apps zu installieren, muss das Gerät zum Zeitpunkt der Installation über Internetzugriff verfügen. Auf unternehmenseigenen Geräten können Mitarbeiter mit einem Azure AD-Konto authentifiziert werden, um Online-Apps zu installieren. Bei persönlichen Geräten müssen Mitarbeiter das Gerät bei Azure AD registrieren, um Online-Apps mit Unternehmenslizenz zu installieren. Benutzer unternehmenseigener Geräte können Apps mit Unternehmenslizenz in der Store-App auf Ihrem Smartphone in einem privaten Katalog finden. Ist ein MDM-System mit dem Microsoft Store für Unternehmen verknüpft, können IT-Administratoren Store-Apps im App-Katalog des MDM-Systems anzeigen lassen. Benutzer können dann dort die gewünschten Apps suchen und installieren. IT-Administratoren können erforderliche Apps auch direkt an Mitarbeitergeräte mithilfe von Push übertragen, ohne dass ein Eingreifen des Mitarbeiters erforderlich ist.

Mitarbeiter mit persönlichen Geräten können die von ihrer Organisation lizenzierten Apps über die Store-App auf

ihrem Gerät installieren. Sie können entweder das Azure AD-Konto oder das Microsoft-Konto in der Store-App verwenden, um persönliche Apps zu erwerben. Wenn Sie zulassen, dass Mitarbeiter mit unternehmenseigenen Geräten ein sekundäres Microsoft-Konto hinzufügen, können private und geschäftliche Apps über die Store-App auf dem Gerät auf einheitliche Weise installiert werden.

Online lizenzierte Apps müssen nicht aus dem Microsoft Store an das MDM-System übertragen oder heruntergeladen werden, um verteilt und verwaltet zu werden. Wenn ein Mitarbeiter eine unternehmenseigene App auswählt, wird diese automatisch aus der Cloud installiert. Darüber hinaus werden Apps automatisch aktualisiert, wenn eine neue Version verfügbar ist, oder sie können bei Bedarf entfernt werden. Wird eine App durch das MDM-System oder den Benutzer vom Gerät entfernt, geht die Lizenz wieder an den Microsoft Store für Unternehmen über, sodass sie für einen anderen Benutzer oder auf einem anderen Gerät verwendet werden kann.

Um eine App offline zu verteilen (von der Organisation verwaltet), muss die App aus dem Microsoft Store für Unternehmen heruntergeladen werden. Dies kann im Portal des Microsoft Store für Unternehmen durch einen autorisierten Administrator durchgeführt werden. Bei der Offline-Lizenzierung muss der App-Entwickler dem Lizenzierungsmodell zustimmen, da der Microsoft Store nicht mehr die Lizenzen für den Entwickler nachverfolgen kann. Lässt der App-Entwickler das Herunterladen der App aus dem Microsoft Store nicht zu, müssen Sie die Dateien direkt beim Entwickler anfordern oder die Online-Lizenzierungsmethode verwenden.

Um erworbene Microsoft Store- oder branchenspezifische Apps offline auf einem Windows10 Mobile-Gerät zu installieren, können IT-Administratoren ein MDM-System verwenden. Das MDM-System verteilt die App-Pakete, die Sie aus dem Microsoft Store auf die Windows10 Mobile-Geräte heruntergeladen haben (auch als Querladen bezeichnet). Die Unterstützung für die Verteilung von Offline-Apps ist vom verwendeten MDM-System abhängig. In der Dokumentation Ihres MDM-Anbieters finden Sie weitere Informationen. Der App-Bereitstellungsprozess lässt sich vollständig automatisieren und ganz ohne Benutzereingriff abwickeln.

Microsoft Store-Apps oder branchenspezifische Apps, die in den Microsoft Store für Unternehmen hochgeladen wurden, werden automatisch auf allen Windows-Geräten als vertrauenswürdig behandelt, da sie mit Microsoft Store-Zertifikaten kryptografisch signiert sind. Branchenspezifische Apps, die in den Microsoft Store für Unternehmen hochgeladen werden, sind nur für Ihre Organisation verfügbar und für andere Unternehmen und Kunden nicht sichtbar. Wenn Sie Ihre branchenspezifischen Apps nicht hochladen möchten, müssen Sie eine Vertrauensstellung für die App auf Ihren Geräten herstellen. Zur Herstellung dieser Vertrauensstellung müssen Sie ein Signaturzertifikat mit Ihrer Public Key-Infrastruktur generieren und Ihre Vertrauenskette den vertrauenswürdigen Zertifikaten auf dem Gerät hinzufügen (siehe Abschnitt „Zertifikate"). Auf einem Gerät mit Windows10 Mobile können bis zu 20 selbstsignierte branchenspezifische Apps installiert werden. Um mehr als 20 Apps auf einem Gerät zu installieren, können Sie ein Signaturzertifikat von einer vertrauenswürdigen öffentlichen Zertifizierungsstelle erwerben oder Ihre Geräte auf Windows10 Mobile Enterprise Edition aktualisieren.

Weitere Informationen finden Sie unter Microsoft Store für Unternehmen.

Verwalten von Apps

Gilt für: unternehmenseigene Geräte

IT-Administratoren können steuern, welche Apps auf Windows10 Mobile-Geräten installiert werden dürfen und wie sie aktualisiert werden sollen.

Windows10 Mobile umfasst AppLocker. Damit können Administratoren Positiv- oder Negativlisten für Apps aus dem Microsoft Store erstellen. Diese Funktion erstreckt sich auch auf integrierte Apps, z.B. Xbox, Groove, SMS-Nachrichten, E-Mail, Kalender usw. Durch die Möglichkeit, Apps zuzulassen oder zu verweigern, können Sie sicherstellen, dass Mitarbeiter ihre Mobilgeräte für den vorgesehenen Zweck verwenden. Es ist jedoch nicht immer leicht, Anforderungen und Wünschen der Mitarbeiter und Sicherheitsaspekten gleichermaßen gerecht zu werden. Beim Erstellen von Positiv- oder Negativlisten muss außerdem die sich ändernde App-Landschaft des Microsoft Store berücksichtigt werden.

Ausführlichere Informationen finden Sie unter AppLocker CSP.

Neben der Steuerung, welche Apps zulässig sind, können IT-Experten mit einem MDM-System auch zusätzliche App-Verwaltungseinstellungen unter Windows10 Mobile implementieren.

- **Allow All Trusted Apps** Gibt an, ob Benutzer Apps auf dem Gerät querladen können.
- **Allow App Store Auto Update** Gibt an, ob automatische App-Updates aus dem Microsoft Store zulässig sind.
- **Allow Developer Unlock** Gibt an, ob die Entwicklersperre aufgehoben werden darf.
- **Allow Shared User App Data** Gibt an, ob mehrere Benutzer der gleichen App Daten gemeinsam nutzen können.
- **Allow Store** Gibt an, ob Microsoft Store-Apps ausgeführt werden dürfen. Hiermit wird das Installieren von Apps aus dem Store durch den Benutzer vollständig verhindert, die App-Verteilung über ein MDM-System ist jedoch weiterhin möglich.
- **Application Restrictions** Ein XML-BLOB, das die App-Einschränkungen für ein Gerät definiert. Das XML-BLOB kann eine Positiv- oder Negativliste für Apps enthalten. Apps können auf der Grundlage der App-ID oder des Herausgebers zugelassen oder verweigert werden. Siehe AppLocker weiter oben.
- **Disable Store Originated Apps** Deaktiviert das Starten aller Apps aus dem Microsoft Store, die vorinstalliert sind oder die heruntergeladen wurden, bevor die Richtlinie angewendet wurde.
- **Require Private Store Only** Gibt an, ob Benutzern ausschließlich der private Store in der Store-App auf dem Gerät zur Verfügung steht. Bei Aktivierung ist nur der private Store verfügbar. Bei deaktivierter Option sind sowohl der Einzelhandelskatalog als auch der private Store verfügbar.
- **Restrict App Data to System Volume** Gibt an, ob App-Daten nur auf dem Systemlaufwerk oder auch auf der SD-Karte gespeichert werden dürfen.
- **Restrict App to System Volume** Gibt an, ob Apps nur auf dem Systemlaufwerk oder auch auf der SD-Karte installiert werden dürfen.
- **Start screen layout** Ein zum Konfigurieren des Startbildschirms verwendetes XML-BLOB. (Weitere Informationen finden Sie unter Startlayout für Windows10 Mobile-Editionen.)

Weitere Details zu Anwendungsverwaltungsoptionen finden Sie unter Policy CSP

Schutz vor Datenverlust

Gilt für: unternehmenseigene und persönliche Geräte

Eine der größten Herausforderungen beim Schutz unternehmenseigener Informationen auf mobilen Geräten ist die Trennung dieser Daten von den persönlichen Daten. Die meisten verfügbaren Lösungen zur Datentrennung verlangen vom Benutzer, sich mit einem separaten Benutzernamen und Kennwort bei einem Container anzumelden, in dem alle unternehmenseigenen Apps und Daten gespeichert sind. Dies beeinträchtigt die Produktivität der Benutzer.

Windows10 Mobile umfasst Windows Information Protection, um Unternehmens- und private Daten auf transparente Weise zu schützen. Dabei werden persönliche und unternehmenseigene Daten automatisch gekennzeichnet und Richtlinien für die Apps angewendet, die auf die als unternehmenseigen klassifizierten Daten zugreifen können. Dies betrifft auch Daten, die auf lokalen oder Wechseldatenträgern gespeichert sind. Da Unternehmensdaten immer geschützt sind, können Benutzer diese nicht in öffentliche Speicherorte wie soziale Netzwerke oder persönliche E-Mails kopieren.

Windows Information Protection funktioniert mit allen Apps. Diese werden in zwei Kategorien unterteilt: optimiert und nicht optimiert. Optimierte Apps können zwischen unternehmenseigenen und privaten Daten unterscheiden und auf Grundlage von Richtlinien bestimmen, welche zu schützen sind. Unternehmensdaten sind jederzeit verschlüsselt und Versuche, sie zu kopieren und einzufügen oder mit nicht zum Unternehmen gehörenden Apps oder Benutzern zu teilen, schlagen fehl. Nicht optimierte Apps behandeln alle Daten als Unternehmensdaten und verschlüsseln in der Standardeinstellung alles.

Jede App, die auf der UWA-Plattform entwickelt wird, kann optimiert werden. Microsoft hat alle Anstrengungen unternommen, um mehrere der am häufigsten verwendeten Apps zu optimieren, darunter:

- Microsoft Edge
- Microsoft Kontakte
- Mobile Office-Apps (Word, Excel, PowerPoint und OneNote)
- Outlook-Mail und -Kalender
- Microsoft Fotos
- MicrosoftOneDrive
- Groove-Musik
- Microsoft Filme & TV
- Microsoft-Nachrichten

Die folgende Tabelle enthält die Einstellungen, die für Windows Information Protection konfiguriert werden können:

- **Erzwingungsstufe*** Legen Sie die Erzwingungsstufe für den Informationsschutz fest:
  - Aus (kein Schutz)
  - Silent mode (nur verschlüsseln und überwachen)
  - Override mode (verschlüsseln, auffordern und überwachen)
  - Block mode (verschlüsseln, blockieren und überwachen)
- **Unternehmensgeschützte Domänennamen*** Eine Liste von Domänen, die vom Unternehmen für die zugehörigen Benutzeridentitäten verwendet wird. Benutzeridentitäten von einer dieser Domänen werden als vom Unternehmen verwaltete Konten betrachtet, und die damit verknüpften Daten werden geschützt.
- **Entschlüsselung durch Benutzer zulassen** Ermöglicht Benutzern das Entschlüsseln von Dateien. Wird Entschlüsseln nicht zugelassen, kann der Benutzer den Schutz unternehmenseigener Inhalte über das Betriebssystem oder die Benutzeroberfläche der App nicht aufheben.
- **Require protection under lock configuration** Gibt an, ob der Schutz von Daten bei Sperre (auch als Verschlüsseln unter PIN bezeichnet) konfiguriert werden soll.
- **Datenwiederherstellungszertifikat*** Gibt ein Wiederherstellungszertifikat an, das für die Datenwiederherstellung verschlüsselter Dateien verwendet werden kann. Dieses ist identisch mit dem Datenwiederherstellungs-Agent-Zertifikat (Data Recovery Agent, DRA) für das verschlüsselnde Dateisystem (Encrypting File System, EFS). Es wird lediglich über MDM anstatt durch die Gruppenrichtlinie bereitgestellt.
- **Revoke on unenroll** Gibt an, ob die Informationsschutzschlüssel widerrufen werden, wenn die Registrierung eines Geräts im Verwaltungsdienst aufgehoben wird.
- **RMS template ID for information protection** Ermöglicht dem IT-Administrator, den Zugriff auf RMS-geschützte Dateien zu konfigurieren, z.B. wer diesen erhält und wie lange.
- **Allow Azure RMS for information protection** Gibt an, ob Azure RMS-Verschlüsselung für den Informationsschutz zugelassen wird.
- **Show information protection icons** Gibt an, ob Symbolen für informationsgeschützte Dateien im Webbrowser und Kacheln für reine Unternehmens-Apps im Startmenü Überlagerungen hinzugefügt werden.
- **Status** Eine schreibgeschützte Bitmaske, die den aktuellen Status des Informationsschutzes auf dem Gerät angibt. Der MDM-Dienst kann anhand dieses Werts den aktuellen Gesamtzustand des Informationsschutzes ermitteln.
- **Unternehmens-IP-Bereich*** Die Unternehmens-IP-Bereiche zur Definition der Computer im Unternehmensnetzwerk. Daten, die von diesen Computern stammen, werden als Unternehmensdaten betrachtet und geschützt.
- **Unternehmensnetzwerk-Domänennamen*** Eine Liste von Domänen, die die Grenzen des Unternehmens umfassen. Daten von einer dieser Domänen, die an ein Gerät gesendet werden, werden als Unternehmensdaten betrachtet und geschützt.
- **Unternehmenscloudressourcen** Eine Liste mit Domänen von Unternehmensressourcen, die in der Cloud gehostet werden und geschützt werden müssen.

> **Hinweis:** * Hierbei handelt es sich um erforderliche Windows Information Protection-Richtlinien. Für eine ordnungsgemäße Funktionsweise von Windows Information Protection müssen die Einstellungen für AppLocker und Netzwerkisolation – speziell Unternehmens-IP-Bereich und Unternehmensnetzwerk-Domänennamen – konfiguriert werden. So wird die Quelle aller Unternehmensdaten definiert, die Schutz benötigen. Außerdem wird dadurch sichergestellt, dass Daten, die an diese Speicherorte geschrieben werden, nicht durch den Verschlüsselungsschlüssel des Benutzers verschlüsselt werden (damit andere Benutzer im Unternehmen darauf zugreifen können).

Weitere Informationen zu Windows Information Protection finden Sie unter EnterpriseDataProtection CSP sowie in der ausführlichen Artikelserie Schützen von Unternehmensdaten mit Windows Information Protection.

Verwalten von Benutzeraktivitäten

Gilt für: unternehmenseigene Geräte

Auf unternehmenseigenen Geräten führen manche Benutzeraktivitäten zu unnötigen Risiken für Unternehmensdaten. Benutzer können z.B. eine Bildschirmaufnahme von Unternehmensinformationen aus einer internen branchenspezifischen App erstellen. Zur Verringerung dieses Risikos können Sie die Benutzeroberfläche von Windows10 Mobile einschränken, um Unternehmensdaten zu schützen und Datenlecks zu verhindern. Nachfolgend werden diese Möglichkeiten zur Verhinderung von Datenlecks veranschaulicht.

- **Kopieren und Einfügen zulassen** Gibt an, ob Benutzer Inhalte kopieren und einfügen können.
- **Cortana zulassen** Gibt an, ob Benutzer Cortana auf dem Gerät verwenden dürfen (sofern verfügbar).
- **Allow device discovery** Gibt an, ob die Benutzeroberfläche der Geräteerkennung auf dem Sperrbildschirm verfügbar ist. (Damit können Sie beispielsweise steuern, ob ein Gerät einen Projektor [oder ein anderes Gerät] erkennen kann, wenn der Sperrbildschirm angezeigt wird.)
- **Eingabeanpassung zulassen** Gibt an, ob personenbezogene Informationen das Gerät verlassen oder lokal gespeichert werden dürfen (beispielsweise von Cortana gespeicherte Informationen, Freihandeingaben, Diktate).
- **Allow manual MDM unenrollment** Gibt an, ob Benutzer das Unternehmensbereichskonto löschen (d.h. die Registrierung des Geräts beim MDM-System aufheben) dürfen.
- **Bildschirmaufnahme zulassen** Gibt an, ob Benutzer auf dem Gerät Bildschirmaufnahmen erstellen dürfen.
- **Allow SIM error dialog prompt** Gibt an, ob ein Dialogfeld angezeigt werden soll, wenn keine SIM-Karte eingelegt ist.
- **Allow sync my settings** Gibt an, ob die Einstellungen der Benutzerumgebung zwischen Geräten synchronisiert werden sollen. (Funktioniert nur bei Microsoft-Konten.)
- **Allow toasts notifications above lock screen** Gibt an, ob auf dem Sperrbildschirm des Geräts Popupbenachrichtigungen angezeigt werden können.
- **Sprachaufzeichnung zulassen** Gibt an, ob Benutzer Sprachaufzeichnungen erstellen dürfen.
- **Feedbackbenachrichtigungen nicht mehr anzeigen** Verhindert, dass auf Geräten Feedbackfragen von Microsoft angezeigt werden.
- **Allow Task Switcher** Lässt die Aufgabenumschaltung auf dem Gerät zu, um die Sichtbarkeit von Tombstones für App-Bildschirme in der Aufgabenumschaltfunktion zu verhindern.
- **Enable Offline Maps Auto Update** Deaktiviert das automatische Herunterladen und Aktualisieren von Kartendaten.
- **Allow Offline Maps Download Over Metered Connection** Lässt das Herunterladen und Aktualisieren von Kartendaten über getaktete Verbindungen zu.

Weitere Informationen zu Benutzerflächeneinstellungen finden Sie unter „Policy CSP“.

Microsoft Edge

Gilt für: unternehmenseigene und persönliche Geräte

MDM-Systeme ermöglichen auch die Verwaltung von Microsoft Edge auf mobilen Geräten. Microsoft Edge ist der einzige Browser, der auf Windows10 Mobile-Geräten verfügbar ist. Er unterscheidet sich leicht von der Desktopversion, da Flash und Erweiterungen nicht unterstützt werden. Edge ist auch hervorragend als PDF-Anzeige geeignet, da der Browser verwaltet und in Windows Information Protection integriert werden kann.

Die folgenden Einstellungen für Microsoft Edge für Windows10 Mobile können verwaltet werden.

- **Browser zulassen** Gibt an, ob Benutzer Microsoft Edge auf dem Gerät ausführen dürfen.
- **Allow Do Not Track headers** Gibt an, ob DNT-Header (Do Not Track) zulässig sind.
- **Allow InPrivate** Gibt an, ob Benutzer InPrivate-Browsen verwenden können.
- **Kennwort-Manager zulassen** Gibt an, ob Benutzer den Kennwort-Manager zum lokalen Speichern und Verwalten von Kennwörtern verwenden können.
- **Suchvorschläge in der Adressleiste des Browsers zulassen** Gibt an, ob in der Adressleiste Suchvorschläge angezeigt werden.
- **Windows Defender-SmartScreen zulassen** Ob Windows Defender-SmartScreen aktiviert ist
- **Cookies** Gibt an, ob Cookies zulässig sind.
- **Favoriten** Konfigurieren von Favoriten-URLs
- **First Run URL** Die URL, die geöffnet werden soll, wenn ein Benutzer Microsoft Edge zum ersten Mal startet
- **Verhindern, dass die Windows Defender-Bestätigungsaufforderung überschrieben** wird Ob Benutzer die Windows Defender-SmartScreen-Warnungen für URLs außer Kraft setzen können
- **Verhindern der Überschreibung von Smart Screen-Eingabeaufforderungen für Dateien** Ob Benutzer die Windows Defender-SmartScreen-Warnungen für Dateien außer Kraft setzen können

Verwalten

In IT-Umgebungen von Unternehmen muss ein Ausgleich zwischen dem Wunsch, Benutzern stets die neuesten Technologien zur Verfügung zu stellen, und dem Bedarf an Sicherheit und Kostenkontrolle gefunden werden. Da Cyberangriffe inzwischen alltäglich geworden sind, ist es wichtig, den Status Ihrer Windows10 Mobile-Geräte regelmäßig zu überprüfen und zu aktualisieren. Die IT muss die Konfigurationseinstellungen steuern, deren Kompatibilität aufrechterhalten und vorschreiben, welche Geräte auf interne Anwendungen zugreifen dürfen. Windows10 Mobile bietet die notwendigen Verwaltungsfunktionen für mobile Vorgänge, um sicherzustellen, dass die Geräte mit den Richtlinien des Unternehmens in Einklang stehen.

Wartungsoptionen

Ein optimierter Updateprozess

Gilt für: unternehmenseigene und persönliche Geräte

Microsoft hat den Windows-Engineering- und -Freigabezyklus optimiert, sodass neue Features, Umgebungen und Funktionen, die auf dem Markt nachgefragt werden, schneller bereitgestellt werden können als jemals zuvor. Microsoft plant die Bereitstellung von zwei Funktionsupdates pro Jahr (12-Monats-Zeitraum). **Funktionsupdates** eröffnen einen Current Branch (CB) und weisen eine zugeordnete Version auf.

Branch	Version	Datum der Veröffentlichung
Current Branch	1511	November 2015
Current Branch for Business	1511	März 2016
Current Branch	1607	Juli 2016

Microsoft stellt außerdem monatliche Updates für Sicherheit und Stabilität direkt auf Windows10 Mobile-Geräten bereit und installiert diese dort. Diese **Qualitätsupdates**, über Windows Update unter der Kontrolle von

Microsoft veröffentlicht, sind für alle Geräte mit Windows10 Mobile verfügbar. Windows10 Mobile-Geräte nutzen Funktionsupdates und Qualitätsupdates im Rahmen des Standard-Updateprozesses.

Qualitätsupdates sind in der Regel kleiner als Funktionsupdates, der Installationsvorgang ist jedoch sehr ähnlich, wobei größere Updates mehr Zeit für die Installation benötigen. Unternehmenskunden können das Verhalten und den Prozess für Updates auf Windows10 Mobile-Geräten mit einem MDM-System verwalten, nachdem die Geräte auf die Enterprise Edition aktualisiert wurden. In den meisten Fällen gelten die Richtlinien zum Verwalten des Updateprozesses sowohl für Funktions- als auch für Qualitätsupdates.

Microsoft ist bestrebt, die Windows10 Mobile-Geräte aller Kunden automatisch und ohne Unterbrechung des Arbeitsflusses mit den neuesten Updates zu versorgen. Bei der Erstverwendung sucht ein Windows10 Mobile-Gerät automatisch nach verfügbaren Updates. Je nach Netzwerk- und Energiestatus des Geräts können Methode und Zeitpunkt für Updates jedoch variieren.

Netzwerkverbindung	**Beschreibung**	**Automatische Überprüfung**	**Automatisches Herunterladen**	**Automatisches Installieren**	**Automatischer Neustart**
WLAN	Das Gerät ist mit einem persönlichen oder unternehmenseigenen WLAN-Netzwerk verbunden (keine Datengebühren).	Ja	Ja/TD>	Ja	Ja – außerhalb der Nutzungszeit (erzwungener Neustart nach sieben Tagen, wenn der Benutzer den Neustart verschiebt)
Mobilfunk	Das Gerät ist nur mit einem Mobilfunknetz verbunden (Standarddatengebühren fallen an)	Die tägliche Überprüfung wird übersprungen, wenn sie in den letzten fünf Tagen erfolgreich durchgeführt wurde.	Wird nur durchgeführt, wenn das Updatepaket klein ist und das Datenlimit des Mobilfunkanbieters nicht übersteigt.	Ja	s.o.
Mobilfunk – Roaming	Das Gerät ist nur mit einem Mobilfunknetz verbunden und es fallen Roaming-Gebühren an.	Nein	Nein	Nein	s.o.

Verwalten von Updateversionen

Gilt für: unternehmenseigene und persönliche Geräte

Microsoft veröffentlicht in regelmäßigen Abständen neue Funktionsupdates für Windows10 und Windows10 Mobile. Auf der Seite mit Windows10-Versionsinformationen können Sie ermitteln, ob Ihre Geräte bei den Funktions- und Qualitätsupdates von Windows10 auf dem neuesten Stand sind. Die auf dieser Seite veröffentlichten Versionsinformationen gelten sowohl für Windows10 für PCs als auch für Windows10 Mobile. Darüber hinaus erhalten Sie auf der Seite mit dem Windows10-Updateverlauf Informationen zum Zweck dieser Updates.

> **Hinweis:** Damit wir Windows10 Mobile noch besser machen können, laden wir IT-Experten zur Teilnahme am Windows-Insider-Programm ein, um Updates noch vor ihrer offiziellen Veröffentlichung zu testen. Senden Sie

> uns Ihr Feedback über den Feedback-Hub, wenn Sie Probleme feststellen.

Windows as a Service

Gilt für: unternehmenseigene und persönliche Geräte

Microsoft hat eine neue Methode zum direkten Bereitstellen und Installieren von Updates auf Windows10 Mobile-Geräten ohne Genehmigung des Mobilfunkanbieters entwickelt. Da mit dieser Funktion Updates nicht mehr verwaltet werden müssen, um die Sicherheit von Geräten aufrechtzuerhalten, können die Updatebereitstellungen und fortlaufende Verwaltung vereinfacht, mehr Mitarbeiter mit den neuesten Windows-Features versorgt und die Gesamtbetriebskosten für Organisationen gesenkt werden.

Die Verfügbarkeit von Updates ist von der Wartungsoptionen abhängig, die Sie für das Gerät auswählen. Diese Wartungsoptionen werden in der folgenden Tabelle beschrieben:

Wartungsoption	Verfügbarkeit neuer Funktionen zur Installation	Mindestlänge der Wartungslebensdauer	Wichtigste Vorteile	Unterstützte Editionen
Windows-Insider-Builds	Nur für Windows-Insider zugänglich, soweit während des Entwicklungszyklus angemessen	Variabel, bis zur Veröffentlichung des nächsten Insider-Builds für Windows-Insider	Ermöglicht es Insidern, die neue Funktions-und Anwendungskompatibilität zu testen, bevor ein Funktions Update veröffentlicht wird/TD>	Mobile
Current Branch (CB)	Unmittelbar nach der Veröffentlichung des Funktionsupdates auf Windows Update durch Microsoft	Microsoft veröffentlicht in der Regel zwei Funktionsupdates in einem Zeitraum von 12Monaten (etwa alle vier Monate, möglicherweise auch länger).	Stellt Benutzern neue Funktionen so schnell wie möglich zur Verfügung	Mobiles & mobiles Unternehmen
Current Branch for Business (CBB)	Mindestens vier Monate nach der ersten Veröffentlichung des entsprechenden Funktionsupdates auf Windows Update durch Microsoft	Mindestens vier Monate, möglicherweise auch längerNein	Bietet zusätzliche Zeit zum Testen neuer Funktionen vor der Bereitstellung	Nur Mobile Enterprise

Enterprise Edition

Gilt für: unternehmenseigene Geräte

Windows10 Mobile stellt Updates aus Windows Update zwar direkt auf Benutzergeräten bereit, viele Organisationen möchten Updates auf unternehmenseigenen Geräten jedoch nachverfolgen, testen und zeitlich planen. Um diese Anforderungen zu unterstützen, wurde die Windows10 Mobile Enterprise Edition entwickelt.

Das Upgrade auf Windows10 Mobile Enterprise Edition bietet zusätzliche Geräte- und App-Verwaltungsfunktionen für Organisationen, darunter:

- **Das Zurückstellen, Genehmigen und Bereitstellen von Funktions- und Qualitätsupdates:** Windows10 Mobile-Geräte beziehen Updates direkt von Windows Update. Wenn Sie Updates vor der Bereitstellung überprüfen möchten, ist ein Upgrade auf Windows10 Mobile Enterprise Edition erforderlich. Sobald die Enterprise Edition aktiviert ist, kann das Smartphone auf die Wartungsoption Current Branch for Business festgelegt werden, sodass die IT zusätzliche Zeit zum Testen von Updates vor deren Veröffentlichung erhält.

- **Bereitstellung einer unbegrenzten Anzahl selbstsignierter branchenspezifischer Apps auf einem einzelnen Gerät:** Wenn Sie branchenspezifische Apps mithilfe eines MDM-Systems direkt auf Geräten bereitstellen möchten, müssen die Softwarepakete kryptografisch mit einem von der Zertifizierungsstelle (ZS) Ihres Unternehmens generierten Codesignaturzertifikat signiert werden. Sie können maximal 20 selbstsignierte branchenspezifische Apps auf einem Windows10 Mobile-Gerät bereitstellen. Wenn Sie mehr als 20 selbstsignierte branchenspezifische Apps bereitstellen möchten, ist Windows10 Mobile Enterprise erforderlich.
- **Festlegen der Diagnosedatenstufe:** Microsoft erfasst Diagnosedaten, um Windows-Geräte zu schützen und die Qualität von Windows und Microsoft-Diensten zu verbessern. Um die Diagnosedatenstufe so festzulegen, dass nur die zum Schutz von Geräten erforderlichen Diagnosedaten erfasst werden, ist ein Upgrade auf Windows10 Mobile Enterprise Edition erforderlich.

Weitere Informationen zu Diagnosedaten finden Sie unter Konfigurieren von Windows-Diagnosedaten in Ihrer Organisation.

Verwenden Sie zum Aktivieren von Windows10 Mobile Enterprise Ihr MDM-System oder ein Bereitstellungspaket, um die Windows10 Enterprise-Lizenz auf einem Windows10 Mobile-Gerät einzufügen. Lizenzen können aus dem Portal zur Volumenlizenzierung abgerufen werden. Für Testzwecke können Sie eine Lizenzdatei aus dem MSDN Download Center abrufen. Ein gültiges MSDN-Abonnement ist erforderlich.

Informationen zum Aktualisieren eines Geräts auf die Enterprise Edition finden Sie unter WindowsLicensing CSP

> **Empfehlung:** Microsoft empfiehlt die Verwendung der Enterprise Edition nur auf Unternehmensgeräten. Nach dem Upgrade eines Geräts ist ein Downgrade nicht mehr möglich. Auch bei einem Zurücksetzen oder Löschen des Geräts wird die Enterprise-Lizenz von persönlichen Geräten nicht entfernt.

Zurückstellen und Genehmigen von Updates mit MDM

Gilt für: unternehmenseigene Geräte mit Enterprise Edition

Nach dem Upgrade von Geräten auf die Windows10 Mobile Enterprise Edition können Sie Geräte, die Updates von Windows Update (oder Windows Update for Business) erhalten, mit einer Reihe von Updaterichtlinien verwalten.

Zur Steuerung von Funktionsupdates müssen Sie für Ihre Geräte die Wartungsoption Current Branch for Business (CBB) aktivieren. Ein Gerät mit CBB-Abonnement wartet bis zur Veröffentlichung des nächsten CBB durch Microsoft Update. Während das Gerät bei Funktionsupdates bis zum nächsten CBB wartet, erhält es weiterhin Qualitätsupdates.

Zum Steuern der monatlichen Qualitätsupdates müssen zusätzliche Zurückstellungsrichtlinien auf den gewünschten Zurückstellungszeitraum festgelegt werden. Wenn Qualitätsupdates für Ihre Windows10 Mobile-Geräte über Windows Update verfügbar sind, werden diese Updates erst nach Ablauf des Zurückstellungszeitraums installiert. Dadurch erhalten IT-Experten Zeit zum Testen der Auswirkungen der Updates auf Geräte und Apps.

Vor der Verteilung und Installation von Updates können Sie diese auf Probleme oder Anwendungskompatibilität testen. IT-Experten können festlegen, dass Updates genehmigt werden müssen. Dadurch kann der MDM-Administrator bestimmte Updates für die Installation auf einem Gerät auswählen und genehmigen und den Endbenutzer-Lizenzvertrag für das Update im Namen des Benutzers annehmen. Bitte beachten Sie, dass auf Windows10 Mobile alle Updates als „Betriebssystemupdates“ und niemals als einzelne Patches verpackt sind.

Sie können festlegen, dass Qualitäts- und Funktionsupdates auf die gleiche Art behandelt werden und dass nicht bis zur Veröffentlichung des nächsten CBB für Ihre Geräte gewartet wird. Dadurch wird die Veröffentlichung von Updates mithilfe des gleichen Verfahrens zur Genehmigung und Veröffentlichung vereinfacht. Sie können für jeden Updatetyp verschiedene Zurückstellungszeiträume anwenden. In Version 1607 wurden von Microsoft zusätzliche Richtlinieneinstellungen hinzugefügt, um eine detailliertere Kontrolle über Updates zu ermöglichen.

Nachdem Updates auf Ihren Geräten bereitgestellt wurden, können Sie die Einführung der Updates auf Unternehmensgeräten unterbrechen. Nach dem Starten der Einführung eines Qualitätsupdate sind beispielsweise einige Telefonmodelle in ihrer Funktion beeinträchtigt, oder Benutzer melden, dass eine bestimmte branchenspezifische App keine Verbindung herstellen und eine Datenbank nicht aktualisiert werden kann. Es können Probleme auftreten, die bei ersten Tests nicht erkannt wurden. IT-Experten können Updates unterbrechen, um unerwartete Probleme zu untersuchen und zu beheben.

In der folgenden Tabelle sind die anwendbaren Richtlinieneinstellungen für Updates nach Windows10 Mobile-Version zusammengefasst. Alle Richtlinieneinstellungen sind abwärtskompatibel und werden in zukünftigen Funktionsupdates beibehalten. In der Dokumentation zu Ihrem MDM-System finden Sie Informationen zur Unterstützung dieser Einstellungen in Ihrem MDM-System.

Aktivität (Richtlinie)	Einstellungen für Version 1511	Einstellungen für Version 1607
CBB für das Gerät abonnieren, um Funktionsupdates zurückzustellen	RequireDeferUpgrade Stellt das Funktionsupdate bis zur nächsten CBB-Veröffentlichung zurück. Das Gerät erhält Qualitätsupdates vom Current Branch for Business (CBB). Das Funktionsupdate wird bis mindestens vier Monate nach Veröffentlichung des Current Branch zurückgestellt.	BranchReadinessLevel Stellt das Funktionsupdate bis zur nächsten CBB-Veröffentlichung zurück. Das Gerät erhält Qualitätsupdates vom Current Branch for Business (CBB). Das Funktionsupdate wird bis mindestens vier Monate nach Veröffentlichung des Current Branch zurückgestellt.
Zurückstellen von Updates	DeferUpdatePeriod Zurückstellen von Qualitätsupdates für vier Wochen bzw. 28Tage	DeferQualityUpdatePeriodInDays Zurückstellen von Funktions- und Qualitätsupdates für bis zu 30Tage
Genehmigen von Updates	RequireUpdateApproval	RequireUpdateApproval
Unterbrechen der Einführung eines Updates, nachdem ein genehmigtes Update bereitgestellt wurde	PauseDeferrals Unterbrechen von Funktionsupdates für bis zu 35Tage	PauseQualityUpdates Unterbrechen von Funktionsupdates für bis zu 35Tage

Verwalten des Update-Verhaltens

Gilt für: unternehmenseigene Geräte mit Enterprise Edition

Legen Sie das Verhalten des Update-Clients für Ihre Mitarbeiter mit der Allowautomaticupdate-Richtlinie fest. Dadurch können IT-Spezialisten das Verhalten des Update-Clients auf Geräten in Bezug auf das Suchen, Herunterladen und Installieren von Updates beeinflussen.

Dazu zählt Folgendes:

- Das Benachrichtigen von Benutzern über das Herunterladen von Updates
- Das automatische Herunterladen von Updates und das Auffordern des Benutzers, einen Neustart zu planen. (Dies ist das Standardverhalten, wenn diese Richtlinie nicht konfiguriert ist.)
- Das automatische Herunterladen und erneute Starten von Geräten mit Benutzerbenachrichtigung
- Das automatische Herunterladen und erneute Starten von Geräten zu einem bestimmten Zeitpunkt
- Das automatische Herunterladen und erneute Starten von Geräten ohne Benutzereingriff
- Das Deaktivieren automatischer Updates Diese Option sollte nur zur Erfüllung gesetzlicher Auflagen für Systeme verwendet werden. Das Gerät erhält keine Updates.

In Version 1607 können Sie darüber hinaus konfigurieren, wann das Update auf dem Mitarbeitergerät installiert wird, um sicherzustellen, dass Updateinstallationen oder Neustarts nicht die Produktivität des Unternehmens oder Mitarbeiters beeinträchtigen. Updateinstallationen und Neustarts können für außerhalb der Nutzungszeit (unterstützte Werte sind 0 bis 23, wobei 0 für 0:00Uhr steht, 1 für 1:00Uhr usw.) oder für einen bestimmten

Wochentag (unterstützte Werte sind 0 bis 7, wobei 0 für alle Tage steht, 1 für Sonntag, 2 für Montag usw.) geplant werden.

Verwalten der Quelle von Updates mit MDM

Gilt für: unternehmenseigene Geräte mit Enterprise Edition

IT-Administratoren können unter Windows10Enterprise die Installation neuer Updates über Windows Update zurückstellen, Unternehmen benötigen jedoch möglicherweise zusätzliche Kontrolle über Update-Prozesse. Aus diesem Grund wurde Windows Update for Business von Microsoft entwickelt. Microsoft hat Windows Update for Business entwickelt, um IT-Administratoren weitere Verwaltungsfunktionen rund um Windows Update bereitzustellen, wie beispielsweise die Möglichkeit, Updates für Gruppen von Geräten bereitzustellen oder Wartungszeitfenster für die Installation von Updates festzulegen. Wenn Sie ein MDM-System verwenden, ist die Verwendung von Windows Update for Business nicht erforderlich, da Sie diese Features über Ihr MDM-System verwalten können.

Informationen zu Windows Update for Business

IT-Administratoren können mit AllowUpdateService angeben, woher das Gerät Updates bezieht. Dabei kann es sich um Microsoft Update, Windows Update for Business oder Windows Server Update Services (WSUS) handeln.

Verwalten von Updates mit Windows Update-Server

Gilt für: unternehmenseigene Geräte mit Enterprise Edition

Legen Sie bei Verwendung von WSUS die Option **UpdateServiceUrl** fest, damit das Gerät nach Updates von einem WSUS-Server anstatt von Windows Update sucht. Dies ist hilfreich für lokale MDMs, die Geräte aktualisieren müssen, die keine Verbindung zum Internet herstellen können, normalerweise Handheld-Geräte zur Durchführung von Aufgaben oder andere Windows IoT-Geräte.

Informationen zum Verwalten von Updates mit Windows Server Update Services (WSUS)

Abfragen des Updatestatus von Geräten

Gilt für: unternehmenseigene und persönliche Geräte

MDM-Administratoren können nicht nur konfigurieren, wie Windows10 Mobile Enterprise Updates erhalten soll, sondern auch Updateinformationen von Windows10 Mobile-Geräten abrufen, sodass der Updatestatus anhand einer Liste genehmigter Updates überprüft werden kann.

Bei dieser Statusabfrage für Geräteupdates wird eine Übersicht mit folgenden Informationen bereitgestellt:

- Installierte Updates: eine Liste mit den auf dem Gerät installierten Updates
- Installierbare Updates: eine Liste mit Updates, die zur Installation bereitstehen
- Fehlgeschlagene Updates: eine Liste mit Updates, die während der Installation fehlgeschlagen sind, einschließlich der Fehlerursache
- Ausstehender Neustart: eine Liste mit Updates, deren Installation erst nach einem Neustart abgeschlossen werden kann
- Zeitpunkt der letzten erfolgreichen Überprüfung: der letzte Zeitpunkt, zu dem eine erfolgreiche Überprüfung durchgeführt wurde
- Upgrade zurückstellen: Gibt an, ob das Upgrade bis zum nächsten Updatezyklus verzögert wird.

Geräteintegrität

Gilt für: unternehmenseigene und persönliche Geräte

Der Integritätsnachweis für Geräte ist eine weitere neue Schutzmaßnahme in Windows10 Mobile. Damit können per Remotezugriff Geräte erkannt werden, die eine mangelhafte Sicherheitskonfiguration oder Schwachstellen

aufweisen, durch die sie ein leichtes Ziel von Angriffen werden.

Windows10 Mobile erleichtert die Integration mit Microsoft Intune oder MDM-Lösungen von Drittanbietern, indem ein allgemeiner Überblick über Zustand und Kompatibilität von Geräten bereitgestellt wird. Mit der Kombination dieser Lösungen können Sie Jailbreak-Geräte erkennen, die Gerätekompatibilität überwachen, Kompatibilitätsberichte erstellen, Benutzer oder Administratoren über Probleme benachrichtigen, Gegenmaßnahmen ergreifen und den bedingten Zugriff auf Ressourcen wie Office365 oder VPN verwalten.

Die erste Version des Integritätsnachweises für Geräte wurde im Juni2015 für Windows10-Geräte veröffentlicht, die TPM2.0 unterstützen und in einer cloudbasierten Unternehmenstopologie ausgeführt werden. In der Jubiläumsversion von Windows10 werden die Funktionen des Integritätsnachweises auf ältere Geräte ausgedehnt, die TPM1.2 sowie Hybrid- und lokale Umgebungen unterstützen und die Zugriff auf das Internet haben oder in Air Gap-Netzwerken ausgeführt werden.

Der Integritätsnachweis basiert auf OMA-Standards (Open Mobile Alliance). IT-Manager können den Integritätsnachweis zur Überprüfung von Geräten verwenden, die Folgendes erfüllen:

- Auf dem Gerät wird das Windows10-Betriebssystem ausgeführt (Smartphone oder PC).
- TPM (Trusted Module Platform) 1.2 und 2.0 wird im eigenständigen oder Firmware-Format unterstützt.
- Das Gerät wird durch eine Geräteverwaltungslösung verwaltet, die Integritätsnachweise unterstützt (Intune oder Drittanbieter-MDM).
- Das Gerät wird in Cloud-, Hybrid-, lokalen und BYOD-Szenarien ausgeführt.

Geräteverwaltungslösungen mit Unterstützung für Integritätsnachweise bieten IT-Managern die Möglichkeit, eine einheitliche Sicherheitsbarriere auf allen verwalteten Windows10 Mobile-Geräten zu erstellen. Dadurch erhalten IT-Manager folgende Möglichkeiten:

- Remote-Erfassung von zertifizierten Daten (äußerst sicher)
- Überwachen der Kompatibilität der Geräteintegrität und Erkennen von Geräten mit Schwachstellen, die Ziele von Angriffen sein könnten
- Ergreifen von Maßnahmen für potenziell gefährdete Geräte, z.B.:
- Remote-Auslösung von Gegenmaßnahmen, sodass auf das entsprechende Gerät nicht mehr zugegriffen werden kann (Sperren, Zurücksetzen oder Löschen des Geräts)
- Verhindern des Gerätezugriffs auf wertvolle Ressourcen (bedingter Zugriff)
- Auslösen weiterer Untersuchungen und Überwachungsmaßnahmen (Weiterleiten des Geräts zu einem Honeypot für eine weitere Überwachung)
- Benachrichtigen des Benutzers oder Administrators über die Notwendigkeit der Problembehebung

> **Hinweis:** Der Integritätsnachweisdienst für Windows-Geräte kann für Szenarien mit bedingtem Zugriff verwendet werden, die durch MDM-Lösungen (z.B. Microsoft Intune) und andere Arten von separat erhältlichen Verwaltungssystemen (z.B. SCCM) ermöglicht werden.

Weitere Informationen zum Integritätsnachweis unter Windows 10 Mobile finden Sie im Sicherheitshandbuch für Windows 10 Mobile.

Hierbei handelt es sich um eine Liste von Attributen, die von DHA unterstützt werden und die oben genannten korrigierenden Aktionen auslösen können.

- **Attestation Identity Key (AIK) present** Gibt an, dass ein AIK vorhanden ist. (Das Gerät ist also vertrauenswürdiger als ein Gerät ohne AIK.)
- **Data Execution Prevention (DEP) enabled** Gibt an, ob für das Gerät eine DEP-Richtlinie aktiviert ist, die angibt, dass das Gerät vertrauenswürdiger ist als ein Gerät ohne DEP-Richtlinie.
- **BitLocker-Status** BitLocker schützt den Speicher auf dem Gerät. Ein Gerät mit BitLocker ist vertrauenswürdiger als ein Gerät ohne BitLocker.

- **Sicherer Start aktiviert** Gibt an, ob auf dem Gerät „Sicherer Start" aktiviert ist. Ein Gerät, auf dem „Sicherer Start" aktiviert ist, ist vertrauenswürdiger als ein Gerät ohne „Sicherer Start". Auf Geräten unter Windows 10 Mobile ist „Sicherer Start" immer aktiviert.
- **Codeintegrität aktiviert** Gibt an, ob die Codeintegrität eines Laufwerks oder einer Systemdatei bei jedem Laden in den Arbeitsspeicher überprüft wird. Ein Gerät mit aktivierter Codeintegrität ist vertrauenswürdiger als ein Gerät ohne Codeintegrität.
- **Abgesicherter Modus** Gibt an, ob Windows im abgesicherten Modus ausgeführt wird. Ein Gerät, auf dem Windows im abgesicherten Modus ausgeführt wird, ist weniger vertrauenswürdig als ein Gerät, auf dem Windows im Standardmodus ausgeführt wird.
- **Boot debug enabled** Gibt an, ob auf dem Gerät der Startdebugger aktiviert ist. Ein Gerät mit aktiviertem Startdebugger ist weniger sicher (vertrauenswürdig) als ein Gerät ohne aktivierten Startdebugger.
- **OS kernel debugging enabled** Gibt an, ob auf dem Gerät das Betriebssystem-Kerneldebugging aktiviert ist. Ein Gerät mit aktiviertem Betriebssystem-Kerneldebugging ist weniger sicher (vertrauenswürdig) als ein Gerät mit deaktiviertem Betriebssystem-Kerneldebugging.
- **Test signing enabled** Gibt an, ob die Testsignierung deaktiviert ist. Ein Gerät mit deaktivierter Testsignierung ist vertrauenswürdiger als ein Gerät mit aktivierter Testsignierung.
- **Start-Manager-Version** Die Version des auf dem Gerät ausgeführten Start-Managers. Der HAS kann diese Version überprüfen, um zu ermitteln, ob der neueste Start-Manager ausgeführt wird, was die Sicherheit (Vertrauenswürdigkeit) erhöht.
- **Code integrity version** Gibt die Version des Codes an, von dem während der Startsequenz Integritätstests durchgeführt werden. Der HAS kann diese Version überprüfen, um zu ermitteln, ob die neueste Codeversion ausgeführt wird, was die Sicherheit (Vertrauenswürdigkeit) erhöht.
- **Secure Boot Configuration Policy (SBCP) present** Gibt an, ob der Hash der benutzerdefinierten SBCP vorhanden ist. Ein Gerät mit einem SBCP-Hash ist vertrauenswürdiger als ein Gerät ohne SBCP-Hash.
- **Boot cycle whitelist** Die Ansicht der Hostplattform zwischen Startzyklen gemäß Herstellerdefinition im Vergleich zu einer veröffentlichten Positivliste. Ein Gerät, das der Positivliste entspricht, ist vertrauenswürdiger (sicherer) als ein nicht konformes Gerät.

Beispielszenarien

Windows10 Mobile verfügt über Schutzmaßnahmen, die zusammenarbeiten und sich mit Microsoft Intune oder MDM-Lösungen von Drittanbietern integrieren lassen. IT-Administratoren können die Kompatibilität überwachen, um anhand der in die Gerätehardware eingebundenen Sicherheit und Vertrauenswürdigkeit sicherzustellen, dass Unternehmensressourcen vollständig geschützt sind.

Folgendes geschieht beim Einschalten eines Smartphones:

1. Das Feature „Sicherer Start" von Windows10 schützt die Startsequenz, ermöglicht dem Gerät das Starten in einer definierten und vertrauenswürdigen Konfiguration und lädt ein Startladeprogramm, dem der Hersteller vertraut.
2. Der vertrauenswürdige Start von Windows10 übernimmt die Kontrolle, überprüft die digitale Signatur des Windows-Kernels, und die Komponenten werden während des Windows-Startvorgangs geladen und ausgeführt.
3. Parallel zu den Schritten1 und 2 wird das Windows10 Mobile-TPM (Trusted Platform Module – kontrollierter Start) unabhängig in einer hardwaregeschützten Sicherheitszone ausgeführt (d.h. isoliert vom Ausführungspfad, der Startaktivitäten überwacht), um ein integres und manipulationssicheres Überwachungsprotokoll zu erstellen, das mit einem geheimen Schlüssel signiert wird, auf den nur das TPM zugreifen kann.
4. Geräte, die von einer MDM-Lösung mit Unterstützung für Integritätsnachweise verwaltet werden, senden eine Kopie dieses Überwachungsprotokolls über einen geschützten und manipulationssicheren Kommunikationskanal an den Microsoft-Integritätsnachweisdienst (Health Attestation Service, HAS).
5. Microsoft HAS überprüft die Überwachungsprotokolle, stellt einen verschlüsselten und signierten Bericht aus

und leitet diesen an das Gerät weiter.

6. IT-Manager können den Bericht mithilfe einer MDM-Lösung mit Unterstützung für Integritätsnachweise in einem geschützten, manipulationssicheren Kommunikationskanal anzeigen. Sie können bewerten, ob ein Gerät in einem kompatiblen (integren) Zustand ausgeführt wird, Zugriff gewähren oder Korrekturmaßnahmen gemäß Sicherheitsanforderungen und Unternehmensrichtlinien auslösen.

Bestandsberichte

Gilt für: unternehmenseigene Geräte mit Enterprise Edition

Mit dem Gerätebestand können Organisationen ihre Geräteverwaltung verbessern, da ihnen nun ausführliche Informationen zu den Geräten zur Verfügung stehen. MDM-Systeme sammeln per Remotezugriff Bestandsinformationen, und mithilfe der Berichtsfunktionen des Systems können Sie Geräteressourcen und Informationen analysieren. Diese Daten informieren die IT über aktuelle Hardware- und Softwareressourcen des Geräts (z.B. installierte Updates).

Nachfolgend sind Beispiele für die von einem Gerätebestand bereitgestellten Software- und Hardwareinformationen unter Windows10 Mobile aufgeführt. Neben diesen Informationen kann das MDM-System jegliche der in diesem Handbuch beschriebenen Konfigurationseinstellungen lesen.

- **Installed enterprise apps** Eine Liste mit den auf dem Gerät installierten Unternehmens-Apps
- **Gerätename** Der für das Gerät konfigurierte Gerätename
- **Firmwareversion** Die Version der auf dem Gerät installierten Firmware
- **Betriebssystemversion** Die Version des auf dem Gerät installierten Betriebssystems
- **Device local time** Die lokale Zeit auf dem Gerät
- **Prozessortyp** Der Prozessortyp des Geräts
- **Gerätemodell** Das Modell des Geräts gemäß Herstellerdefinition
- **Gerätehersteller** Der Hersteller des Geräts
- **Device processor architecture** Die Prozessorarchitektur des Geräts
- **Gerätesprache** Die auf dem Gerät verwendete Sprache
- **Telefonnummer** Die dem Gerät zugewiesene Telefonnummer
- **Roaming status** Gibt an, ob das Gerät über eine Roaming-Mobilfunkverbindung verfügt.
- **International Mobile Equipment Identity (IMEI) und International Mobile Subscriber Identity (IMSI) – Eindeutige IDs für die Mobilfunkverbindung des Smartphones. GSM-Netzwerke (Global System for Mobile Communications) identifizieren gültige Geräte mithilfe der IMEI, und alle Mobilfunknetze identifizieren das Gerät und den Benutzer anhand der IMSI.
- **Wi-Fi IP address** IPv4- und IPv6-Adressen, die derzeit dem WLAN-Adapter des Geräts zugewiesen sind
- **Wi-Fi media access control (MAC) address** MAC-Adresse, die derzeit dem WLAN-Adapter des Geräts zugewiesen ist
- **Wi-Fi DNS suffix and subnet mask** DNS-Suffix und IP-Subnetzmaske, die dem WLAN-Adapter des Geräts zugewiesen sind
- **Sicherer Startzustand** Gibt an, ob „Sicherer Start" aktiviert ist.
- **Enterprise encryption policy compliance** Gibt an, ob das Gerät verschlüsselt ist.

Verwalten von Diagnosedaten

Betrifft: Unternehmenseigene Geräte mit Windows10 Mobile Enterprise Edition

Microsoft verwendet Diagnose-, Leistungs- und Nutzungsdaten von Windows-Geräten, um fundierte Entscheidungen zu treffen und die robusteste und leistungsfähigste Plattform für Ihr Unternehmen und die Personen bereitzustellen, die auf Windows setzen, um bei ihrer Arbeit ein Höchstmaß an Produktivität zu erreichen. Diagnosedaten tragen dazu bei, Windows-Geräte in einem einwandfreien Zustand zu halten, das Betriebssystem zu verbessern sowie Features und Dienste zu personalisieren.

Sie können den Umfang der von Diagnosedatensystemen gesammelten Daten steuern. Geben Sie zum

Konfigurieren der Geräte in der Einstellung „Telemetrie zulassen" mit Ihrem MDM-System eine dieser Stufen an.

Weitere Informationen finden Sie unter Konfigurieren von Windows-Diagnosedaten in Ihrer Organisation.

> **Hinweis:** Diagnosedaten können nur verwaltet werden, wenn das Gerät auf die Windows 10 Mobile Enterprise Edition aktualisiert wird.

Remoteunterstützung

Gilt für: unternehmenseigene und persönliche Geräte

Die Remoteunterstützungsfeatures unter Windows 10 Mobile helfen beim Beheben möglicher Benutzerprobleme, auch wenn der Helpdesk keinen physischen Zugriff auf das Gerät hat. Verfügbare Features:

- **Remotesperre** Supportmitarbeiter können ein Gerät per Remotezugriff sperren. Dies kann hilfreich sein, wenn ein Benutzer sein mobiles Gerät verliert und später wiederbeschaffen kann (beispielsweise, wenn er es bei einem Kunden vergessen hat).
- **Remote PIN reset** Supportmitarbeiter können die PIN per Remotezugriff zurücksetzen, wenn Benutzer ihre PIN vergessen und nicht auf ihr Gerät zugreifen können. Dabei gehen keine Unternehmens- oder Benutzerdaten verloren, und Benutzer können schnell wieder auf ihr Gerät zugreifen.
- **Remote ring** Supportmitarbeiter können Geräte per Remotezugriff klingeln lassen. Dadurch können Benutzer, die ihr Gerät verlegt haben, bei der Suche unterstützt werden. Und in Kombination mit der Remotesperrung kann sichergestellt werden, dass nicht autorisierte Benutzer, die das Gerät finden, nicht auf das Gerät zugreifen können.
- **Remote find** Supportmitarbeiter können per Remotezugriff die Position eines Geräts auf einer Karte anzeigen, um den geografischen Standort des Geräts zu ermitteln. Die Parameter für die Remotesuche können über die Telefoneinstellungen konfiguriert werden (siehe Tabelle weiter unten). Bei der Remotesuche werden der aktuelle Längen- und Breitengrad sowie die Höhe des Geräts zurückgegeben.

Richtlinien für die Remoteunterstützung

- **Desired location accuracy** Die gewünschte Genauigkeit als Radiuswert zwischen einem Meter und 1.000 Metern
- **Maximum remote find** Der maximale Zeitraum in Minuten, in dem der Server eine erfolgreiche Remotesuche akzeptiert. Der Wert muss zwischen 0 und 1.000 Minuten liegen.
- **Remote find timeout** Die Anzahl von Sekunden, die Geräte auf den Abschluss einer Remotesuche warten sollen. Der Wert muss zwischen 0 und 1.800 Sekunden liegen.

Mit diesen Remoteverwaltungsfeatures können Organisationen den für die Geräteverwaltung erforderlichen IT-Aufwand verringern. Außerdem können Benutzer, die ihr Gerät verlegt oder das Gerätekennwort vergessen haben, ihr Gerät schnell wieder verwenden.

> **Remoteüberwachungssoftware** Microsoft stellt keine integrierte Remoteüberwachungssoftware bereit, arbeitet jedoch mit Partnern zusammen, um diese Funktionen und Dienste anzubieten. Mit Version 1607 sind Apps zur Remoteunterstützung und -überwachung im Microsoft Store verfügbar.

Ausmustern

Gilt für: unternehmenseigene und persönliche Geräte

Die Ausmusterung ist die letzte Phase des Gerätelebenszyklus, der in der heutigen Geschäftsumgebung im Durchschnitt etwa 18Monate beträgt. Nach Ablauf dieses Zeitraums möchten Mitarbeiter in den Genuss der Produktivitäts- und Leistungssteigerungen der neuesten Hardware kommen. Geräte, die durch neuere Modelle ersetzt werden, müssen unbedingt sicher ausgemustert werden, da keine vertraulichen Unternehmensdaten auf entsorgten Geräten zurückbleiben dürfen. Bei unternehmenseigenen Geräten ist dies in der Regel kein Problem,

bei persönlichen Geräten kann dies jedoch eine Herausforderung darstellen. Sie müssen in der Lage sein, alle Unternehmensdaten selektiv zu entfernen, ohne persönliche Apps und Daten auf dem Gerät zu beeinträchtigen. Die IT erfordert auch eine Möglichkeit, Benutzer beim Zurücksetzen von gestohlenen oder verloren gegangenen Geräten angemessen zu unterstützen.

Windows10 Mobile unterstützt die Ausmusterung von persönlichen und unternehmenseigenen Geräten, sodass die IT sicher sein kann, dass Unternehmensdaten vertraulich bleiben und die Privatsphäre von Benutzern geschützt wird.

> **Hinweis:** All diese MDM-Funktionen stehen zusätzlich zu den Software- und Hardwarezurücksetzungsfeatures des Geräts zur Verfügung, mit denen Mitarbeiter Geräte auf die Werkseinstellungen zurücksetzen können.

Persönliche Geräte: Windows10 Mobile unterstützt die Anforderungen von US-Behörden für einen „Kill Switch" für den Fall, dass das Smartphone verloren geht oder gestohlen wird. Der Rücksetzschutz ist ein kostenloser Dienst auf account.microsoft.com, der sicherstellt, dass das Smartphone nicht einfach zurückgesetzt und wiederverwendet werden kann. Zur Aktivierung des **Rücksetzschutzes** müssen Sie sich lediglich mit Ihrem Microsoft-Konto anmelden und die empfohlenen Einstellungen übernehmen. Die manuelle Aktivierung können Sie unter „Einstellungen > Updates und Sicherheit > Mein Handy finden" durchführen. Zu diesem Zeitpunkt ist der Rücksetzschutz nur mit einem Microsoft-Konto und nicht mit einem Azure AD-Konto verfügbar. Außerdem ist er nicht außerhalb der USA verfügbar.

Wenn Sie ein Gerät vollständig zurücksetzen möchten, falls das Gerät verloren geht oder ein Mitarbeiter das Unternehmen verlässt, muss die Zustimmung des Benutzers eingeholt werden, und regionale Gesetze zum Schutz der persönlichen Daten des Benutzers müssen eingehalten werden.

Eine bessere Lösung als das Zurücksetzen des gesamten Geräts ist die Verwendung von Windows Information Protection, um nur unternehmenseigene Daten von einem persönlichen Gerät zu entfernen. Wie im Kapitel „Apps" erläutert, werden alle Unternehmensdaten entsprechend gekennzeichnet. Wenn die Registrierung des Geräts im MDM-System Ihrer Wahl aufgehoben wird, werden alle verschlüsselten Unternehmensdaten, Apps, Einstellungen und Profile unmittelbar vom Gerät entfernt, ohne die vorhandenen persönlichen Daten des Mitarbeiters zu beeinträchtigen. Ein Benutzer kann die Aufhebung der Registrierung über den Einstellungsbildschirm initiieren, oder die Aufhebung kann über die MDM-Verwaltungskonsole durch die IT erfolgen. Die Aufhebung der Registrierung ist ein Verwaltungsereignis, das dem MDM-System gemeldet wird.

Unternehmens Gerät: Sie können den Verschlüsselungsschlüssel des Benutzers bei einem Geräte diebstahlsicher ablaufen lassen, aber denken Sie daran, dass auch die verschlüsselten Daten auf anderen Windows-Geräten für den Benutzer unlesbar sind. Eine bessere Methode zum Ausmustern eines veralteten oder verloren gegangenen Geräts ist die vollständige Zurücksetzung des Geräts. Das Helpdesk oder der Benutzer des Geräts kann die vollständige Zurücksetzung initiieren. Wenn die Zurücksetzung abgeschlossen ist, versetzt Windows10 Mobile das Gerät in einen einwandfreien Zustand und beginnt mit dem OOBE-Prozess.

Einstellungen für die Ausmusterung persönlicher oder unternehmenseigener Geräte

- **Allow manual MDM unenrollment** Gibt an, ob Benutzer das Unternehmensbereichskonto löschen (d.h. die Registrierung des Geräts beim MDM-System aufheben) dürfen.
- **Allow user to reset phone** Gibt an, ob Benutzer das Gerät über die Einstellungen oder mithilfe von Hardwaretastenkombinationen auf die Werkseinstellungen zurücksetzen dürfen.

Verwandte Themen

- Mobile Geräteverwaltung
- Enterprise Mobility + Security
- Übersicht über die mobile Geräteverwaltung für Office365

- Microsoft Store für Unternehmen

Revisionen

- November2015 Aktualisiert für Windows10 Mobile (Version 1511)
- August 2016 Aktualisiert für Windows10 Mobile Anniversary Update (Version 1607)

Windows-Bibliotheken

08.08.2019 • 6 minutes to read

Gilt für: Windows 10, Windows 8,1, Windows 7, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

Bibliotheken sind virtuelle Container für Benutzerinhalte. Eine Bibliothek kann auf dem lokalen Computer oder in einem entfernten Speicherort gespeicherte Dateien und Ordner enthalten. In Windows-Explorer interagieren Benutzer mit Bibliotheken auf ähnliche Weise wie die Interaktion mit anderen Ordnern. Bibliotheken basieren auf den bekannten Legacy Ordnern (wie "eigene Dateien", "meine Bilder" und "meine Musik"), mit denen die Benutzer vertraut sind, und diese bekannten Ordner werden automatisch in die Standardbibliotheken aufgenommen und als Standardspeicherort festgesetzt.

Features für Benutzer

Windows-Bibliotheken werden durch vollständige Inhaltssuche und umfassende Metadaten gesichert. Bibliotheken bieten Benutzern die folgenden Vorteile:

- Aggregieren von Inhalten aus mehreren Speicherorten in einer einzelnen, einheitlichen Präsentation
- Ermöglichen Sie Benutzern das Stapeln und Gruppieren von bibliotheksinhalten auf der Grundlage von Metadaten.
- Aktivieren Sie die Schnelle Volltextsuche an mehreren Speicherorten, über den Windows-Explorer oder über das Startmenü.
- Unterstützen Sie angepasste Filter Suchvorschläge basierend auf den Dateitypen, die in der Bibliothek enthalten sind.
- Ermöglichen Sie Benutzern das Erstellen neuer Bibliotheken, und geben Sie an, welche Ordner Sie hinzufügen möchten.

Features für Administratoren

Administratoren können Windows-Bibliotheken wie folgt konfigurieren und Steuern:

- Erstellen Sie benutzerdefinierte Bibliotheken, indem Sie Bibliotheks Beschreibungsdateien (*. Library-MS) erstellen und bereitstellen.
- Blenden Sie die Standardbibliotheken aus, oder löschen Sie Sie. (Der Bibliotheksknoten selbst kann nicht im Navigationsbereich von Windows Explorer ausgeblendet oder gelöscht werden.)
- Geben Sie einen Satz von Bibliotheken an, die für Standardbenutzer verfügbar sind, und stellen Sie diese Bibliotheken dann für Benutzer bereit, die vom Standardbenutzer abgeleitet sind.
- Geben Sie die Speicherorte an, die in eine Bibliothek einbezogen werden sollen.
- Entfernen eines Standardspeicherorts aus einer Bibliothek
- Entfernen Sie erweiterte Bibliotheksfeatures, wenn die Umgebung die lokale Zwischenspeicherung von Dateien nicht unterstützt, indem Sie die Windows-Bibliotheksfeatures deaktivieren, die von der Gruppenrichtlinie für indizierte Dateidaten abhängig sind. Dadurch werden alle Bibliotheken Basic (siehe Indizierungs Anforderungen und grundlegende Bibliotheken), Bibliotheken aus dem Bereich der Start Menü Suche entfernt und andere Features entfernt, um Benutzer zu verwirren und Ressourcen zu verbrauchen.

Weitere Informationen zu Bibliotheken

Im folgenden sind wichtige Informationen zu Bibliotheken zu sehen, die Sie möglicherweise verstehen müssen,

um Ihr Unternehmen erfolgreich zu verwalten.

Bibliotheksinhalte

Wenn Sie einen Ordner in einer Bibliothek einfügen, wird der Speicherort der Dateien oder Ordner nicht physisch verschoben oder geändert; die Bibliothek ist eine Ansicht in diesen Ordnern. Benutzer, die mit Dateien in einer Bibliothek interagieren, kopieren, verschieben und löschen jedoch die Dateien selbst, keine Kopien dieser Dateien.

Standardbibliotheken und bekannte Ordner

Zu den Standardbibliotheken gehören:

- Dokumente
- Musik
- Bilder
- Videos

Bibliotheken sind auf den bekannten Legacy Ordnern (wie "eigene Dateien", "meine Bilder" und "meine Musik") aufgebaut, mit denen die Benutzer vertraut sind. Diese bekannten Ordner werden automatisch in die Standardbibliotheken aufgenommen und als Standardspeicherort für den Speicherort angegeben. Das heißt, wenn Benutzer eine Datei in die Dokumentbibliothek ziehen, kopieren oder speichern, wird die Datei in den Ordner "eigene Dateien" verschoben, kopiert oder gespeichert. Administratoren und Benutzer können den Standardspeicherort für Save-to ändern.

Ausblenden von Standardbibliotheken

Benutzer oder Administratoren können die Standardbibliotheken ausblenden oder löschen, allerdings kann der Knoten Bibliotheken im Navigationsbereich nicht ausgeblendet oder gelöscht werden. Das Ausblenden einer Standardbibliothek ist dem Löschen vorzuziehen, da Anwendungen wie Windows Media Player auf die Standardbibliotheken zurückgreifen und Sie neu erstellen, wenn Sie auf dem Computer nicht vorhanden sind. Anweisungen finden Sie unter Ausblenden von Standardbibliotheken .

Standardspeicherorte für Bibliotheken

Jede Bibliothek verfügt über einen Standardspeicherort für "Speichern". Dateien werden an diesen Speicherort gespeichert oder kopiert, wenn der Benutzer eine Datei in einer Bibliothek anstatt an einer bestimmten Stelle in der Bibliothek speichern oder kopieren möchte. Bekannte Ordner sind die Standardspeicherorte; Benutzer können jedoch einen anderen Speicherort für die Speicherung auswählen. Wenn der Benutzer den Standardspeicherort aus einer Bibliothek entfernt, wird der nächste Speicherort automatisch als neuer Standardspeicherort ausgewählt. Wenn die Bibliothek leer ist oder wenn alle enthaltenen Speicherorte nicht gespeichert werden können, schlägt der Speichervorgang fehl.

Indizierungs Anforderungen und "grundlegende" Bibliotheken

Bestimmte Bibliotheksfeatures hängen vom Inhalt der Bibliotheken ab, die indiziert werden. Bibliotheksspeicherorte müssen für die lokale Indizierung verfügbar sein oder auf eine Weise indiziert werden, die dem Windows-Indizierungs Protokoll entspricht. Wenn die Indizierung für einen oder mehrere Speicherorte in einer Bibliothek nicht aktiviert ist, wird die gesamte Bibliothek auf grundlegende Funktionen zurückgesetzt:

- Keine Unterstützung für das Browsen von Metadaten über **Anordnen nach** Ansichten.
- Nur grep-Suchvorgänge.
- Suchvorschläge für grep-only. Die einzigen verfügbaren Eigenschaften für Eingabe Vorschläge sind **Datumsänderungen** und **Größe**.
- Keine Unterstützung für die Suche über das Startmenü. Im Startmenü werden keine Dateien aus einfachen Bibliotheken zurückgegeben.
- Keine Vorschau von Datei Ausschnitten für Suchergebnisse, die im Inhalts Modus zurückgegeben werden.

Um diese begrenzte Funktionalität zu vermeiden, müssen alle Speicherorte in der Bibliothek entweder lokal oder Remote indiziert werden können. Wenn Benutzer lokale Ordner zu Bibliotheken hinzufügen, fügt Windows die

Position zum Indizierungs Bereich hinzu und indiziert den Inhalt. Remotespeicherorte, die nicht Remote indiziert sind, können mithilfe der Offline Dateisynchronisierung zum lokalen Index hinzugefügt werden. Dadurch erhält der Benutzer die Vorteile des lokalen Speichers, auch wenn der Standort Remote ist. Wenn Sie einen Ordner "immer offline verfügbar" erstellen, wird eine lokale Kopie der Ordner Dateien erstellt, diese Dateien dem Index hinzugefügt und die lokalen und Remotekopien synchron gehalten. Benutzer können Speicherorte, die nicht Remote indiziert sind, manuell synchronisieren und keine Ordnerumleitung verwenden, um die Vorteile der lokalen Indizierung zu nutzen.

Anweisungen zum Aktivieren der Indizierung finden Sie unter Aktivieren der Indizierung von Bibliotheksspeicher Orten.

Wenn Ihre Umgebung das Zwischenspeichern von Dateien lokal nicht unterstützt, sollten Sie die Windows-Bibliotheken deaktivieren, die auf die Gruppenrichtlinien für indizierte Datei Daten angewiesen sind. Dadurch werden alle Bibliotheken grundlegend vereinfacht. Weitere Informationen finden Sie unter Gruppenrichtlinien für Windows-Suche, durchsuchen und organisieren.

Ordnerumleitung

Während Bibliotheksdateien selbst nicht umgeleitet werden können, können Sie bekannte Ordner, die in Bibliotheken enthalten sind, mithilfe der OrdnerUmleitung umleiten. So können Sie beispielsweise den Ordner "eigene Dateien" umleiten, der in der Standardbibliothek "Dokumente" enthalten ist. Beim Umleiten von bekannten Ordnern sollten Sie sicherstellen, dass das Ziel entweder indiziert oder immer offline verfügbar ist, um die vollständige Bibliotheks Funktionalität beizubehalten. In beiden Fällen werden die Dateien für den Zielordner in Bibliotheken indiziert und unterstützt. Diese Einstellungen werden auf der Serverseite konfiguriert.

Unterstützte Speicherorte

In der folgenden Tabelle wird gezeigt, welche Speicherorte in Windows-Bibliotheken unterstützt werden.

UNTERSTÜTZTE SPEICHERORTE	NICHT UNTERSTÜTZTE SPEICHERORTE
Feste lokale Volumes (NTFS/FAT)	Austauschbare Laufwerke
Indexierte Freigaben (Abteilungsserver *, Windowshome-PCs)	Wechselmedien (wie DVDs) Netzwerkfreigaben, auf die über DFS-Namespaces zugegriffen werden kann oder die Teil eines Failoverclusters sind
Offline verfügbare Freigaben (umgeleitete Ordner, die Offlinedateien verwenden)	Netzwerkfreigaben, die nicht offline verfügbar oder Remote indiziert sind NAS-Geräte (Network Attached Storage)
	Andere Datenquellen: SharePoint, Exchange usw.

\ * Für Freigaben, die auf einem Abteilungsserver indiziert sind, funktioniert die Windows-Suche in Arbeitsgruppen oder auf einem Domänenserver mit ähnlichen Eigenschaften wie ein Arbeitsgruppenserver. So funktioniert die Windows-Suche beispielsweise auf einem einzelnen Share-Abteilungsserver mit den folgenden Merkmalen:

- Die erwartete maximale Auslastung sind vier gleichzeitige Abfrageanforderungen.
- Erwartetes Indizierungs Corpus ist ein Maximum von 1 Million-Dokumenten.
- Benutzer greifen direkt auf den Server zu. Das bedeutet, dass der Server nicht über DFS-Namespaces zur Verfügung gestellt wird.
- Benutzer werden nicht an einen anderen Server umgeleitet, wenn ein Fehler auftritt. Das heißt, Servercluster werden nicht verwendet.

Bibliotheks Attribute

Die folgenden Bibliotheks Attribute können im Windows-Explorer, im Dialogfeld Bibliotheksverwaltung oder in der Bibliotheks Beschreibungsdatei (*. Library-MS) geändert werden:

- Name
- Bibliotheksspeicherorte
- Reihenfolge von Bibliotheksspeicher Orten
- Standardspeicherort

Das Bibliothekssymbol kann vom Administrator oder Benutzer geändert werden, indem die Schemadatei für die Bibliotheks Beschreibung direkt bearbeitet wird.

Informationen zum Erstellen von Bibliotheks Beschreibungsdateien finden Sie im Thema " Library Description Schema " auf MSDN.

Weitere Informationen:

Konzepte

- Windows-Such Features
- Windows-Indizierungs Features
- Features für die Verbundsuche
- Anleitungen für administrative Anleitungen
- Gruppenrichtlinie für Windows-Suche, durchsuchen und organisieren
- Zusätzliche Ressourcen für Windows-Suche,-durchsuchen und-Organisation

Weitere Ressourcen

- Ordnerumleitung, Offlinedateien und Roamingbenutzerprofile
- Bibliotheks Beschreibungs Schema

Behandeln von Problemen mit dem Windows 10-Client

04.12.2019 • 2 minutes to read

Microsoft gibt regelmäßig beide Updates für Windows Server frei. Um sicherzustellen, dass Ihre Server zukünftige Updates einschließlich der Sicherheitsupdates erhalten können, ist es wichtig, sie auf dem neuesten Stand zu halten. Eine vollständige Liste der veröffentlichten Updates finden Sie unter Windows 10-und Windows Server 2016-Updateverlauf .

Dieser Abschnitt enthält erweiterte Problembehandlungsthemen und Links, die Ihnen bei der Behebung von Problemen mit Windows 10 in einer Enterprise-oder IT pro-Umgebung helfen. Weitere Themen werden hinzugefügt, sobald diese verfügbar sind.

Problembehandlung bei der 802.1 x-Authentifizierung

- Erweiterte Problembehandlung bei der 802.1 x-Authentifizierung
- Datensammlung für die Problembehandlung der 802.1X-Authentifizierung

Problembehandlung bei BitLocker

- Richtlinien für die Problembehandlung bei BitLocker
- BitLocker kann ein Laufwerk nicht verschlüsseln: bekannte Probleme
- Erzwingen von BitLocker-Richtlinien mithilfe von InTune: bekannte Probleme
- BitLocker-Netzwerksperre: bekannte Probleme
- BitLocker-Wiederherstellung: bekannte Probleme
- BitLocker-Konfiguration: bekannte Probleme
- BitLocker kann ein Laufwerk nicht verschlüsseln: bekannte TPM-Probleme
- BitLocker und TPM: andere bekannte Probleme
- Decodieren der gemessenen Start Protokolle zum nachvollziehen von PCR-Änderungen
- Häufig gestellte Fragen (Frequently Asked Questions, FAQ) zu BitLocker

Problembehandlung bei BugCheck und Abbruchfehlern

- Einführung in die Auslagerungsdatei
- Bestimmen der geeigneten Auslagerungsdateigröße für 64-Bit-Versionen von Windows
- Konfigurieren von Systemausfall- und Wiederherstellungsoptionen in Windows
- Generieren eines Kernels oder eines vollständigen Absturzabbilds
- Erweiterte Problembehandlung für Stoppfehler und Bluescreens
- Erweiterte Problembehandlung für Stoppfehler 7B oder Inaccessible_Boot_Device
- Blue-Screen-Daten – Windows-Treiber
- Code Referenz zur Fehlerüberprüfung – Windows-Treiber

Problembehandlung bei der Anmelde Informations Überwachung

- Windows Defender Credential Guard – bekannte Probleme (Windows10)

Problembehandlung bei Datenträgern

- MBR2GPT
- Häufig gestellte Fragen zu Windows und GPT

Behandeln von Problemen mit dem Kiosk Modus

- Problembehandlung bei der Kiosk-Modus

Problembehandlung beim Booten

- Erweiterte Problembehandlung für Windows-Startprobleme

Problembehandlung beim Zurücksetzen des Push-Buttons

- Häufig gestellte Fragen (FAQ) zum Zurücksetzen auf Knopfdruck
- Häufig gestellte Fragen (FAQ) zum Zurücksetzen auf Knopfdruck
- Wiederherstellungskomponenten

Problembehandlung bei der Energieverwaltung

- Moderne Standby-FAQs

Problembehandlung beim sicheren Booten

- Der sichere Start ist nicht ordnungsgemäß konfiguriert: Problembehandlung

Problembehandlung beim Einrichten und installieren

- Problembehandlung und Protokolldateien für die Bereitstellung

Problembehandlung im Startmenü

- Behandeln von Startmenüfehlern

Problembehandlung bei der Aktivierung von Abonnements

- Bereitstellen von Lizenzen für Windows 10 Enterprise

Problembehandlung beim System Absturz

- Erweiterte Problembehandlung für Windows-basierte Computer, die einfrieren

Problembehandlung bei der TCP/IP-Kommunikation

- Sammeln von Daten mithilfe des Netzwerkmonitors
- Problembehandlung für die TCP/IP-Verbindung
- Problembehandlung für Portmangel
- Problembehandlung für Remote Procedure Call (RPC)-Fehler

Behandeln von Problemen mit dem Benutzerstatus-Migrations-Toolkit (USMT)

- Allgemeine Probleme

- Häufig gestellte Fragen
- Protokolldateien
- Rückgabecodes

Problembehandlung bei Windows Hello for Business (WHFB)

- Häufig gestellte Fragen zu Windows Hello for Business
- Windows Hello-Fehler während der PIN-Erstellung (Windows 10)
- Ereignis-ID 300 – Windows Hello erfolgreich erstellt (Windows 10)

Behandeln von Problemen mit Windows Analytics

- Häufig gestellte Fragen und Problembehandlung bei Windows Analytics

Problembehandlung bei Windows Update

- Funktionsweise von Windows Update
- Windows Update-Protokolldateien
- Windows Update-Problembehandlung
- Häufige Fehler und Minderungs Probleme in Windows Update
- Windows Update – zusätzliche Ressourcen
- Erste Schritte mit Windows Update
- Servicing Stack-updates

Problembehandlung bei Windows-Upgrades

- Schnellkorrekturen – Windows IT pro
- SetupDiag
- Problembehandlung bei Windows 10-Upgrade-Fehlern – Windows IT pro
- Windows-Fehlerberichterstattung – Windows IT pro
- Update-Fehlercodes – Windows IT pro
- Protokolldateien – Windows IT pro
- Lösungsverfahren – Windows IT Pro

Problembehandlung bei der Windows-Wiederherstellung (WinRE)

- Features zur Problembehandlung von Windows RE

Problembehandlung für drahtlose Verbindungen

- Erweiterte Problembehandlung für drahtlose Netzwerkverbindungen

Weitere Ressourcen

Behandeln von Problemen mit Windows Server-Komponenten

Erweiterte Problembehandlung für Windows-Networking

19.06.2019 • 2 minutes to read

Die folgenden Themen stehen Ihnen bei der Behebung allgemeiner Probleme im Zusammenhang mit dem Windows-Netzwerk zur Verfügung.

- Erweiterte Problembehandlung für drahtlose Netzwerkkonnektivität
- Erweiterte Problembehandlung für 802.1X-Authentifizierung
  - Datensammlung für die Problembehandlung der 802.1X-Authentifizierung
- Erweiterte Problembehandlung für TCP/IP
  - Sammeln von Daten mithilfe des Netzwerkmonitors
  - Problembehandlung für die TCP/IP-Verbindung
  - Problembehandlung für Portmangel
  - Problembehandlung für Remote Procedure Call (RPC)-Fehler

Konzepte und technische Bezüge

Übersicht über den 802.1 x-authentifizierten Kabel Zugriff
Übersicht über den 802.1 x-authentifizierten Drahtloszugriff
Übersicht über die drahtlose cccess-Bereitstellung
TCP/IP-Technische Referenz
Netzwerk Monitor
RPC und das Netzwerk
Funktionsweise von RPC
NPS-Ursachencodes

Erweiterte Problembehandlung für drahtlose Netzwerkverbindungen

29.10.2019 • 11 minutes to read

> **NOTE**
> Privatbenutzer: Dieser Artikel ist für die Verwendung durch Support-Mitarbeiter und IT-Experten vorgesehen. Wenn Sie nach weiteren allgemeinen Informationen zu WLAN-Problemen in Windows 10 suchen, lesen Sie diesen Artikel zu Windows 10 Wi-Fi Fix.

Übersicht

Dies ist eine allgemeine Problembehandlung beim Einrichten von WLAN-Verbindungen von Windows-Clients. Für die Problembehandlung von WLAN-Verbindungen müssen Sie den grundlegenden Fluss des Wi-Fi-Auto verbinden-Statuscomputers verstehen. Wenn Sie diesen Fluss verstehen, ist es einfacher, den Ausgangspunkt in einem Repro Szenario zu ermitteln, in dem ein anderes Verhalten gefunden wird. Dieser Workflow umfasst Kenntnisse und die Verwendung von TextAnalysisTool, einem umfangreichen Textfilter Tool, das bei komplexen Ablaufverfolgungen mit zahlreichen etw-Anbietern wie wireless_dbg-Ablaufverfolgungsszenario hilfreich ist.

Szenarien

Dieser Artikel bezieht sich auf Szenarien, in denen WLAN-Verbindungen nicht hergestellt werden können. Die Problembehandlung wurde mit Windows 10-Clients im Fokus entwickelt, kann aber auch bei Ablaufverfolgungen bis zu Windows 7 nützlich sein.

> **NOTE**
> Diese Problembehandlung verwendet Beispiele, die eine allgemeine Strategie zum Navigieren und Interpretieren der Ereignisablaufverfolgung für drahtlose Komponenten für Windows (ETW) veranschaulichen. Es ist nicht dazu gedacht, für jedes WLAN-Problemszenario repräsentativ zu sein.

Wireless etw ist unglaublich ausführlich und ruft viele harmlose Fehler hervor (eher gekennzeichnete Verhaltensweisen, die mit dem Problemszenario wenig oder gar nichts zu tun haben). Das einfache Suchen nach oder Filtern nach "Err", "Fehler" und "Fail" führt selten zur Ursache für ein problematisches WLAN-Szenario. Stattdessen wird der Bildschirm mit sinnlosen Protokollen überflutet, die den Kontext des eigentlichen Problems verschleiern werden.

Es ist wichtig, die verschiedenen beteiligten WLAN-Komponenten, deren erwartete Verhaltensweisen und die Abweichung des Problemszenarios von den erwarteten Verhaltensweisen zu verstehen. Die Absicht dieser Problembehandlung besteht darin, zu zeigen, wie Sie einen Ausgangspunkt in der Ausführlichkeit von wireless_dbg etw und Home in auf den Verantwortlichen Komponenten finden, die das Verbindungsproblem verursachen.

Bekannte Probleme und Fehlerbehebungen

BETRIEBSSYSTEMVERSION	BEHOBEN IN
Windows10, Version1803	KB4284848

BETRIEBSSYSTEMVERSION	BEHOBEN IN
Windows10, Version1709	KB4284822
Windows10, Version1703	KB4338827

Stellen Sie sicher, dass Sie die neuesten Updates für Windows-Updates, kumulative Updates und Rollups installieren. Informationen zum Überprüfen des Updatestatus finden Sie auf der entsprechenden Update-History-Webseite für Ihr System:

- Windows 10, Version 1809
- Windows 10, Version 1803
- Windows 10, Version 1709
- Windows 10, Version 1703
- Windows 10, Version 1607 und Windows Server 2016
- Windows 10, Version 1511
- Windows 8,1 und Windows Server 2012 R2
- Windows Server 2012
- Windows 7 SP1 und Windows Server 2008 R2 SP1

Datensammlung

1. Netzwerkerfassung mit etw Geben Sie an einer Eingabeaufforderung mit erhöhten Rechten Folgendes ein:

   ```
   netsh trace start wireless_dbg capture=yes overwrite=yes maxsize=4096 tracefile=c:\tmp\wireless.etl
   ```

2. Reproduzieren Sie das Problem.
   - Wenn die Verbindung nicht hergestellt werden konnte, versuchen Sie, die Verbindung manuell herzustellen.
   - Wenn es sich um eine intermittierende, aber einfach reproduzierbare Anwendung handelt, versuchen Sie, die Verbindung manuell herzustellen, bis Sie fehlschlägt. Zeichnen Sie die Zeit jedes Verbindungsversuchs auf, und geben Sie an, ob dies ein Erfolg oder Fehler war.
   - Wenn das Problem vorübergehend, aber selten ist, muss der Befehl Netsh Trace Stop automatisch ausgelöst werden (oder zumindest für den Administrator schnell benachrichtigt werden), um sicherzustellen, dass die Reprodaten durch die Ablaufverfolgung nicht überschrieben werden.
   - Wenn die zeitweilige Verbindung den Befehl Stoppbefehl für ein Skript abbricht (Ping-oder Testnetzwerk ständig, bis ein Fehler auftritt, wird Netsh Trace beendet).
3. Beenden Sie die Ablaufverfolgung, indem Sie den folgenden Befehl eingeben:

   ```
   netsh trace stop
   ```

4. So konvertieren Sie die Ausgabedatei in das Text Format:

   ```
   netsh trace convert c:\tmp\wireless.etl
   ```

Ein Beispiel für die Befehlsausgabe finden Sie im Beispiel für etw-Aufnahme am Ende dieses Artikels. Nachdem Sie diese Befehle ausgeführt haben, gibt es drei Dateien: Wireless. cab, Wireless. ETL und Wireless. txt.

Problembehandlung

Im folgenden sehen Sie eine allgemeine Ansicht der wichtigsten WLAN-Komponenten in Windows.

Windows Connection Manager (Wcmsvc)	Der **Windows-Verbindungs** -Manager (Wcmsvc) ist eng mit den UI-Steuerelementen (Taskleistensymbol) verknüpft, um eine Verbindung mit verschiedenen Netzwerken, einschließlich Drahtlosnetzwerken, herzustellen. Sie akzeptiert und verarbeitet Eingaben des Benutzers und speist sie an den Core Wireless Service.
WLAN Autoconfig Service (WlanSvc)	Der **WLAN-AutoConfig** -Dienst (WlanSvc) behandelt die folgenden Kernfunktionen von Drahtlosnetzwerken in Windows: - Überprüfen von Drahtlosnetzwerken in einem Bereich - Verwalten der Konnektivität von Drahtlosnetzwerken
Media Specific Module (MSM)	Das **medienspezifische Modul** (MSM) behandelt Sicherheitsaspekte einer Verbindung, die hergestellt wird.
Native Wifi stack	Der **Native WiFi-** Stack besteht aus Treibern und WLAN-APIs für die Interaktion mit drahtlosen Miniports und der unterstützenden Benutzermodus-WLANSVC.
Wifi miniport	Schnittstelle für **drahtlose Miniport** -Treiber von Drittanbietern mit dem oberen drahtlos Stapel zum Bereitstellen von Benachrichtigungen und empfangen von Befehlen von Windows.

Der WLAN-Verbindungsstatus Automat hat die folgenden Zustände:

- Auffrischen
- Ihv_Configuring
- Konfigurieren
- Zuordnen
- Authentifizierung
- Roaming
- Wait_For_Disconnected
- Getrennt

Standard mäßige WLAN-Verbindungen neigen dazu, zwischen Zuständen zu wechseln:

Verbindung wird hergestellt

Reset--#a0 Ihv_Configuring--#a1 Konfiguration--#a2 Zuordnung--#a3-Authentifizierung--> verbunden

Trennen

Verbunden--#a0 Roaming--#a1 Wait_For_Disconnected--#a2 getrennt--#a3 zurücksetzen

> Das Filtern der etw-Ablaufverfolgung mit dem TextAnalysisTool (Tat) ist ein einfacher erster Schritt, um festzustellen, wo eine fehlgeschlagene Verbindungseinrichtung abbricht. Am Ende dieses Artikels ist eine nützliche WLAN-Filter Datei enthalten.

Verwenden Sie den **FSM-Übergangs** Ablaufverfolgungsfilter, um den Verbindungsstatus Computer anzuzeigen. Ein Beispiel für diesen Filter, der in der Tat am unteren Rand dieser Seite angewendet wird, wird angezeigt.

Der folgende Code ist ein Beispiel für ein gutes Verbindungssetup:

```
44676 [2]0F24.1020::2018-09-17 10:22:14.658 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Disconnected to State: Reset
45473 [1]0F24.1020::2018-09-17 10:22:14.667 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Reset to State: Ihv_Configuring
45597 [3]0F24.1020::2018-09-17 10:22:14.708 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Ihv_Configuring to State: Configuring
46085 [2]0F24.17E0::2018-09-17 10:22:14.710 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Configuring to State: Associating
47393 [1]0F24.1020::2018-09-17 10:22:14.879 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Associating to State: Authenticating
49465 [2]0F24.17E0::2018-09-17 10:22:14.990 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Authenticating to State: Connected
```

Der folgende Code ist ein Beispiel für eine fehlgeschlagene Verbindungseinrichtung:

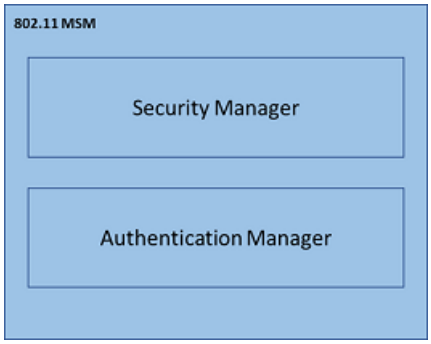
```
44676 [2]0F24.1020::2018-09-17 10:22:14.658 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Disconnected to State: Reset
45473 [1]0F24.1020::2018-09-17 10:22:14.667 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Reset to State: Ihv_Configuring
45597 [3]0F24.1020::2018-09-17 10:22:14.708 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Ihv_Configuring to State: Configuring
46085 [2]0F24.17E0::2018-09-17 10:22:14.710 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Configuring to State: Associating
47393 [1]0F24.1020::2018-09-17 10:22:14.879 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Associating to State: Authenticating
49465 [2]0F24.17E0::2018-09-17 10:22:14.990 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State: Authenticating to State: Roaming
```

Durch das Identifizieren des Zustands, in dem die Verbindung fehlschlägt, kann man sich genauer auf die Ablaufverfolgung von Protokollen konzentrieren, die sich unmittelbar vor dem letzten als funktionierend bekannten Zustand befinden.

Das Überprüfen von **[Microsoft-Windows-WLAN-AutoConfig]** -Protokollen unmittelbar vor der fehlerhaften Zustandsänderung sollte einen Fehler Beweis aufweisen. Häufig wird der Fehler jedoch über andere drahtlose Komponenten weitergegeben. In vielen Fällen ist die nächste Komponente von Interesse die MSM, die direkt unter WLANSVC liegt.

Zu den wichtigen Komponenten der MSM gehören:

- Security Manager (SecMgr) – behandelt alle Sicherheitsvorgänge vor und nach der Verbindung.
- Authentifizierungsmodul (AuthMgr) – verwaltet 802.1 x-auth-Anforderungen



Jede dieser Komponenten verfügt über eigene einzelne Zustandsmaschinen, die bestimmten Übergängen folgen.

Aktivieren Sie die Übergangs Filter **FSM Transition, SecMgr Transition** und **AuthMgr** in TextAnalysisTool, um weitere Details zu finden.

Wenn Sie das obige Beispiel fortsetzen, sehen die kombinierten Filter wie folgt aus:

```
[2] 0C34.2FF0::08/28/17-13:24:28.693 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State:
Reset to State: Ihv_Configuring
[2] 0C34.2FF0::08/28/17-13:24:28.693 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State:
Ihv_Configuring to State: Configuring
[1] 0C34.2FE8::08/28/17-13:24:28.711 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State:
Configuring to State: Associating
[0] 0C34.275C::08/28/17-13:24:28.902 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition INACTIVE (1) --> ACTIVE (2)
[0] 0C34.275C::08/28/17-13:24:28.902 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition ACTIVE (2) --> START AUTH (3)
[4] 0EF8.0708::08/28/17-13:24:28.928 [Microsoft-Windows-WLAN-AutoConfig]Port (14) Peer
0x186472F64FD2 AuthMgr Transition ENABLED  --> START_AUTH
[3] 0C34.2FE8::08/28/17-13:24:28.902 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State:
Associating to State: Authenticating
[1] 0C34.275C::08/28/17-13:24:28.960 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition START AUTH (3) --> WAIT FOR AUTH SUCCESS (4)
[4] 0EF8.0708::08/28/17-13:24:28.962 [Microsoft-Windows-WLAN-AutoConfig]Port (14) Peer
0x186472F64FD2 AuthMgr Transition START_AUTH  --> AUTHENTICATING
[2] 0C34.2FF0::08/28/17-13:24:29.751 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition WAIT FOR AUTH SUCCESS (7) --> DEACTIVATE (11)
[2] 0C34.2FF0::08/28/17-13:24:29.7512788 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition DEACTIVATE (11) --> INACTIVE (1)
[2] 0C34.2FF0::08/28/17-13:24:29.7513404 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State:
Authenticating to State: Roaming
```

NOTE

In der neben letzten Zeile wird der SecMgr-Übergang plötzlich deaktiviert:
\ [2] 0C 34,2 ff0:: 08/28/17-13:24:29.7512788 \ [Microsoft-Windows-WLAN-AutoConfig] Port \ [13] Peer 8a: 15:14: B6:25:10 SecMgr Übergang deaktivieren (11)--#a0 inaktiv (1)

Dieser Übergang wird letztendlich an den Haupt Verbindungsstatus Computer weitergegeben und bewirkt, dass die Authentifizierungsphase in den roamingstatus übertragen wird. Wie zuvor ist es sinnvoll, sich direkt vor diesem SecMgr-Verhalten auf die Ablaufverfolgung zu konzentrieren, um den Grund für die Deaktivierung zu ermitteln.

Wenn Sie den Filter **Microsoft-Windows-WLAN-Auto config** aktivieren, werden weitere Details angezeigt, die zum Deaktivieren des Übergangs führen:

```
[3] 0C34.2FE8::08/28/17-13:24:28.902 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State:
Associating to State: Authenticating
[1] 0C34.275C::08/28/17-13:24:28.960 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition START AUTH (3) --> WAIT FOR AUTH SUCCESS (4)
[4] 0EF8.0708::08/28/17-13:24:28.962 [Microsoft-Windows-WLAN-AutoConfig]Port (14) Peer
0x186472F64FD2 AuthMgr Transition START_AUTH  --> AUTHENTICATING
[0]0EF8.2EF4::08/28/17-13:24:29.549 [Microsoft-Windows-WLAN-AutoConfig]Received Security Packet:
PHY_STATE_CHANGE
[0]0EF8.2EF4::08/28/17-13:24:29.549 [Microsoft-Windows-WLAN-AutoConfig]Change radio state for
interface = Intel(R) Centrino(R) Ultimate-N 6300 AGN :  PHY = 3, software state = on , hardware
state = off )
[0] 0EF8.1174::08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-AutoConfig]Received Security Packet:
PORT_DOWN
[0] 0EF8.1174::08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-AutoConfig]FSM Current state
Authenticating , event Upcall_Port_Down
[0] 0EF8.1174:: 08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-AutoConfig]Received IHV PORT DOWN,
peer 0x186472F64FD2
[2] 0C34.2FF0::08/28/17-13:24:29.751 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition WAIT FOR AUTH SUCCESS (7) --> DEACTIVATE (11)
 [2] 0C34.2FF0::08/28/17-13:24:29.7512788 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition DEACTIVATE (11) --> INACTIVE (1)
[2] 0C34.2FF0::08/28/17-13:24:29.7513404 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State:
Authenticating to State: Roaming
```

Der Pfad rückwärts zeigt eine Benachrichtigung über den **Port Down** an:

\ [0] 0EF 8.1174:: 08/28/17-13:24:29.705 \ [Microsoft-Windows-WLAN-AutoConfig] IHV-Port abwärts empfangen, Peer-0x186472F64FD2

Port Ereignisse zeigen Änderungen, die sich näher an der drahtlosen Hardware befinden. Dem Trail können Sie folgen, indem Sie weiterhin den Ursprung dieser Indikation sehen.

Im folgenden ist der MSM der Native WiFi-Stack. Hierbei handelt es sich um Windows Native WiFi-Treiber, die sich mit den WLAN-Miniport-Treibern unterhalten. Sie ist für die Konvertierung von WLAN-Paketen (802,11) in 802,3 (Ethernet) verantwortlich, damit tcpip und andere Protokolle Sie verwenden können.

Aktivieren des Ablaufverfolgungsfilters für **[Microsoft-Windows-NWifi]:**

```
[3] 0C34.2FE8::08/28/17-13:24:28.902 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State:
Associating to State: Authenticating
[1] 0C34.275C::08/28/17-13:24:28.960 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition START AUTH (3) --> WAIT FOR AUTH SUCCESS (4)
[4] 0EF8.0708::08/28/17-13:24:28.962 [Microsoft-Windows-WLAN-AutoConfig]Port (14) Peer
0x8A1514B62510 AuthMgr Transition START_AUTH  --> AUTHENTICATING
[0]0000.0000::08/28/17-13:24:29.127 [Microsoft-Windows-NWiFi]DisAssoc: 0x8A1514B62510 Reason: 0x4
[0]0EF8.2EF4::08/28/17-13:24:29.549 [Microsoft-Windows-WLAN-AutoConfig]Received Security Packet:
PHY_STATE_CHANGE
[0]0EF8.2EF4::08/28/17-13:24:29.549 [Microsoft-Windows-WLAN-AutoConfig]Change radio state for
interface = Intel(R) Centrino(R) Ultimate-N 6300 AGN :  PHY = 3, software state = on , hardware
state = off )
[0] 0EF8.1174::08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-AutoConfig]Received Security Packet:
PORT_DOWN
[0] 0EF8.1174::08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-AutoConfig]FSM Current state
Authenticating , event Upcall_Port_Down
[0] 0EF8.1174:: 08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-AutoConfig]Received IHV PORT DOWN,
peer 0x186472F64FD2
[2] 0C34.2FF0::08/28/17-13:24:29.751 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition WAIT FOR AUTH SUCCESS (7) --> DEACTIVATE (11)
 [2] 0C34.2FF0::08/28/17-13:24:29.7512788 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer
8A:15:14:B6:25:10 SecMgr Transition DEACTIVATE (11) --> INACTIVE (1)
[2] 0C34.2FF0::08/28/17-13:24:29.7513404 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from
State:
Authenticating to State: Roaming
```

In der obigen Ablaufverfolgung wird die Zeile angezeigt:

```
[0]0000.0000::08/28/17-13:24:29.127 [Microsoft-Windows-NWiFi]DisAssoc: 0x8A1514B62510 Reason: 0x4
```

Auf diese Weise werden **PHY_STATE_CHANGE** -und **PORT_DOWN** -Ereignisse angezeigt, die auf eine Zuordnung vom Zugriffspunkt (AP) zurückzuführen sind, um die Verbindung zu verweigern. Dies kann an ungültigen Anmeldeinformationen, Verbindungsparametern, Verlust von Signal/Roaming und verschiedenen anderen Gründen für das Abbrechen einer Verbindung liegen. Die Aktion hier wäre, den Grund für die Zuordnung zu untersuchen, die vom angegebenen AP-Mac gesendet wird (8a: 15:14: B6:25:10). Dies würde durch die Untersuchung interner Protokollierung/Ablaufverfolgung vom AP erfolgen.

Ressourcen

802,11 Wireless-Tools und-Einstellungen
Grundlegendes zur 802.1 x-Authentifizierung für drahtlose Netzwerke

Beispiel für etw-Erfassung

```
C:\tmp>netsh trace start wireless_dbg capture=yes overwrite=yes maxsize=4096
tracefile=c:\tmp\wireless.etl

Trace configuration:
-------------------------------------------------------------------
Status:             Running
Trace File:         C:\tmp\wireless.etl
Append:             Off
Circular:           On
Max Size:           4096 MB
Report:             Off

C:\tmp>netsh trace stop
Correlating traces ... done
Merging traces ... done
Generating data collection ... done
The trace file and additional troubleshooting information have been compiled as
"c:\tmp\wireless.cab".
File location = c:\tmp\wireless.etl
Tracing session was successfully stopped.

C:\tmp>netsh trace convert c:\tmp\wireless.etl

Input file:  c:\tmp\wireless.etl
Dump file:   c:\tmp\wireless.txt
Dump format: TXT
Report file: -
Generating dump ... done

C:\tmp>dir
 Volume in drive C has no label.
 Volume Serial Number is 58A8-7DE5

 Directory of C:\tmp

01/09/2019  02:59 PM    [DIR]          .
01/09/2019  02:59 PM    [DIR]          ..
01/09/2019  02:59 PM         4,855,952 wireless.cab
01/09/2019  02:56 PM         2,752,512 wireless.etl
01/09/2019  02:59 PM         2,786,540 wireless.txt
               3 File(s)     10,395,004 bytes
               2 Dir(s)  46,648,332,288 bytes free
```

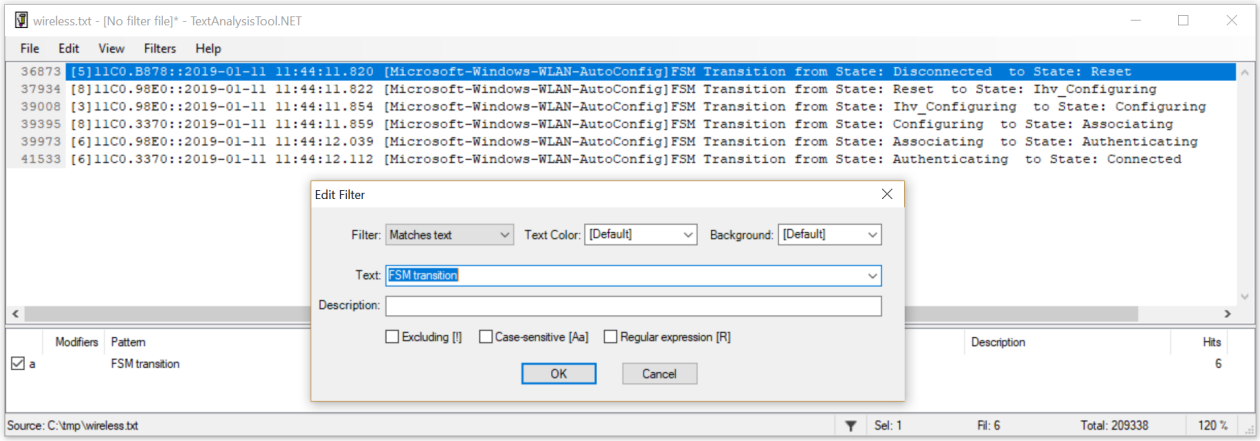
WLAN-Filter Datei

Kopieren Sie alle Zeilen, und fügen Sie Sie in eine Textdatei mit dem Namen "WiFi. Tat" ein. Laden Sie die Filter Datei in die TextAnalysisTool, indem Sie auf **Datei #a0 Filter laden**klicken.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<TextAnalysisTool.NET version="2018-01-03" showOnlyFilteredLines="False">
  <filters>
    <filter enabled="n" excluding="n" description="" foreColor="000000" backColor="d3d3d3" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-OneX]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Unknown]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-EapHost]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[]***" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-Winsock-AFD]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-WinHttp]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-WebIO]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-Winsock-NameResolution]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-TCPIP]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-DNS-Client]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-NlaSvc]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-Iphlpsvc-Trace]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-DHCPv6-Client]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-Dhcp-Client]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-NCSI]" />
    <filter enabled="y" excluding="n" description="" backColor="90ee90" type="matches_text" case_sensitive="n"
regex="n" text="AuthMgr Transition" />
    <filter enabled="y" excluding="n" description="" foreColor="0000ff" backColor="add8e6" type="matches_text"
case_sensitive="n" regex="n" text="FSM transition" />
    <filter enabled="y" excluding="n" description="" foreColor="000000" backColor="dda0dd" type="matches_text"
case_sensitive="n" regex="n" text="SecMgr transition" />
    <filter enabled="y" excluding="n" description="" foreColor="000000" backColor="f08080" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-NWiFi]" />
    <filter enabled="y" excluding="n" description="" foreColor="000000" backColor="ffb6c1" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-WiFiNetworkManager]" />
    <filter enabled="y" excluding="n" description="" foreColor="000000" backColor="dda0dd" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-WLAN-AutoConfig]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-NetworkProfile]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-WFP]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[Microsoft-Windows-WinINet]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="[MSNT_SystemTrace]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000" backColor="ffffff" type="matches_text"
case_sensitive="n" regex="n" text="Security]Capability" />
  </filters>
</TextAnalysisTool.NET>
```

TextAnalysisTool-Beispiel

Im folgenden Beispiel sind die **Ansichts** Einstellungen so konfiguriert, dass **nur gefilterte Zeilen angezeigt**werden.


wireless.txt - [No filter file]* - TextAnalysisTool.NET
File Edit View Filters Help
36873 [5]11C0.B878::2019-01-11 11:44:11.820 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Disconnected to State: Reset
37934 [8]11C0.98E0::2019-01-11 11:44:11.822 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Reset to State: Ihv_Configuring
39008 [3]11C0.98E0::2019-01-11 11:44:11.854 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Ihv_Configuring to State: Configuring
39395 [8]11C0.3370::2019-01-11 11:44:11.859 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Configuring to State: Associating
39973 [6]11C0.98E0::2019-01-11 11:44:12.039 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Associating to State: Authenticating
41533 [6]11C0.3370::2019-01-11 11:44:12.112 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Authenticating to State: Connected
Edit Filter
Filter: Matches text
Text Color: [Default]
Background: [Default]
Text: FSM transition
Description:
Excluding [!]
Case-sensitive [Aa]
Regular expression [R]
OK
Cancel
Modifiers
Pattern
Description
Hits
a
FSM transition
6
Source: C:\tmp\wireless.txt
Sel: 1
Fil: 6
Total: 209338
120 %

Erweiterte Problembehandlung für 802.1X-Authentifizierung

20.02.2020 • 4 minutes to read

Übersicht

Hierbei handelt es sich um eine allgemeine Problembehandlung bei 802.1 x-drahtlos-und-drahtgebundenen Clients. Bei 802.1 x-und WLAN-Problembehandlung ist es wichtig zu wissen, wie der Authentifizierungs Fluss funktioniert, und dann herauszufinden, wo er unterbricht. Es handelt sich um eine Vielzahl von Geräten und Software von Drittanbietern. In den meisten Fällen müssen wir feststellen, wo das Problem liegt, und ein anderer Anbieter muss es beheben. Da wir keine Zugriffspunkte oder Switches einrichten, handelt es sich nicht um eine End-to-End-Lösung von Microsoft.

Szenarien

Dieses Verfahren zur Fehlerbehebung bezieht sich auf Szenarien, in denen drahtlose oder kabelgebundene Verbindungen mit 802.1 x-Authentifizierung versucht werden und dann nicht festgelegt werden können. Der Workflow bezieht sich auf Windows 7-10 für Clients und Windows Server 2008 R2-2012 R2 für NPS.

Bekannte Probleme

Keine

Datensammlung

Siehe Erweiterte Problembehandlung der 802.1 x-Authentifizierungsdaten Sammlung.

Problembehandlung

Das Anzeigen von NPS-Authentifizierungsstatus Ereignissen im Windows-Sicherheits Ereignisprotokoll ist eine der nützlichsten Methoden zur Problembehandlung, um Informationen zu fehlgeschlagenen Authentifizierungen zu erhalten.

NPS-Ereignisprotokolleinträge enthalten Informationen zum Verbindungsversuch, einschließlich des Namens der Verbindungsanforderungsrichtlinie, die dem Verbindungsversuch entspricht, und der Netzwerkrichtlinie, die den Verbindungsversuch akzeptiert oder abgelehnt hat. Wenn sowohl Erfolgs-als auch Fehlerereignisse nicht angezeigt werden, lesen Sie den Abschnitt weiter unten unter NPS-Überwachungsrichtlinien.

Überprüfen Sie das Windows-Sicherheitsereignisprotokoll auf dem NPS-Server für NPS-Ereignisse, die dem abgelehnten (Ereignis-ID 6273) oder akzeptierten Verbindungsversuch (Ereignis-ID 6272) entsprechen.

Scrollen Sie in der Ereignismeldung ganz nach unten, und überprüfen Sie das Feld Ursachen Code und den dazugehörigen Text.

```
Log Name:    Security
Source:      Microsoft Windows Security    Logged:          MM/DD/YYYY hh:mm:ss
Event ID:    6273                          Task Category:   Network Policy Server
Level:       Information                   Keywords:        Audit Failure

Network Policy Server denied access to a user.

....

Authentication Details:
        Connection Request Policy Name:   Use Windows authentication for all users
        Network Policy Name:              Secure Wireless Connections
        Authentication Provider:          Windows
        Authentication Server:            NPS1.contoso.com
        Authentication Type:              EAP
        EAP Type:                         Microsoft: Smart Card or other certificate
        Account Session Identifier:       xxxxx
        Logging Results:                  Accounting information was written to the local log file.
        Reason Code:                      16
        Reason:                           Authentication failed due to a user credentials mismatch.
Either the user name provided does not map to an existing user account or the password was incorrect.
```

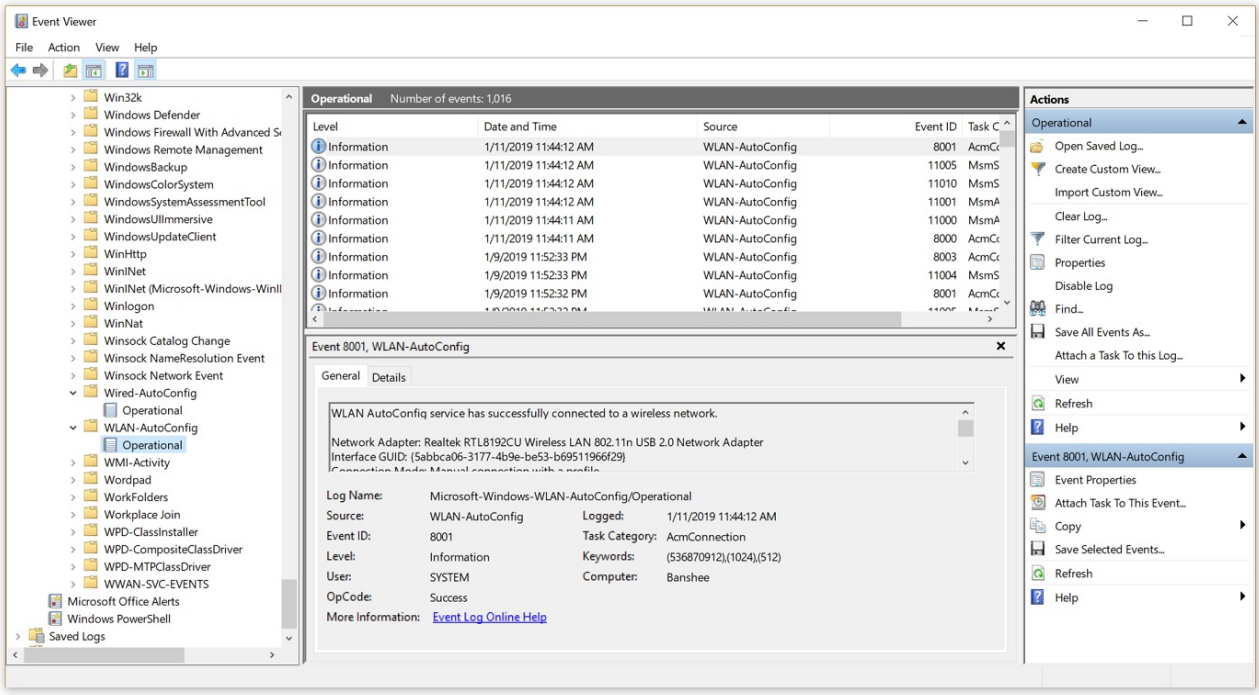
Beispiel: Ereignis-ID 6273 (Überwachungsfehler)

```
Log Name:    Security
Source:      Microsoft Windows Security    Logged:          MM/DD/YYYY hh:mm:ss
Event ID:    6272                          Task Category:   Network Policy Server
Level:       Information                   Keywords:        Audit Success

Network Policy Server granted access to a user.

....

Authentication Details:
        Connection Request Policy Name:   Use Windows authentication for all users
        Network Policy Name:              Secure Wireless Connections
        Authentication Provider:          Windows
        Authentication Server:            NPS1.contoso.com
        Authentication Type:              EAP
        EAP Type:                         Microsoft: Smart Card or other certificate
        Account Session Identifier:       xxxxx
        Logging Results:                  Accounting information was written to the local log file.
```

Beispiel: Ereignis-ID 6272 (Überwachungserfolg)

Im Betriebsprotokoll WLAN-AutoConfig werden Informationen und Fehlerereignisse auf Grundlage von Bedingungen aufgelistet, die vom WLAN-AutoConfig-Dienst erkannt oder gemeldet wurden. Das operative Protokoll enthält Informationen zum Drahtlosnetzwerkadapter, zu den Eigenschaften des drahtlos Verbindungsprofils, zur angegebenen Netzwerkauthentifizierung und im Falle von Verbindungsproblemen den Grund für den Fehler. Für den drahtgebundenen Netzwerkzugriff entspricht das Betriebsprotokoll der drahtgebundenen AutoConfig-Datei einem.

Navigieren Sie auf der Clientseite zu den **\Anwendungs--und Dienstprotokollen der Ereignisanzeige (lokal) \ Microsoft \ Windows \ WLAN-AutoConfig/betriebsbereit** für drahtlose Probleme. Wenn Sie Probleme mit dem Kabelnetzwerkzugriff haben, navigieren Sie zu **.. \ Wired-AutoConfig/Operational**. Siehe hierzu das folgende Beispiel:

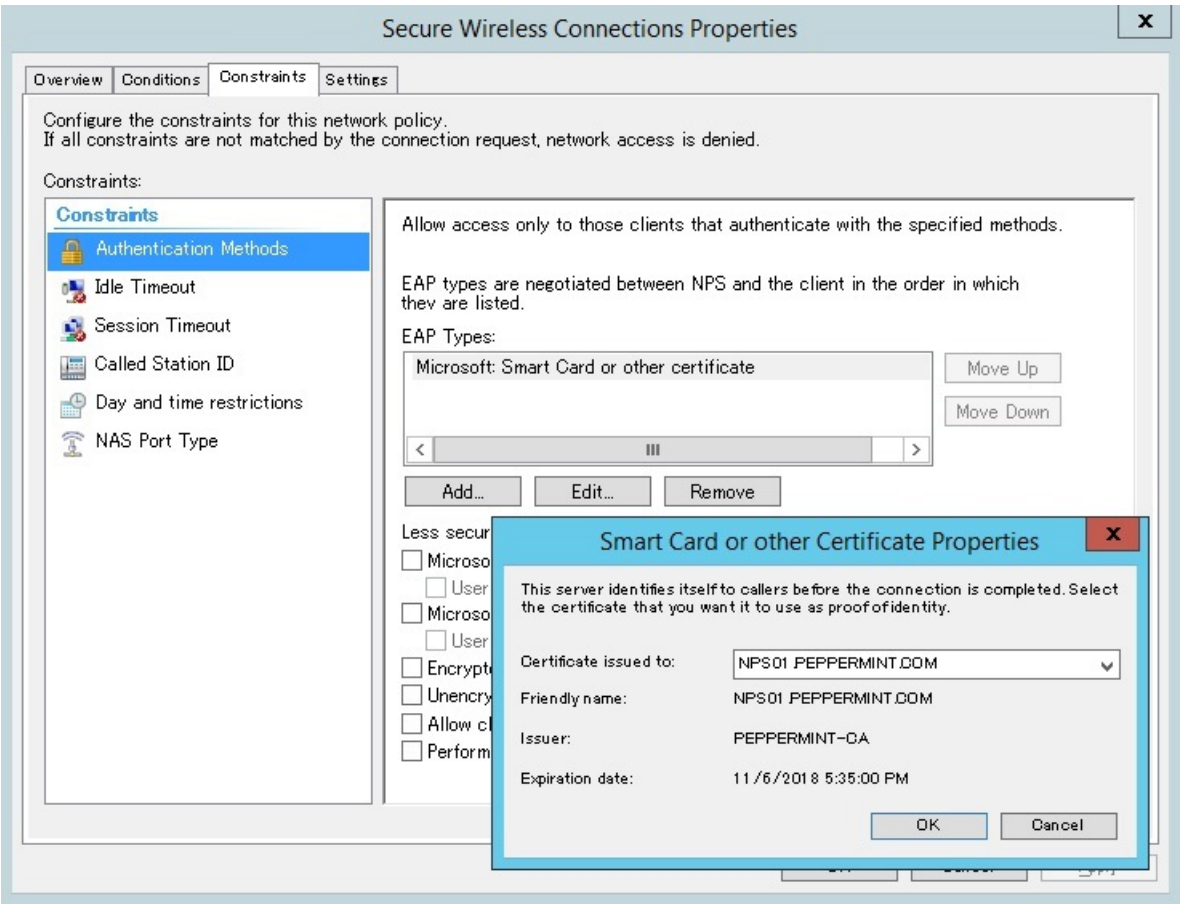


Die meisten Probleme bei der 802.1 x-Authentifizierung sind auf Probleme mit dem Zertifikat zurückzuführen, das für die Client-oder Serverauthentifizierung verwendet wird (beispielsweise ungültiges Zertifikat, Ablauf, Ketten Überprüfungsfehler, Fehler bei der Sperrüberprüfung usw.).

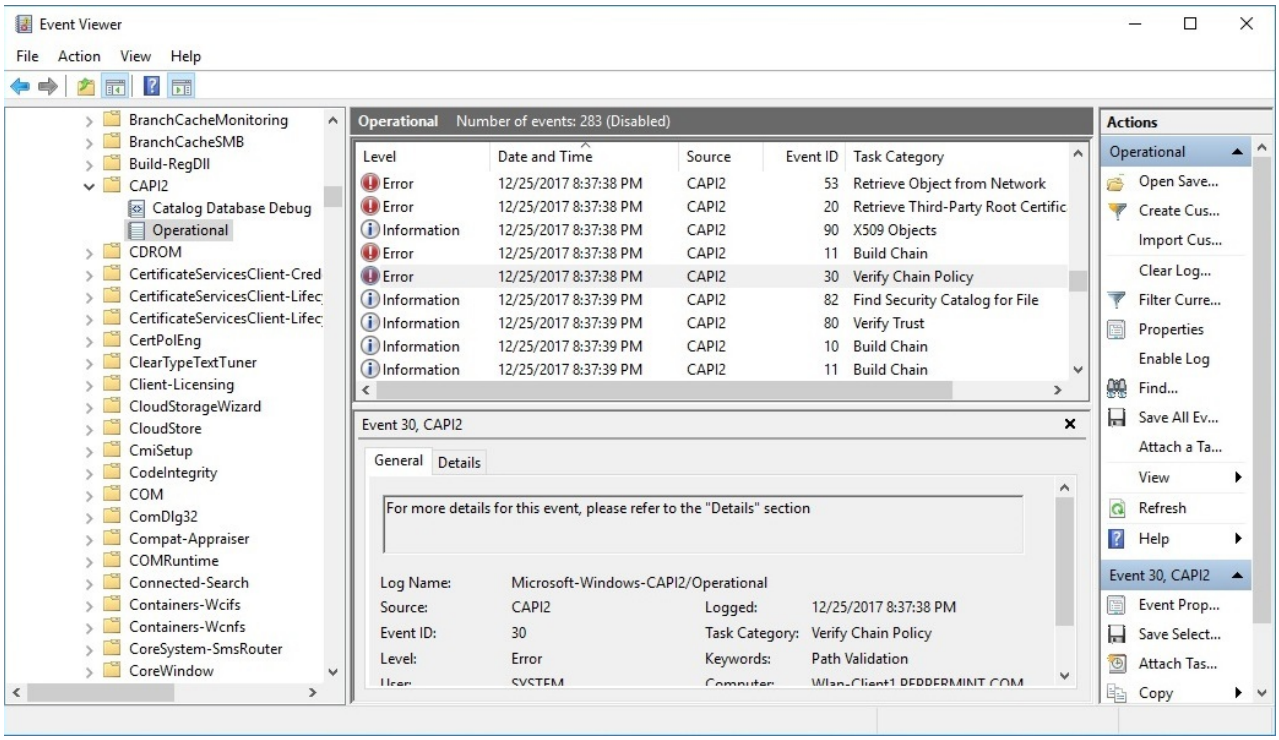
Überprüfen Sie zuerst den Typ der verwendeten EAP-Methode:

EAP Methods	Client Authentication Method	Server Authentication Method
EAP-MSCHAPv2	Username/Password	N/A
EAP-TLS	Certificate	Certificate
PEAP-MSCHAPv2	Username/Password	Certificate
PEAP-TLS	Certificate	Certificate

Wenn ein Zertifikat für seine Authentifizierungsmethode verwendet wird, überprüfen Sie, ob das Zertifikat gültig ist. Auf der Seite Server (NPS) können Sie über das Eigenschaften Menü EAP bestätigen, welches Zertifikat verwendet wird. Wechseln Sie im **NPS-Snap-in**zu **Richtlinien** > -**Netzwerkrichtlinien**. Klicken Sie mit der rechten Maustaste auf die Richtlinie und wählen Sie **Eigenschaften**aus. Wechseln Sie im Popupfenster zur Registerkarte **Einschränkungen** , und wählen Sie den Abschnitt **Authentifizierungsmethoden** aus.

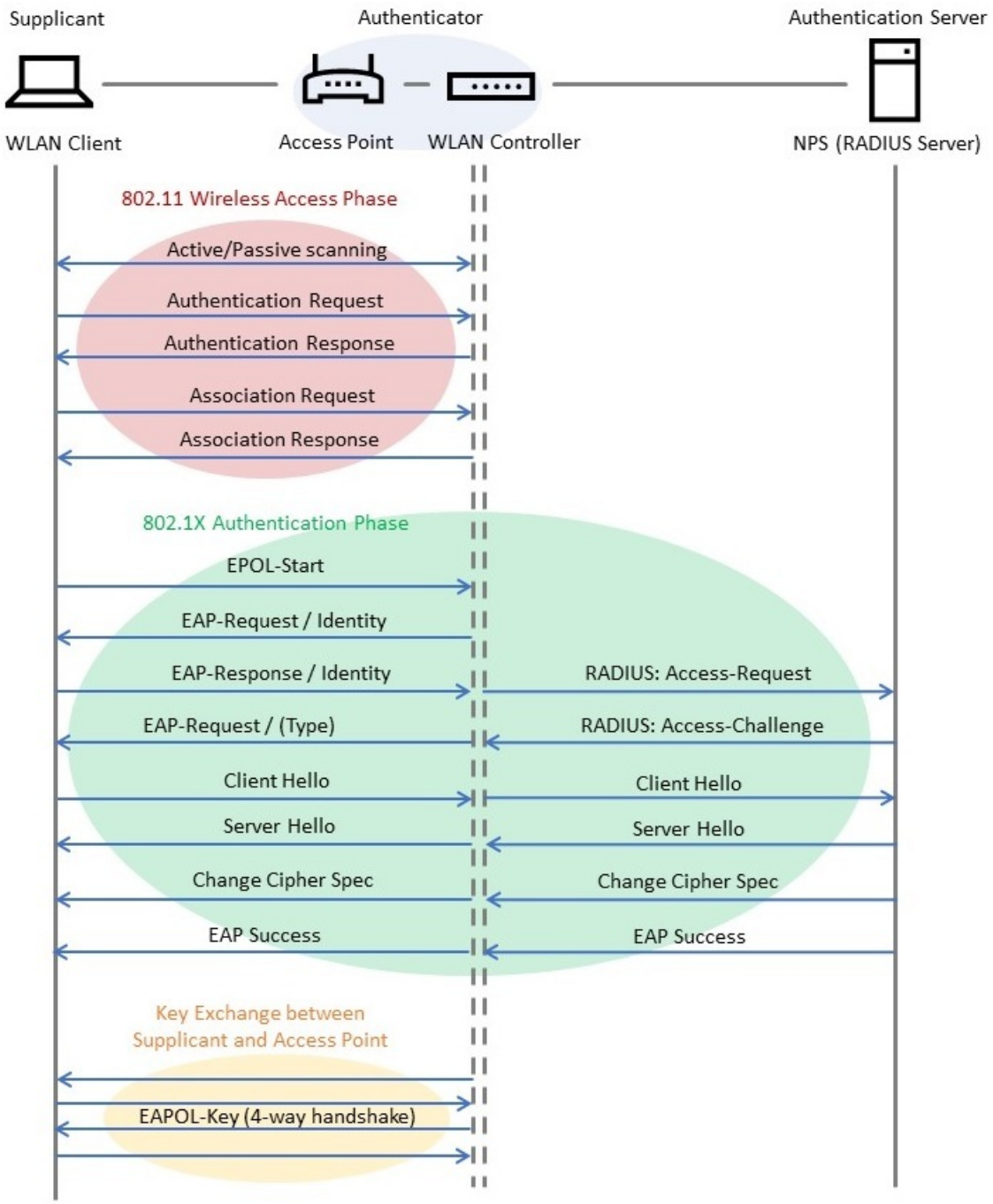


Das CAPI2-Ereignisprotokoll eignet sich für die Behandlung von Problemen mit dem Zertifikat. Dieses Protokoll ist standardmäßig nicht aktiviert. Sie können dieses Protokoll aktivieren, indem Sie die **\Anwendungs--und Dienste-Logs\Microsoft\Windows\CAPI2 der Ereignisanzeige**erweitern, mit der rechten Maustaste auf **Operational** klicken und dann auf **Protokoll aktivieren**klicken.

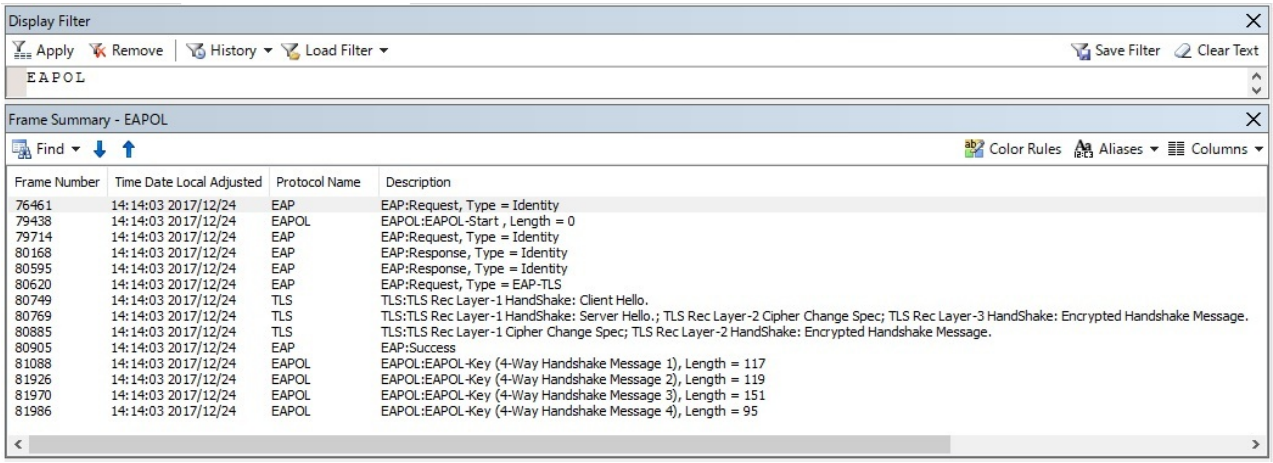


Im folgenden Artikel wird erläutert, wie Sie CAPI2-Ereignisprotokolle analysieren: Problembehandlung bei PKI-Problemen unter Windows Vista.

Bei der Behandlung komplexer 802.1 x-Authentifizierungsprobleme ist es wichtig, den 802.1 x-Authentifizierungsprozess zu verstehen. Die folgende Abbildung zeigt ein Beispiel für einen drahtlos Verbindungsprozess mit 802.1 x-Authentifizierung:

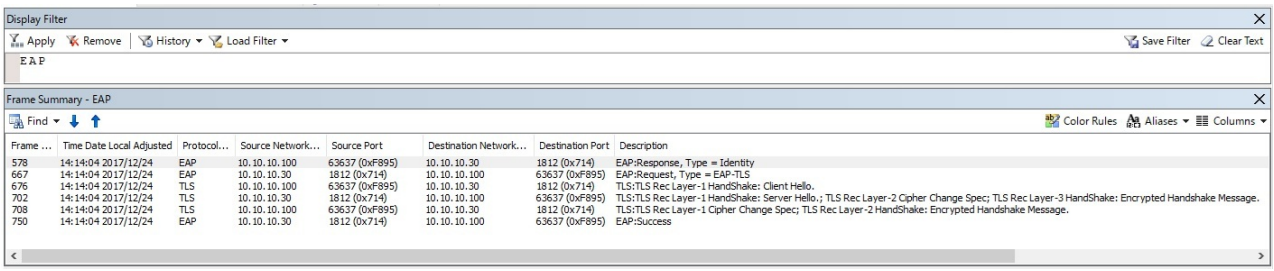


Wenn Sie eine Netzwerkpaketerfassung sowohl auf der Client-als auch auf der Serverseite (NPS) sammeln, können Sie einen Fluss wie den folgenden anzeigen. Geben Sie **EAPOL** in den Anzeige Filter für eine clientseitige Erfassung ein, und **EAP** für eine NPS-Seiten Erfassung. Sehen Sie sich die folgenden Beispiele an:



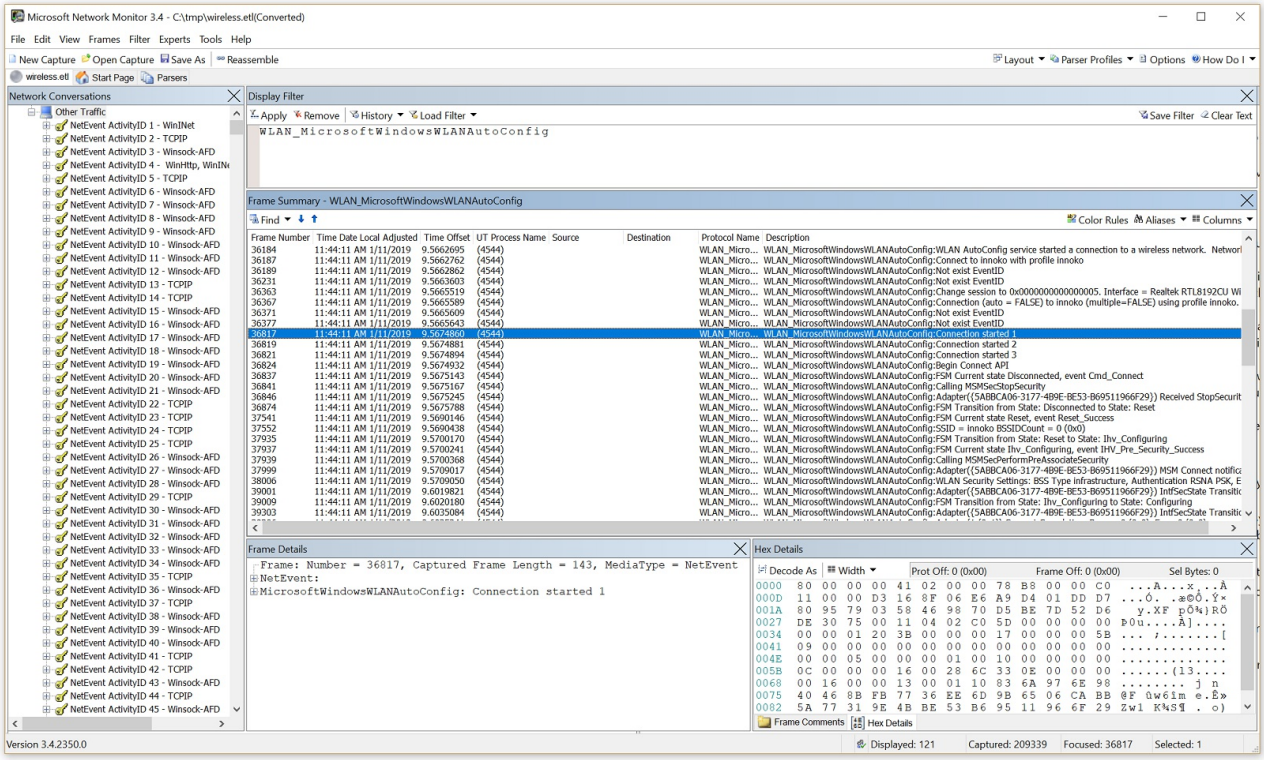
Frame Number	Time Date Local Adjusted	Protocol Name	Description
76461	14:14:03 2017/12/24	EAP	EAP:Request, Type = Identity
79438	14:14:03 2017/12/24	EAPOL	EAPOL:EAPOL-Start , Length = 0
79714	14:14:03 2017/12/24	EAP	EAP:Request, Type = Identity
80168	14:14:03 2017/12/24	EAP	EAP:Response, Type = Identity
80595	14:14:03 2017/12/24	EAP	EAP:Response, Type = Identity
80620	14:14:03 2017/12/24	EAP	EAP:Request, Type = EAP-TLS
80749	14:14:03 2017/12/24	TLS	TLS:TLS Rec Layer-1 HandShake: Client Hello.
80769	14:14:03 2017/12/24	TLS	TLS:TLS Rec Layer-1 HandShake: Server Hello.; TLS Rec Layer-2 Cipher Change Spec; TLS Rec Layer-3 HandShake: Encrypted Handshake Message.
80885	14:14:03 2017/12/24	TLS	TLS:TLS Rec Layer-1 Cipher Change Spec; TLS Rec Layer-2 HandShake: Encrypted Handshake Message.
80905	14:14:03 2017/12/24	EAP	EAP:Success
81088	14:14:03 2017/12/24	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 1), Length = 117
81926	14:14:03 2017/12/24	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 2), Length = 119
81970	14:14:03 2017/12/24	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 3), Length = 151
81986	14:14:03 2017/12/24	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 4), Length = 95

-clientseitige Paket Aufnahmedaten



auf*NPS-Seite mit Paket Aufnahmedaten*

> **NOTE**
>
> Wenn Sie über eine drahtlose Ablaufverfolgung verfügen, können Sie auch ETL-Dateien mit dem Netzwerkmonitor anzeigen und die **ONEX_MicrosoftWindowsOneX** und **WLAN_MicrosoftWindowsWLANAutoConfig** Netzwerkmonitor Filter anwenden. Befolgen Sie die Anweisungen im Menü " **Hilfe** " des Netzwerkmonitors, um den reqired- Parser bei Bedarf zu laden. Sehen Sie sich das Beispiel unten an.



Überwachungsrichtlinie

NPS-Überwachungsrichtlinien (Ereignisprotokollierung) für Verbindungs Erfolg und-Fehler sind standardmäßig aktiviert. Wenn Sie feststellen, dass eine oder beide Protokollierungstypen deaktiviert sind, führen Sie die folgenden Schritte zur Problembehandlung aus.

Zeigen Sie die aktuellen Überwachungsrichtlinieneinstellungen an, indem Sie auf dem NPS-Server den folgenden Befehl ausführen:

```
auditpol /get /subcategory:"Network Policy Server"
```

Wenn sowohl Erfolgs-als auch Fehlerereignisse aktiviert sind, sollte die Ausgabe wie folgt lauten:

```
System audit policy
Category/Subcategory                      Setting
Logon/Logoff
  Network Policy Server                   Success and Failure
```

Wenn "keine Überwachung" angezeigt wird, können Sie diesen Befehl ausführen, um ihn zu aktivieren:

```
auditpol /set /subcategory:"Network Policy Server" /success:enable /failure:enable
```

Auch wenn die Überwachungsrichtlinie anscheinend vollständig aktiviert ist, können Sie diese Einstellung manchmal deaktivieren und dann wieder aktivieren. Sie können die Überwachung des Netzwerkrichtlinienservers auch über Gruppenrichtlinien aktivieren/abmelden. Die Einstellung "Erfolg/Fehler" finden Sie unter **Computer Konfiguration – > Richtlinien – > Windows-Einstellungen – > Sicherheitseinstellungen – > erweiterte Überwachungsrichtlinienkonfiguration – > Überwachungsrichtlinien – #a5 Anmelde-und Abmelden-> Überwachungsnetzwerk Richtlinien Server**.

Weitere Verweise

Behandeln von Problemen mit Windows Vista 802,11-Drahtlosverbindungen
Behandeln von Problemen mit Windows Vista Secure 802,3-Kabelverbindungen

Datensammlung für die Problembehandlung der 802.1X-Authentifizierung

07.06.2019 • 8 minutes to read

Führen Sie die folgenden Schritte aus, um Daten zu sammeln, die zur Behandlung von Problemen mit der 802.1 x-Authentifizierung verwendet werden können. Wenn Sie Daten gesammelt haben, lesen Sie Erweiterte Problembehandlung bei der 802.1 x-Authentifizierung.

Aufzeichnen von Wireless/Wired-Funktions Protokollen

Führen Sie die folgenden Schritte aus, um drahtlos-und kabelgebundene Protokolle unter Windows und Windows Server zu sammeln:

1. Erstellen Sie C:\MSLOG auf dem Clientcomputer, um aufgezeichnete Protokolle zu speichern.
2. Starten Sie eine Eingabeaufforderung mit erhöhten Rechten auf dem Clientcomputer, und führen Sie die folgenden Befehle aus, um ein RAS-Ablaufverfolgungsprotokoll und ein drahtlos/verkabeltes Szenario-Protokoll zu starten.

   Wireless Windows 8,1 und Windows 10:

   ```
   netsh ras set tracing * enabled
   netsh trace start scenario=wlan,wlan_wpp,wlan_dbg,wireless_dbg globallevel=0xff capture=yes
   maxsize=1024 tracefile=C:\MSLOG\%COMPUTERNAME%_wireless_cli.etl
   ```

   Wireless Windows 7 und Windows 8:

   ```
   netsh ras set tracing * enabled
   netsh trace start scenario=wlan,wlan_wpp,wlan_dbg globallevel=0xff capture=yes maxsize=1024
   tracefile=C:\MSLOG\%COMPUTERNAME%_wireless_cli.etl
   ```

   Kabelgebundener Client, unabhängig von der Version

   ```
   netsh ras set tracing * enabled
   netsh trace start scenario=lan globallevel=0xff capture=yes maxsize=1024
   tracefile=C:\MSLOG\%COMPUTERNAME%_wired_cli.etl
   ```

3. Führen Sie den folgenden Befehl aus, um die CAPI2-Protokollierung zu aktivieren und die Größe zu erhöhen:

   ```
   wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:true
   wevtutil sl Microsoft-Windows-CAPI2/Operational /ms:104857600
   ```

4. Erstellen Sie C:\MSLOG auf dem NPS, um aufgezeichnete Protokolle zu speichern.
5. Starten Sie eine Eingabeaufforderung mit erhöhten Rechten auf dem NPS-Server, und führen Sie die folgenden Befehle aus, um ein RAS-Ablaufverfolgungsprotokoll und ein drahtlos/verkabeltes Szenario-Protokoll zu starten:

Windows Server 2012 R2, Drahtlosnetzwerk für Windows Server 2016:

```
netsh ras set tracing * enabled
netsh trace start scenario=wlan,wlan_wpp,wlan_dbg,wireless_dbg globallevel=0xff capture=yes
maxsize=1024 tracefile=C:\MSLOG\%COMPUTERNAME%_wireless_nps.etl
```

Windows Server 2008 R2, Drahtlosnetzwerk für Windows Server 2012

```
netsh ras set tracing * enabled
netsh trace start scenario=wlan,wlan_wpp,wlan_dbg globallevel=0xff capture=yes maxsize=1024
tracefile=C:\MSLOG\%COMPUTERNAME%_wireless_nps.etl
```

Kabelgebundenes Netzwerk

```
netsh ras set tracing * enabled
netsh trace start scenario=lan globallevel=0xff capture=yes maxsize=1024
tracefile=C:\MSLOG\%COMPUTERNAME%_wired_nps.etl
```

6. Führen Sie den folgenden Befehl aus, um die CAPI2-Protokollierung zu aktivieren und die Größe zu erhöhen:

```
wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:true
wevtutil sl Microsoft-Windows-CAPI2/Operational /ms:104857600
```

7. Führen Sie den folgenden Befehl an der Eingabeaufforderung auf dem Clientcomputer aus, und starten Sie PSR, um Bildschirmbilder zu erfassen:

> **NOTE**
> Wenn Sie auf die Maustaste klicken, blinkt der Cursor beim Aufzeichnen eines Bildschirms rot.

```
psr /start /output c:\MSLOG\%computername%_psr.zip /maxsc 100
```

8. Reproduzieren Sie das Problem.
9. Führen Sie den folgenden Befehl auf dem Clientcomputer aus, um die PSR-Aufzeichnung zu beenden:

```
psr /stop
```

10. Führen Sie die folgenden Befehle an der Eingabeaufforderung auf dem NPS-Server aus.

    - So beenden Sie das RAS-Ablaufverfolgungsprotokoll und das Protokoll für drahtlose Szenarien:

      ```
      netsh trace stop
      netsh ras set tracing * disabled
      ```

    - So deaktivieren und kopieren Sie das CAPI2-Protokoll:

```
wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:false
wevtutil.exe epl Microsoft-Windows-CAPI2/Operational C:\MSLOG\%COMPUTERNAME%_CAPI2.evtx
```

11. Führen Sie die folgenden Befehle auf dem Client-PC aus.

    - So beenden Sie das RAS-Ablaufverfolgungsprotokoll und das Protokoll für drahtlose Szenarien:

    ```
    netsh trace stop
    netsh ras set tracing * disabled
    ```

    - So deaktivieren und kopieren Sie das CAPI2-Protokoll:

    ```
    wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:false
    wevtutil.exe epl Microsoft-Windows-CAPI2/Operational C:\MSLOG\%COMPUTERNAME%_CAPI2.evtx
    ```

12. Speichern Sie die folgenden Protokolle auf dem Client und dem NPS:

    Client

    - C:\MSLOG%computername%_psr.zip
    - C:\MSLOG%COMPUTERNAME%_CAPI2.evtx
    - C:\MSLOG%COMPUTERNAME%_wireless_cli.etl
    - C:\MSLOG%COMPUTERNAME%_wireless_cli.cab
    - Alle Protokolldateien und Ordner in%SystemRoot%\Tracing

    NPS

    - C:\MSLOG%COMPUTERNAME%_CAPI2.evtx
    - C:\MSLOG%Computername%_wireless_nps.ETL (% Computername% _wired_nps. ETL für kabelgebundenes Szenario)
    - C:\MSLOG%Computername%_wireless_nps.cab (% Computername% _wired_nps. cab für kabelgebundenes Szenario)
    - Alle Protokolldateien und Ordner in%SystemRoot%\Tracing

Speichern von Umgebungs-und Konfigurationsinformationen

Auf dem Windows-Client

1. Erstellen Sie C:\MSLOG, um aufgezeichnete Protokolle zu speichern.
2. Starten Sie eine Eingabeaufforderung als Administrator.
3. Führen Sie die folgenden Befehle aus.

    - Umgebungsinformationen und Status der Gruppenrichtlinienanwendung

    ```
    gpresult /H C:\MSLOG\%COMPUTERNAME%_gpresult.htm
    msinfo32 /report c:\MSLOG\%COMPUTERNAME%_msinfo32.txt
    ipconfig /all > c:\MSLOG\%COMPUTERNAME%_ipconfig.txt
    route print > c:\MSLOG\%COMPUTERNAME%_route_print.txt
    ```

    - Ereignisprotokolle

```
wevtutil epl Application c:\MSLOG\%COMPUTERNAME%_Application.evtx
wevtutil epl System c:\MSLOG\%COMPUTERNAME%_System.evtx
wevtutil epl Security c:\MSLOG\%COMPUTERNAME%_Security.evtx
wevtutil epl Microsoft-Windows-GroupPolicy/Operational
C:\MSLOG\%COMPUTERNAME%_GroupPolicy_Operational.evtx
wevtutil epl "Microsoft-Windows-WLAN-AutoConfig/Operational" c:\MSLOG\%COMPUTERNAME%_Microsoft-Windows-
WLAN-AutoConfig-Operational.evtx
wevtutil epl "Microsoft-Windows-Wired-AutoConfig/Operational" c:\MSLOG\%COMPUTERNAME%_Microsoft-
Windows-Wired-AutoConfig-Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-CredentialRoaming/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-CredentialRoaming_Operational.evtx
wevtutil epl Microsoft-Windows-CertPoleEng/Operational
c:\MSLOG\%COMPUTERNAME%_CertPoleEng_Operational.evtx
```

- Für Windows 8 und höher können Sie auch diese Befehle für Ereignisprotokolle ausführen:

```
wevtutil epl Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-System_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-Lifecycle-User/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-User_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServices-Deployment/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServices-Deployment_Operational.evtx
```

- Informationen zum Speichern von Zertifikaten:

```
certutil -v -silent -store MY > c:\MSLOG\%COMPUTERNAME%_cert-Personal-Registry.txt
certutil -v -silent -store ROOT > c:\MSLOG\%COMPUTERNAME%_cert-TrustedRootCA-Registry.txt
certutil -v -silent -store -grouppolicy ROOT > c:\MSLOG\%COMPUTERNAME%_cert-TrustedRootCA-
GroupPolicy.txt
certutil -v -silent -store -enterprise ROOT > c:\MSLOG\%COMPUTERNAME%_TrustedRootCA-Enterprise.txt
certutil -v -silent -store TRUST > c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-Reg.txt
certutil -v -silent -store -grouppolicy TRUST > c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-
GroupPolicy.txt
certutil -v -silent -store -enterprise TRUST > c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-
Enterprise.txt
certutil -v -silent -store CA > c:\MSLOG\%COMPUTERNAME%_cert-IntermediateCA-Registry.txt
certutil -v -silent -store -grouppolicy CA > c:\MSLOG\%COMPUTERNAME%_cert-IntermediateCA-
GroupPolicy.txt
certutil -v -silent -store -enterprise CA > c:\MSLOG\%COMPUTERNAME%_cert-Intermediate-Enterprise.txt
certutil -v -silent -store AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-Registry.txt
certutil -v -silent -store -grouppolicy AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-
GroupPolicy.txt
certutil -v -silent -store -enterprise AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-
Enterprise.txt
certutil -v -silent -store SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-Registry.txt
certutil -v -silent -store -grouppolicy SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-
GroupPolicy.txt
certutil -v -silent -store -enterprise SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-
Enterprise.txt
certutil -v -silent -store -enterprise NTAUTH > c:\MSLOG\%COMPUTERNAME%_cert-NtAuth-Enterprise.txt
certutil -v -silent -user -store MY > c:\MSLOG\%COMPUTERNAME%_cert-User-Personal-Registry.txt
certutil -v -silent -user -store ROOT > c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-Registry.txt
certutil -v -silent -user -store -enterprise ROOT > c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-
Enterprise.txt
certutil -v -silent -user -store TRUST > c:\MSLOG\%COMPUTERNAME%_cert-User-EnterpriseTrust-Registry.txt
certutil -v -silent -user -store -grouppolicy TRUST > c:\MSLOG\%COMPUTERNAME%_cert-User-
EnterpriseTrust-GroupPolicy.txt
certutil -v -silent -user -store CA > c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-Registry.txt
certutil -v -silent -user -store -grouppolicy CA > c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-
GroupPolicy.txt
certutil -v -silent -user -store Disallowed > c:\MSLOG\%COMPUTERNAME%_cert-User-UntrustedCertificates-
Registry.txt
certutil -v -silent -user -store -grouppolicy Disallowed > c:\MSLOG\%COMPUTERNAME%_cert-User-
UntrustedCertificates-GroupPolicy.txt
certutil -v -silent -user -store AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-3rdPartyRootCA-
Registry.txt
certutil -v -silent -user -store -grouppolicy AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-
3rdPartyRootCA-GroupPolicy.txt
certutil -v -silent -user -store SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-SmartCardRoot-
Registry.txt
certutil -v -silent -user -store -grouppolicy SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-
SmartCardRoot-GroupPolicy.txt
certutil -v -silent -user -store UserDS > c:\MSLOG\%COMPUTERNAME%_cert-User-UserDS.txt
```

- Wireless LAN-Clientinformationen:

```
netsh wlan show all > c:\MSLOG\%COMPUTERNAME%_wlan_show_all.txt
netsh wlan export profile folder=c:\MSLOG\
```

- Informationen zu verdrahteten LAN-Clients

```
netsh lan show interfaces > c:\MSLOG\%computername%_lan_interfaces.txt
netsh lan show profiles > c:\MSLOG\%computername%_lan_profiles.txt
netsh lan show settings > c:\MSLOG\%computername%_lan_settings.txt
netsh lan export profile folder=c:\MSLOG\
```

4. Speichern der in C:\MSLOG. gespeicherten Protokolle

Auf NPS

1. Erstellen Sie C:\MSLOG, um aufgezeichnete Protokolle zu speichern.
2. Starten Sie eine Eingabeaufforderung als Administrator.
3. Führen Sie die folgenden Befehle aus.

- Umgebungsinformationen und Anwendungsstatus der Gruppenrichtlinien:

```
gpresult /H C:\MSLOG\%COMPUTERNAME%_gpresult.txt
msinfo32 /report c:\MSLOG\%COMPUTERNAME%_msinfo32.txt
ipconfig /all > c:\MSLOG\%COMPUTERNAME%_ipconfig.txt
route print > c:\MSLOG\%COMPUTERNAME%_route_print.txt
```

- Ereignisprotokolle:

```
wevtutil epl Application c:\MSLOG\%COMPUTERNAME%_Application.evtx
wevtutil epl System c:\MSLOG\%COMPUTERNAME%_System.evtx
wevtutil epl Security c:\MSLOG\%COMPUTERNAME%_Security.evtx
wevtutil epl Microsoft-Windows-GroupPolicy/Operational
c:\MSLOG\%COMPUTERNAME%_GroupPolicy_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-CredentialRoaming/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-CredentialRoaming_Operational.evtx
wevtutil epl Microsoft-Windows-CertPoleEng/Operational
c:\MSLOG\%COMPUTERNAME%_CertPoleEng_Operational.evtx
```

- Führen Sie die folgenden 3 Befehle unter Windows Server 2012 und höher aus:

```
wevtutil epl Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-System_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-Lifecycle-User/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-User_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServices-Deployment/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServices-Deployment_Operational.evtx
```

- Informationen zum Informationsspeicher des Zertifikats

```
certutil -v -silent -store MY > c:\MSLOG\%COMPUTERNAME%_cert-Personal-Registry.txt
certutil -v -silent -store ROOT > c:\MSLOG\%COMPUTERNAME%_cert-TrustedRootCA-Registry.txt
certutil -v -silent -store -grouppolicy ROOT > c:\MSLOG\%COMPUTERNAME%_cert-TrustedRootCA-
GroupPolicy.txt
certutil -v -silent -store -enterprise ROOT > c:\MSLOG\%COMPUTERNAME%_TrustedRootCA-Enterprise.txt
certutil -v -silent -store TRUST > c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-Reg.txt
certutil -v -silent -store -grouppolicy TRUST > c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-
GroupPolicy.txt
certutil -v -silent -store -enterprise TRUST > c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-
Enterprise.txt
certutil -v -silent -store CA > c:\MSLOG\%COMPUTERNAME%_cert-IntermediateCA-Registry.txt
certutil -v -silent -store -grouppolicy CA > c:\MSLOG\%COMPUTERNAME%_cert-IntermediateCA-
GroupPolicy.txt
certutil -v -silent -store -enterprise CA > c:\MSLOG\%COMPUTERNAME%_cert-Intermediate-Enterprise.txt
certutil -v -silent -store AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-Registry.txt
certutil -v -silent -store -grouppolicy AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-
GroupPolicy.txt
certutil -v -silent -store -enterprise AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-
Enterprise.txt
certutil -v -silent -store SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-Registry.txt
certutil -v -silent -store -grouppolicy SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-
GroupPolicy.txt
certutil -v -silent -store -enterprise SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-
Enterprise.txt
certutil -v -silent -store -enterprise NTAUTH > c:\MSLOG\%COMPUTERNAME%_cert-NtAuth-Enterprise.txt
certutil -v -silent -user -store MY > c:\MSLOG\%COMPUTERNAME%_cert-User-Personal-Registry.txt
certutil -v -silent -user -store ROOT > c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-Registry.txt
certutil -v -silent -user -store -enterprise ROOT > c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-
Enterprise.txt
certutil -v -silent -user -store TRUST > c:\MSLOG\%COMPUTERNAME%_cert-User-EnterpriseTrust-Registry.txt
certutil -v -silent -user -store -grouppolicy TRUST > c:\MSLOG\%COMPUTERNAME%_cert-User-
EnterpriseTrust-GroupPolicy.txt
certutil -v -silent -user -store CA > c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-Registry.txt
certutil -v -silent -user -store -grouppolicy CA > c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-
GroupPolicy.txt
certutil -v -silent -user -store Disallowed > c:\MSLOG\%COMPUTERNAME%_cert-User-UntrustedCertificates-
Registry.txt
certutil -v -silent -user -store -grouppolicy Disallowed > c:\MSLOG\%COMPUTERNAME%_cert-User-
UntrustedCertificates-GroupPolicy.txt
certutil -v -silent -user -store AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-3rdPartyRootCA-
Registry.txt
certutil -v -silent -user -store -grouppolicy AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-
3rdPartyRootCA-GroupPolicy.txt
certutil -v -silent -user -store SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-SmartCardRoot-
Registry.txt
certutil -v -silent -user -store -grouppolicy SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-
SmartCardRoot-GroupPolicy.txt
certutil -v -silent -user -store UserDS > c:\MSLOG\%COMPUTERNAME%_cert-User-UserDS.txt
```

- NPS-Konfigurationsinformationen:

```
netsh nps show config > C:\MSLOG\%COMPUTERNAME%_nps_show_config.txt
netsh nps export filename=C:\MSLOG\%COMPUTERNAME%_nps_export.xml exportPSK=YES
```

4. Führen Sie die folgenden Schritte aus, um ein NPS-Kontoführungsprotokoll zu speichern.

   a. Öffnen Sie die **Verwaltungstools #a0 Netzwerkrichtlinien Server**.
   b. Wählen Sie im Netzwerkrichtlinien Server-Verwaltungstool **** im linken Bereich Accounting aus.
   c. Klicken Sie auf **Protokolldateieigenschaften ändern**.
   d. Notieren Sie sich auf der Registerkarte **Protokoll** Datei die Namenskonvention für Protokolldateien, die als **Name** angezeigt wird, und den Speicherort der Protokolldatei im Feld **Verzeichnis** .
   e. Kopieren der Protokolldatei in C:\MSLOG.

5. Speichern der in C:\MSLOG. gespeicherten Protokolle

Zertifizierungsstelle (ca) (optional)

1. Starten Sie auf einer Zertifizierungsstelle eine Eingabeaufforderung als Administrator. Erstellen Sie C:\MSLOG, um aufgezeichnete Protokolle zu speichern.
2. Führen Sie die folgenden Befehle aus.

   - Anwendungsstatus von Umgebungsinformationen und Gruppenrichtlinien

```
gpresult /H C:\MSLOG\%COMPUTERNAME%_gpresult.txt
msinfo32 /report c:\MSLOG\%COMPUTERNAME%_msinfo32.txt
ipconfig /all > c:\MSLOG\%COMPUTERNAME%_ipconfig.txt
route print > c:\MSLOG\%COMPUTERNAME%_route_print.txt
```

   - Ereignisprotokolle

```
wevtutil epl Application c:\MSLOG\%COMPUTERNAME%_Application.evtx
wevtutil epl System c:\MSLOG\%COMPUTERNAME%_System.evtx
wevtutil epl Security c:\MSLOG\%COMPUTERNAME%_Security.evtx
wevtutil epl Microsoft-Windows-GroupPolicy/Operational
c:\MSLOG\%COMPUTERNAME%_GroupPolicy_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-CredentialRoaming/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-CredentialRoaming_Operational.evtx
wevtutil epl Microsoft-Windows-CertPoleEng/Operational
c:\MSLOG\%COMPUTERNAME%_CertPoleEng_Operational.evtx
```

   - Führen Sie die folgenden 3 Zeilen unter Windows 2012 und nach oben aus.

```
wevtutil epl Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-System_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-Lifecycle-User/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-User_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServices-Deployment/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServices-Deployment_Operational.evtx
```

   - Informationen zum Informationsspeicher des Zertifikats

```
certutil -v -silent -store MY > c:\MSLOG\%COMPUTERNAME%_cert-Personal-Registry.txt
certutil -v -silent -store ROOT > c:\MSLOG\%COMPUTERNAME%_cert-TrustedRootCA-Registry.txt
certutil -v -silent -store -grouppolicy ROOT > c:\MSLOG\%COMPUTERNAME%_cert-TrustedRootCA-
GroupPolicy.txt
certutil -v -silent -store -enterprise ROOT > c:\MSLOG\%COMPUTERNAME%_TrustedRootCA-Enterprise.txt
certutil -v -silent -store TRUST > c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-Reg.txt
certutil -v -silent -store -grouppolicy TRUST > c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-
GroupPolicy.txt
certutil -v -silent -store -enterprise TRUST > c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-
Enterprise.txt
certutil -v -silent -store CA > c:\MSLOG\%COMPUTERNAME%_cert-IntermediateCA-Registry.txt
certutil -v -silent -store -grouppolicy CA > c:\MSLOG\%COMPUTERNAME%_cert-IntermediateCA-
GroupPolicy.txt
certutil -v -silent -store -enterprise CA > c:\MSLOG\%COMPUTERNAME%_cert-Intermediate-Enterprise.txt
certutil -v -silent -store AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-Registry.txt
certutil -v -silent -store -grouppolicy AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-
GroupPolicy.txt
certutil -v -silent -store -enterprise AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-
Enterprise.txt
certutil -v -silent -store SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-Registry.txt
certutil -v -silent -store -grouppolicy SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-
GroupPolicy.txt
certutil -v -silent -store -enterprise SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-
Enterprise.txt
certutil -v -silent -store -enterprise NTAUTH > c:\MSLOG\%COMPUTERNAME%_cert-NtAuth-Enterprise.txt
certutil -v -silent -user -store MY > c:\MSLOG\%COMPUTERNAME%_cert-User-Personal-Registry.txt
certutil -v -silent -user -store ROOT > c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-Registry.txt
certutil -v -silent -user -store -enterprise ROOT > c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-
Enterprise.txt
certutil -v -silent -user -store TRUST > c:\MSLOG\%COMPUTERNAME%_cert-User-EnterpriseTrust-Registry.txt
certutil -v -silent -user -store -grouppolicy TRUST > c:\MSLOG\%COMPUTERNAME%_cert-User-
EnterpriseTrust-GroupPolicy.txt
certutil -v -silent -user -store CA > c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-Registry.txt
certutil -v -silent -user -store -grouppolicy CA > c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-
GroupPolicy.txt
certutil -v -silent -user -store Disallowed > c:\MSLOG\%COMPUTERNAME%_cert-User-UntrustedCertificates-
Registry.txt
certutil -v -silent -user -store -grouppolicy Disallowed > c:\MSLOG\%COMPUTERNAME%_cert-User-
UntrustedCertificates-GroupPolicy.txt
certutil -v -silent -user -store AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-3rdPartyRootCA-
Registry.txt
certutil -v -silent -user -store -grouppolicy AuthRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-
3rdPartyRootCA-GroupPolicy.txt
certutil -v -silent -user -store SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-SmartCardRoot-
Registry.txt
certutil -v -silent -user -store -grouppolicy SmartCardRoot > c:\MSLOG\%COMPUTERNAME%_cert-User-
SmartCardRoot-GroupPolicy.txt
certutil -v -silent -user -store UserDS > c:\MSLOG\%COMPUTERNAME%_cert-User-UserDS.txt
```

- Informationen zur CA-Konfiguration

```
reg save HKLM\System\CurrentControlSet\Services\CertSvc c:\MSLOG\%COMPUTERNAME%_CertSvc.hiv
reg export HKLM\System\CurrentControlSet\Services\CertSvc c:\MSLOG\%COMPUTERNAME%_CertSvc.txt
reg save HKLM\SOFTWARE\Microsoft\Cryptography c:\MSLOG\%COMPUTERNAME%_Cryptography.hiv
reg export HKLM\SOFTWARE\Microsoft\Cryptography c:\MSLOG\%COMPUTERNAME%_Cryptography.txt
```

3. Kopieren Sie die folgenden Dateien, falls vorhanden, in C:\MSLOG:%windir%\CAPolicy.inf
4. Melden Sie sich bei einem Domänencontroller an, und erstellen Sie C:\MSLOG, um aufgezeichnete Protokolle zu speichern.
5. Starten Sie Windows PowerShell als Administrator.
6. Führen Sie die folgenden PowerShell-Cmdlets aus. Ersetzen Sie den Domänennamen in ";.. , DC = Test, DC = lokal "; mit dem entsprechenden Domänennamen. Das Beispiel zeigt Befehle für "; Test. local"; Domäne.

```
Import-Module ActiveDirectory
Get-ADObject -SearchBase ";CN=Public Key Services,CN=Services,CN=Configuration,DC=test,DC=local"; -
Filter * -Properties * | fl * > C:\MSLOG\Get-ADObject_$Env:COMPUTERNAME.txt
```

7. Speichern Sie die folgenden Protokolle.
   - Alle Dateien in C:\MSLOG auf der Zertifizierungsstelle
   - Alle Dateien in C:\MSLOG auf dem Domänencontroller

Erweiterte Problembehandlung für TCP/IP-Probleme

01.06.2019 • 2 minutes to read

In diesen Themen erfahren Sie, wie häufige Probleme in einer TCP/IP-Netzwerkumgebung behoben werden können.

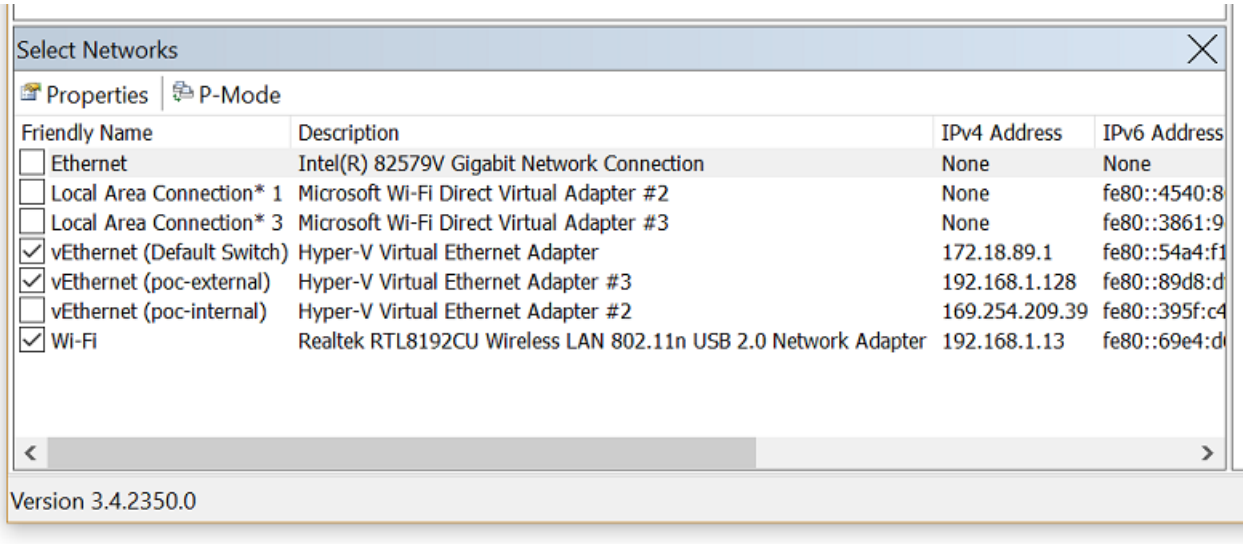
- Sammeln von Daten mithilfe des Netzwerkmonitors
- Problembehandlung für die TCP/IP-Verbindung
- Problembehandlung für Portmangel
- Problembehandlung für Remote Procedure Call (RPC)-Fehler

Sammeln von Daten mithilfe des Netzwerkmonitors

01.06.2019 • 2 minutes to read

In diesem Thema erfahren Sie, wie Sie den Microsoft-Netzwerk Monitor 3,4 verwenden, der ein Tool zum Aufzeichnen von Netzwerkdatenverkehr ist.

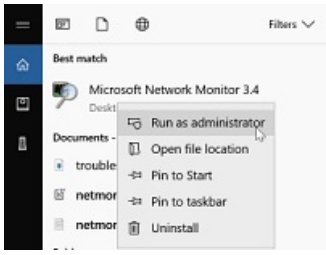
Um zu beginnen, Laden Sie NM34_x64. exe herunter, und führenSie es aus. Wenn Sie den Netzwerk Monitor installieren, wird sein Treiber installiert und mit allen auf dem Gerät installierten Netzwerkadaptern verknüpft. Wie in der folgenden Abbildung gezeigt, können Sie die gleichen Einstellungen für die Adaptereigenschaften sehen.



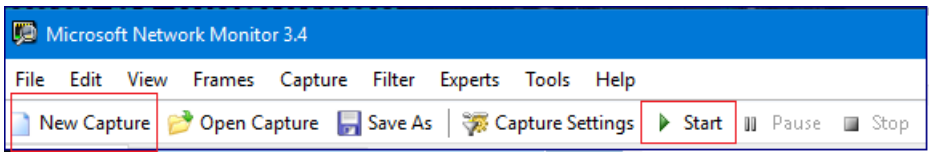
Wenn der Treiber während der Installation mit der Netzwerkschnittstellenkarte (NIC) verbunden wird, wird die NIC neu initialisiert, was zu einem kurzen Netzwerkfehler führen kann.

So erfassen Sie Datenverkehr

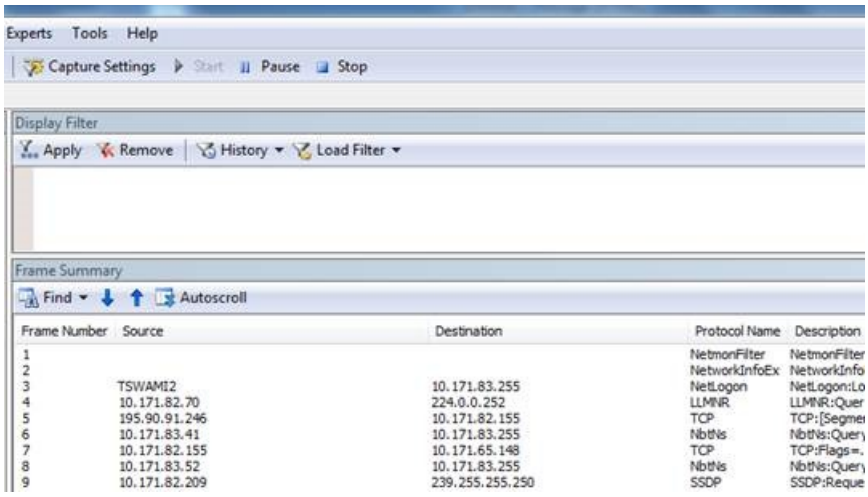
1. Führen Sie Netmon in einem erweiterten Status aus, indem Sie "als Administrator ausführen" auswählen.



2. Der Netzwerk Monitor wird geöffnet, und alle Netzwerkadapter werden angezeigt. Wählen Sie die Netzwerkadapter aus, auf denen Sie den Datenverkehr aufzeichnen möchten, klicken Sie auf **neue Aufzeichnung**, und klicken Sie dann auf **Start**.



3. Reproduzieren Sie das Problem, und Sie werden feststellen, dass der Netzwerk Monitor die Pakete auf dem Kabel packt.



4. Wählen Sie **Beenden**aus, und wechseln Sie zu **Datei #a0 speichern** unter, um die Ergebnisse zu speichern. Standardmäßig wird die Datei als ". Cap"-Datei gespeichert.

Die gespeicherte Datei hat alle Datenströme erfasst, die in die und von den ausgewählten Netzwerkadaptern auf dem lokalen Computer fließen. Ihr Interesse gilt jedoch nur der Untersuchung des Datenverkehrs/der Pakete, die mit dem jeweiligen Verbindungsproblem in Verbindung stehen. Sie müssen also die Netzwerkerfassung filtern, um nur den zugehörigen Datenverkehr anzuzeigen.

Häufig verwendete Filter

- IPv4. Address = = "Client-IP" und IPv4. Address = = "Server-IP"
- TCP. Port = =
- UDP. Port = =
- ICMP
- ARP
- Property. tcpretranmits
- Property. tcprequestfastretransmits
- TCP. Flags. SYN = = 1

> **TIP**
> Wenn Sie die Erfassung für ein bestimmtes Feld filtern möchten und die Syntax für diesen Filter nicht kennen, klicken Sie einfach mit der rechten Maustaste auf das Feld, und wählen Sie ** *den ausgewählten Wert* hinzufügen aus, um den Filter anzuzeigen**.

Netzwerkablaufverfolgungen, die mit den in Windows integrierten **netsh** -Befehlen erfasst werden, sind die Erweiterung "ETL". Diese ETL-Dateien können jedoch zur weiteren Analyse mithilfe des Netzwerkmonitors geöffnet werden.

Weitere Informationen

Einführung in das Filtern mit dem Netzwerk Monitor 3,0
Beispiele für Netzwerk Monitor Filter
Netzwerk Monitor-drahtlos Filterung
Netzwerk Monitor-TCP-Filterung
Netzwerk Monitor-Unterhaltungs Filterung
Einrichten und Sammeln von Netzwerk Aufnahmen mithilfe des Netzwerk Monitor Tools

Problembehandlung für TCP/IP-Verbindung

27.10.2019 • 5 minutes to read

Möglicherweise stoßen Sie auf Verbindungsfehler in den Anwendungs Ende-oder Timeoutfehlern. Zu den häufigsten Szenarien gehören die Anwendungskonnektivität mit einem Datenbankserver, SQL-Timeout-Fehler, BizTalk-Anwendungs Timeoutfehler, RDP-Fehler (Remote Desktop Protokoll), Fehler beim Zugriff auf Dateifreigaben oder allgemeine Konnektivität.

Wenn Sie vermuten, dass das Problem im Netzwerk liegt, erfassen Sie eine Netzwerkablaufverfolgung. Anschließend wird die Netzwerkablaufverfolgung gefiltert. Bei der Problembehandlung von Verbindungsfehlern können Sie in einer Netzwerkerfassung TCP-Reset durchführen, die auf ein Netzwerkproblem hindeuten könnten.

- TCP ist als verbindungsorientiertes und zuverlässiges Protokoll definiert. Eine der Möglichkeiten, wie TCP Dies gewährleistet, ist der Handshake-Prozess. Das Einrichten einer TCP-Sitzung beginnt mit einem 3-Wege-Handshake, gefolgt von Datenübertragung und anschließend einem 4-Wege-Abschluss. Die 4-Wege-Closure, bei der sich Absender und Empfänger beim Schließen der Sitzung einig sind, wird als ansprechend *geschlossen*bezeichnet. Nach dem 4-Wege-Abschluss ermöglicht der Server 4 Minuten Zeit (Standard), während der alle ausstehenden Pakete im Netzwerk verarbeitet werden sollen, dies ist der TIME_WAIT-Zustand. Sobald der TIME_WAIT-Status abgeschlossen ist, werden alle für diese Verbindung zugewiesenen Ressourcen freigegeben.
- TCP-Reset ist ein abrupter Abschluss der Sitzung, wodurch die der Verbindung zugewiesenen Ressourcen sofort freigegeben werden und alle anderen Informationen zur Verbindung gelöscht werden.
- TCP-Reset wird durch das Reset-Flag im TCP-Header auf `1` festgelegt.

Eine Netzwerkablaufverfolgung für die Quelle und das Ziel, mit der Sie den Fluss des Datenverkehrs ermitteln und erkennen können, an welchem Punkt der Fehler beobachtet wird.

In den folgenden Abschnitten werden einige der Szenarien beschrieben, in denen Sie einen Reset sehen.

Paket-DROPS

Wenn ein TCP-Peer TCP-Pakete sendet, für die keine Antwort vom anderen Ende empfangen wird, würde der TCP-Peer die Daten am Ende erneut übertragen, und wenn keine Antwort empfangen wird, würde die Sitzung durch Senden eines ACK-Reset beendet (Bedeutung , erkennt die Anwendung alle Daten, die bisher ausgetauscht wurden, aber aufgrund eines Paket Abfalls, der die Verbindung schließt).

Die gleichzeitigen Netzwerkablaufverfolgungen für Quelle und Ziel werden Ihnen dabei helfen, dieses Verhalten zu überprüfen, wenn auf der Quellseite die Pakete erneut übertragen werden und am Ziel keines dieser Pakete zu sehen ist. Dies würde bedeuten, dass das Netzwerkgerät zwischen Quelle und Ziel die Pakete abwirft.

Wenn der anfängliche TCP-Handshake aufgrund von Paket Abbrüchen fehlschlägt, sehen Sie, dass das TCP-SYN-Paket nur dreimal erneut übertragen wird.

Quellseitige Verbindung mit Port 445:

Apply Remove History Load Filter

```
ipv4.Address==10.10.10.1 and ipv4.Address==10.10.10.2
```

Frame Summary - tcp.port==445

Find Autoscroll

Source	Destination	Protocol Name	Description
10.10.10.1	10.10.10.2	TCP	TCP:Flags=CE....S., SrcPort=59110, DstPort=Microsoft-DS(445), PayloadLen=0, Seq=93
10.10.10.1	10.10.10.2	TCP	TCP:[SynReTransmit #3]Flags=CE....S., SrcPort=59110, DstPort=Microsoft-DS(445), Pay
10.10.10.1	10.10.10.2	TCP	TCP:[SynReTransmit #3]Flags=.....S., SrcPort=59110, DstPort=Microsoft-DS(445), Paylo

Ziel Seite: Wenn Sie denselben Filter anwenden, werden keine Pakete angezeigt.

Apply Remove History Load Filter

```
ipv4.Address==10.10.10.1 and ipv4.Address==10.10.10.2
```

Frame Summary - ipv4.Address==10.10.10.1 and ipv4.Address==10.10.10.2

Find Autoscroll

Source	Destination	Protocol Name	Description

Für die restlichen Daten sendet TCP die Pakete fünfmal erneut.

Quell-192.168.1.62-Seitenablaufverfolgung:

192.168.1.62	192.168.1.2	SMB2	SMB2:C CREATE (0x5), Sh(RWD), DHnQ+MxAc, File=NULL@#559
192.168.1.62	192.168.1.2	TCP	TCP:[ReTransmit #554]Flags=...AP..., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=536, Seq=815994039 - 815994
192.168.1.62	192.168.1.2	TCP	TCP:[ReTransmit #554]Flags=...AP..., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=536, Seq=815994039 - 815994
192.168.1.62	192.168.1.2	TCP	TCP:[ReTransmit #554]Flags=...AP..., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=756, Seq=815994039 - 815994
192.168.1.62	192.168.1.2	TCP	TCP:[ReTransmit #554]Flags=...AP..., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=756, Seq=815994039 - 815994
192.168.1.62	192.168.1.2	TCP	TCP:[ReTransmit #554]Flags=...AP..., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=756, Seq=815994039 - 815994
192.168.1.62	192.168.1.2	TCP	TCP:Flags=...A.R.., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=0, Seq=815994795, Ack=4172207889, Win=0 (sc

Ziel 192.168.1.2-Seitenablaufverfolgung:

Sie würden keine der oben genannten Pakete sehen. Wenden Sie Ihr Netzwerkteam an, um mit den verschiedenen Hops zu untersuchen, und überprüfen Sie, ob eine dieser potenziell zu Abstürzen im Netzwerk führt.

Wenn Sie feststellen, dass die SYN-Pakete das Ziel erreichen, das Ziel aber immer noch nicht reagiert, überprüfen Sie, ob sich der Port, mit dem Sie eine Verbindung herstellen möchten, im Überwachungszustand befindet. (Netstat-Ausgabe hilft). Wenn der Port abgehört und immer noch keine Antwort vorhanden ist, kann es zu einem WFP-Dropdown führen.

Falscher Parameter im TCP-Header

Dieses Verhalten wird angezeigt, wenn die Pakete im Netzwerk von mittleren Geräten geändert werden und TCP auf dem Empfänger Ende das Paket nicht akzeptieren kann, beispielsweise die zu ändernde Sequenznummer oder Pakete, die von einem mittleren Gerät wiedergegeben werden, indem die Sequenznummer geändert wird. Die gleichzeitige Netzwerkablaufverfolgung auf Quelle und Ziel kann Ihnen erneut mitteilen, ob ein TCP-Header geändert wird. Beginnen Sie, indem Sie die Quell-und Ziel Ablaufverfolgung vergleichen, können Sie feststellen, ob sich die Pakete selbst ändern oder ob neue Pakete das Ziel für die Quelle erreichen.

In diesem Fall benötigen Sie erneut Hilfe vom Netzwerkteam, um ein solches Gerät zu identifizieren, das Pakete ändert oder Pakete an das Ziel wiedergibt. Die häufigsten sind RiverBed-Geräte oder WAN-Beschleuniger.

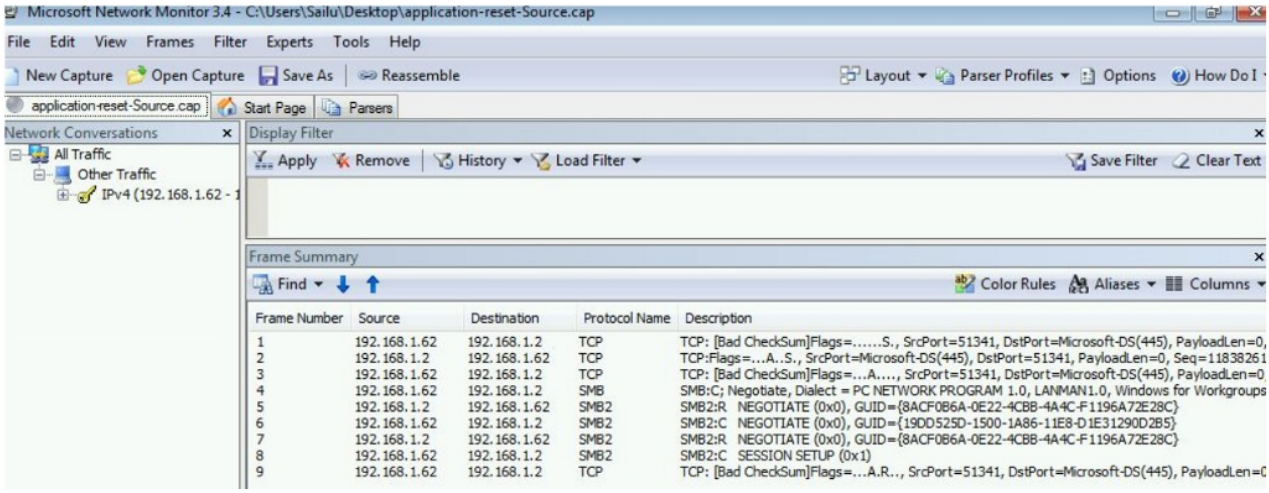
Anwendungs seitige Zurücksetzung

Wenn Sie festgestellt haben, dass die Zurücksetzung nicht auf erneute Übertragungen oder fehlerhafte Parameter oder Pakete zurückzuführen ist, die mithilfe der Netzwerkablaufverfolgung geändert wurden, haben Sie den Reset auf Anwendungsebene eingeschränkt.

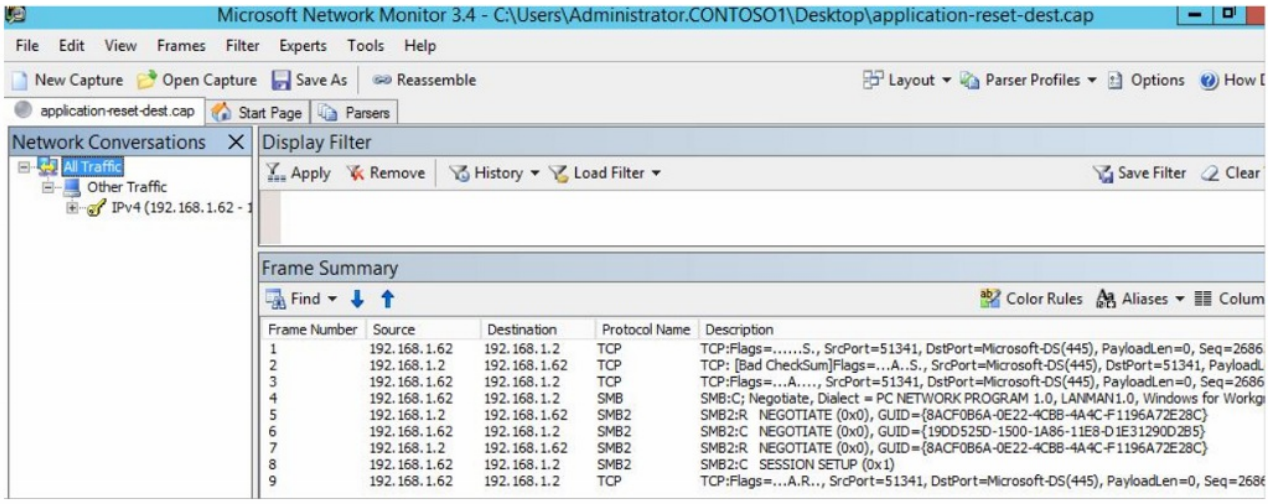
Die Anwendung wird zurückgesetzt, `1` wenn das Bestätigungskennzeichen zusammen mit dem Reset-Flag festgelegt ist. Dies würde bedeuten, dass der Server den Empfang des Pakets bestätigt, die Verbindung aber aus irgendeinem Grund nicht akzeptiert wird. Dies ist der Fall, wenn die Anwendung, die das Paket empfangen hat, etwas nicht gefällt hat.

In den folgenden Screenshots sehen Sie, dass die Pakete, die auf der Quelle und dem Ziel angezeigt werden, ohne Änderungen oder Ausfälle identisch sind, es wird jedoch eine explizite Zurücksetzung angezeigt, die vom Ziel an die Quelle gesendet wird.

Quellseite



Auf der Ziel seitigen Ablaufverfolgung



Außerdem wird ein ACK + RST-Flag-Paket in einem Fall angezeigt, wenn das TCP-Establishment-Paket SYN gesendet wird. Das TCP-SYN-Paket wird gesendet, wenn der Client eine Verbindung mit einem bestimmten Port herstellen möchte, aber wenn das Ziel/der Server aus irgendeinem Grund das Paket nicht akzeptieren möchte, würde es ein ACK + RST-Paket senden.

Source	Destination	Protocol ...	Description
10.10.10.1	10.10.10.2	TCP	TCP:Flags=.....S., SrcPort=4434, DstPort=4437, PayloadLen=0, Seq=873742159, Ack=0, Win=8188 ...
10.10.10.2	*10.10.10.1*	*TCP*	*TCP: [Bad CheckSum]Flags=...A.R.., SrcPort=4437, DstPort=4434, PayloadLen=0, Seq=0, Ack=873...*

Die Anwendung, die das Zurücksetzen verursacht (identifiziert durch Portnummern), sollte untersucht werden, um zu verstehen, was dazu führt, dass die Verbindung zurückgesetzt wird.

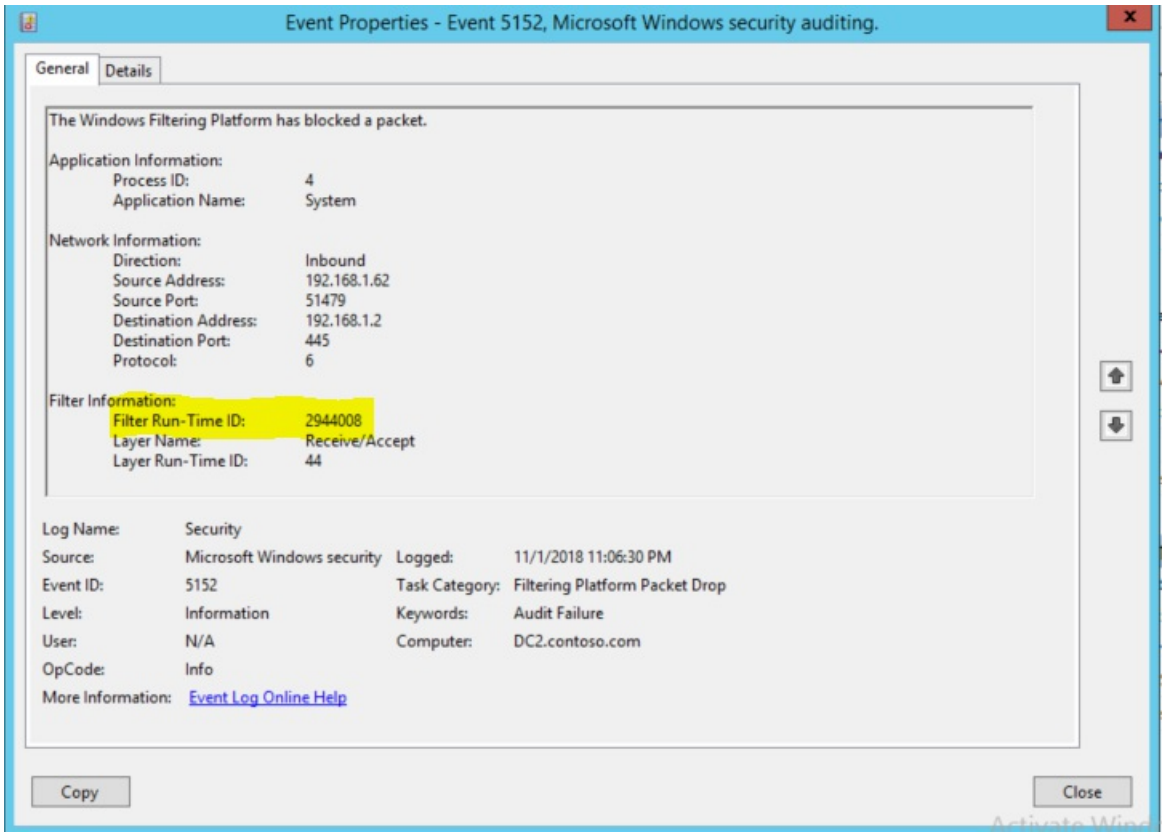
> **NOTE**
>
> Bei den obigen Informationen handelt es sich um das Zurücksetzen von einem TCP-Standpunkt und nicht UDP. UDP ist ein verbindungslos-Protokoll, und die Pakete werden unzuverlässig gesendet. Wenn Sie UDP als Transportprotokoll verwenden, wird keine erneute Übertragung oder Zurücksetzung angezeigt. UDP nutzt ICMP jedoch als Fehler Berichterstattungs Protokoll. Wenn Sie das UDP-Paket an einem Port gesendet haben und für das Ziel kein Port aufgeführt ist, sehen Sie, dass das Ziel " **ICMP-Zielhost nicht erreichbar** " angezeigt wird: Nachricht "Port nicht erreichbar" unmittelbar nach dem UDP-Paket

```
10.10.10.1  10.10.10.2  UDP UDP:SrcPort=49875,DstPort=3343

10.10.10.2  10.10.10.1  ICMP    ICMP:Destination Unreachable Message, Port Unreachable,10.10.10.2:3343
```

Im Verlauf der Problembehandlung bei Verbindungsproblemen sehen Sie möglicherweise auch in der Netzwerkablaufverfolgung, dass ein Computer Pakete empfängt, auf die aber nicht reagiert. In solchen Fällen kann es einen Rückgang auf Serverebene geben. Sie sollten die Firewall-Überwachung auf dem Computer aktivieren, um zu verstehen, ob die lokale Firewall das Paket abfällt.

```
auditpol /set /subcategory:"Filtering Platform Packet Drop" /success:enable /failure:enable
```

Anschließend können Sie die Sicherheitsereignisprotokolle überprüfen, um eine Paket Ablage für eine bestimmte Port-IP-Adresse und eine zugehörige Filter-ID anzuzeigen.



Führen Sie nun den Befehl `netsh wfp show state` aus, um eine wfpstate. XML-Datei zu generieren. Nachdem Sie diese Datei geöffnet und nach der ID gefiltert haben, die Sie im obigen Ereignis (2944008) finden, können Sie einen Firewall-Regelnamen sehen, der dieser ID zugeordnet ist, die die Verbindung blockiert.

wfpstate - Notepad

File Edit Format View Help


```
                <uint64>274877906944</uint64>
        </effectiveWeight>
</item>
<item>
        <displayData>
                <name>tcp port 445</name>
                <description/>
        </displayData>

        <action>
                <type>FWP_ACTION_BLOCK</type>
                <filterType/>
        </action>
        <rawContext>0</rawContext>
        <reserved/>
        <filterId>2944008</filterId>
        <effectiveWeight>
                <type>FWP_UINT64</type>
                <uint64>11531326108393799680</uint64>
        </effectiveWeight>
</item>
<item>
```

Problembehandlung für Portmangel

07.08.2019 • 9 minutes to read

TCP-und UDP-Protokolle funktionieren basierend auf Portnummern, die zum Herstellen einer Verbindung verwendet werden. Für alle Anwendungen oder Dienste, die eine TCP/UDP-Verbindung herstellen müssen, ist ein Port auf der Seite erforderlich.

Es gibt zwei Arten von Ports:

- *Ephemere Ports*, bei denen es sich normalerweise um dynamische Ports handelt, sind die Ports, die von jedem Computer standardmäßig für eine ausgehende Verbindung bereitgestellt werden.
- Bekannte *Ports* sind der definierte Port für eine bestimmte Anwendung oder einen bestimmten Dienst. Der Dateiserverdienst befindet sich beispielsweise auf Port 445, HTTPS ist 443, http ist 80, und RPC ist 135. Die benutzerdefinierte Anwendung hat auch Ihre definierten Portnummern.

Clients beim Herstellen einer Verbindung mit einer Anwendung oder einem Dienst wird ein ephemerer Port von seinem Computer verwendet, um eine Verbindung mit einem bekannten Port herzustellen, der für diese Anwendung oder diesen Dienst definiert ist. Ein Browser auf einem Clientcomputer verwendet einen kurzlebigen Port zum Herstellen einer Verbindung https://www.microsoft.com mit Port 443.

In einem Szenario, in dem derselbe Browser viele Verbindungen mit mehreren Websites erstellt, wird für jede neue Verbindung, die der Browser versucht, ein ephemerer Port verwendet. Nach einiger Zeit werden Sie feststellen, dass die Verbindungen zu einem Ausfall führen, und eine Möglichkeit besteht darin, dass der Browser alle verfügbaren Anschlüsse verwendet, um Verbindungen außerhalb zu erstellen, und jeder neue Versuch, eine Verbindung herzustellen, schlägt fehl, da es keine mehr gibt. Anschlüsse verfügbar. Wenn alle Ports auf einem Computer verwendet werden, wird dies als *Port Erschöpfung*bezeichnet.

Dynamischer Standardportbereich für TCP/IP

Um die IANA-Empfehlungen (Internet Assigned Numbers Authority) zu erfüllen, hat Microsoft den dynamischen Client-Portbereich für ausgehende Verbindungen erhöht. Der neue standardmäßige startport ist **49152**, und der neue Standardport ist **65535**. Hierbei handelt es sich um eine Änderung gegenüber der Konfiguration früherer Windows-Versionen, die einen Standardportbereich von **1025** bis **5000**verwendet hat.

Mit den folgenden Netsh-Befehlen können Sie den dynamischen Portbereich auf einem Computer anzeigen:

- `netsh int ipv4 show dynamicport tcp`
- `netsh int ipv4 show dynamicport udp`
- `netsh int ipv6 show dynamicport tcp`
- `netsh int ipv6 show dynamicport udp`

Der Bereich wird für jeden Transport (TCP oder UDP) separat gesetzt. Der Portbereich ist nun ein Bereich, der einen Ausgangspunkt und einen Endpunkt aufweist. Microsoft-Kunden, die Server bereitstellen, auf denen Windows Server ausgeführt wird, haben möglicherweise Probleme, die sich auf die RPC-Kommunikation zwischen Servern auswirken, wenn Firewalls im internen Netzwerk verwendet werden. In diesen Fällen empfiehlt es sich, die Firewalls neu zu konfigurieren, um den Datenverkehr zwischen Servern im dynamischen Portbereich von **49152** bis **65535**zu ermöglichen. Dieser Bereich ist zusätzlich zu bekannten Ports, die von Diensten und Anwendungen verwendet werden. Oder der von den Servern verwendete Portbereich kann auf jedem Server geändert werden. Sie passen diesen Bereich an, indem Sie den Befehl netsh wie folgt verwenden: Der obige Befehl legt den dynamischen Portbereich für TCP fest.

```
netsh int <ipv4|ipv6> set dynamic <tcp|udp> start=number num=range
```

Der Start-Port ist Number, und die Gesamtzahl der Ports ist Range. Im folgenden finden Sie Beispielbefehle:

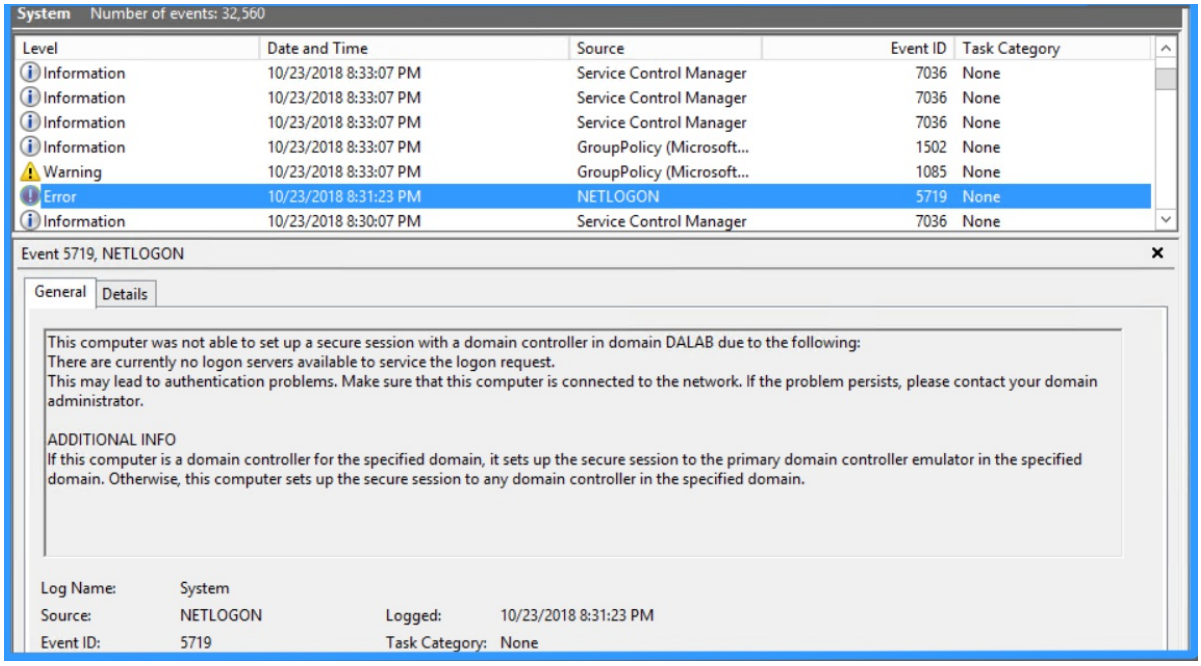
- `netsh int ipv4 set dynamicport tcp start=10000 num=1000`
- `netsh int ipv4 set dynamicport udp start=10000 num=1000`
- `netsh int ipv6 set dynamicport tcp start=10000 num=1000`
- `netsh int ipv6 set dynamicport udp start=10000 num=1000`

Mit diesen Beispielbefehlen wird der dynamische Portbereich so eingestellt, dass er bei Port 10000 beginnt und bei Port 10999 (1000-Ports) endet. Der Mindest-Portbereich, der festzulegen ist, ist 255. Der minimale startport, der festgesetzt werden kann, ist 1025. Der maximale End-Port (basierend auf dem konfigurierten Bereich) darf 65535 nicht überschreiten. Wenn Sie das Standardverhalten von Windows Server 2003 duplizieren möchten, verwenden Sie 1025 als Startanschluss, und verwenden Sie dann 3976 als Bereich für TCP und UDP. Dies führt zu einem Start-Port von 1025 und einem End-Port von 5000.

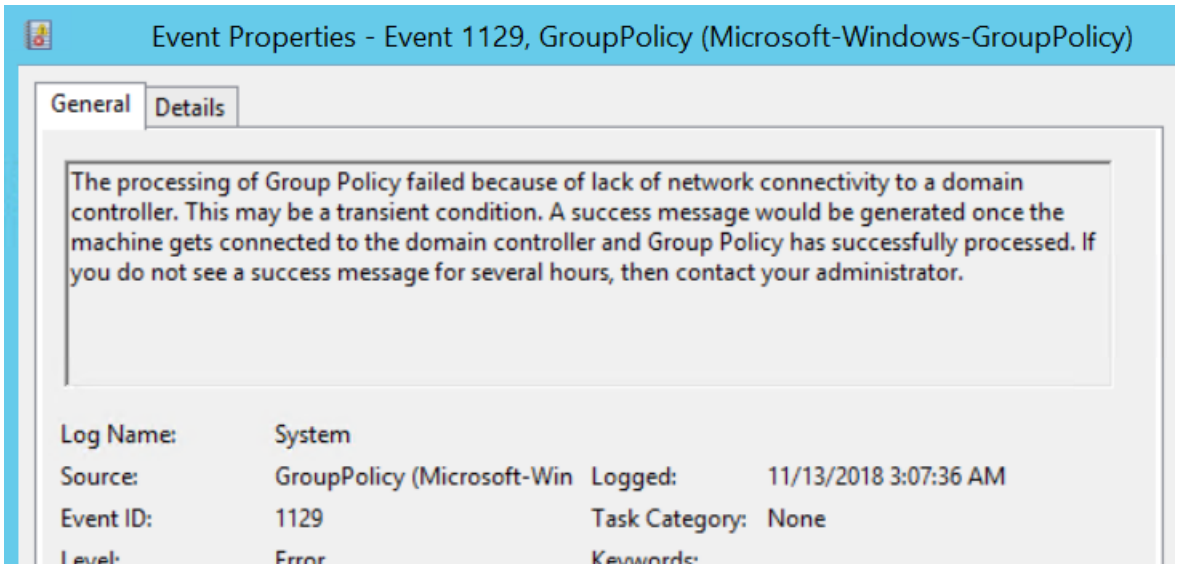
Insbesondere für ausgehende Verbindungen als eingehende Verbindungen ist kein ephemerer Port für das annehmen von Verbindungen erforderlich.

Da ausgehende Verbindungen zu einem Fehler führen, werden viele der folgenden Verhaltensweisen angezeigt:

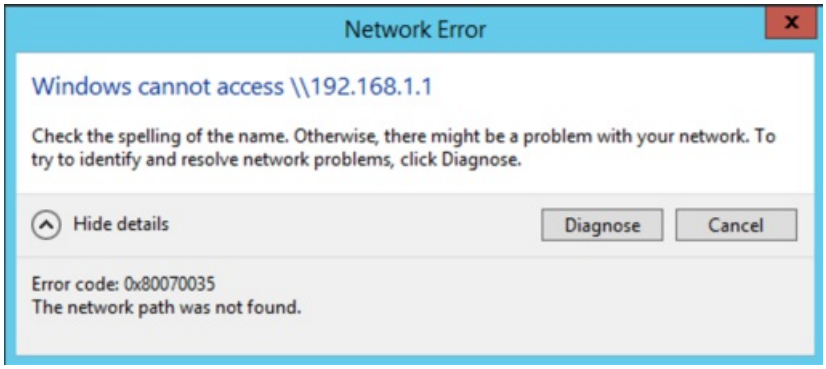
- Die Anmeldung beim Computer mit Domänenanmeldeinformationen ist nicht möglich, doch die Anmeldung mit dem lokalen Konto funktioniert. Bei der Domänenanmeldung ist es erforderlich, dass Sie sich an den DC für die Authentifizierung wenden, bei der es sich wieder um eine ausgehende Verbindung handelt. Wenn Sie über Cache Anmeldeinformationen verfügen, kann die Domänenanmeldung weiterhin funktionieren.



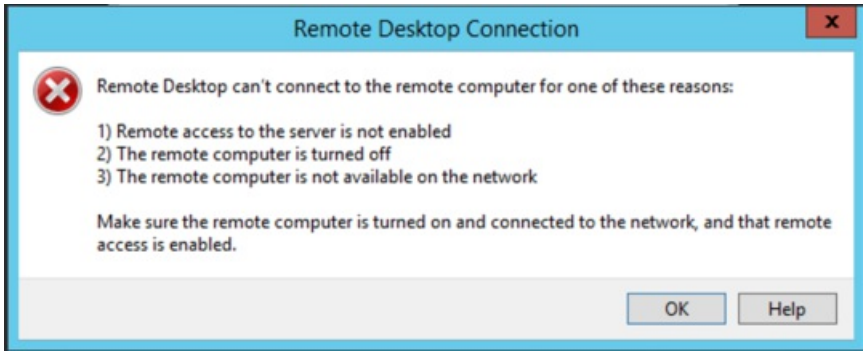
- Fehler bei der Gruppenrichtlinienaktualisierung:



- Auf Dateifreigaben kann nicht zugegriffen werden:



- RDP vom betroffenen Server schlägt fehl:



- Alle anderen Anwendungen, die auf dem Computer ausgeführt werden, geben Fehler ab.

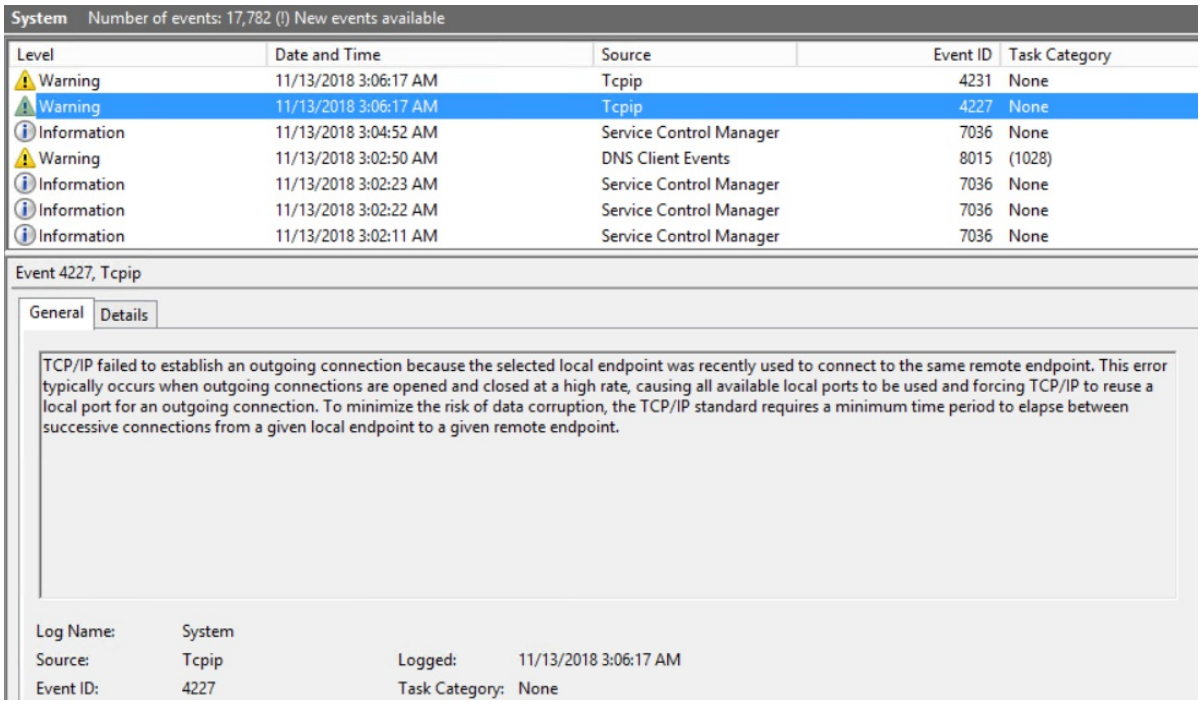
Wenn der Server neu gestartet wird, wird das Problem vorübergehend behoben, allerdings werden alle Symptome nach einer gewissen Zeit wieder angezeigt.

Wenn Sie vermuten, dass sich der Computer in einem Zustand der Port Erschöpfung befindet:

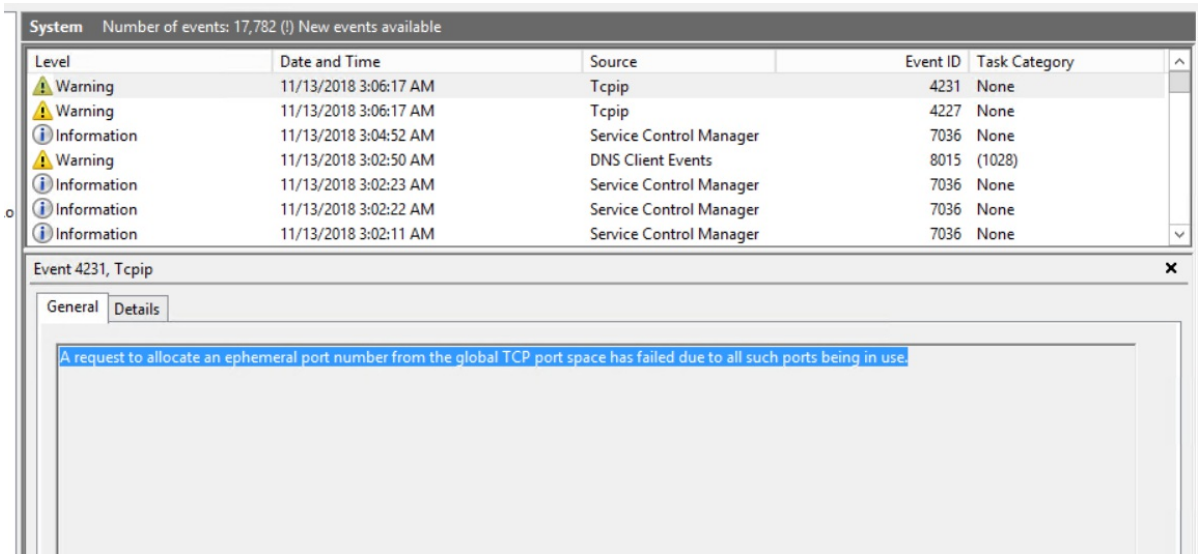
1. Versuchen Sie, eine ausgehende Verbindung herzustellen. Greifen Sie auf dem Server/Computer auf eine Remotefreigabe zu, oder versuchen Sie, ein RDP zu einem anderen Server oder zu einem Server auf einem Port zu verwenden. Wenn die ausgehende Verbindung für alle diese Fehler fehlschlägt, fahren Sie mit dem nächsten Schritt fort.

2. Öffnen Sie die Ereignisanzeige, und suchen Sie unter den Systemprotokollen nach den Ereignissen, die den aktuellen Zustand deutlich angeben:

   a. **Ereignis-ID 4227**



b. **Ereignis-ID 4231**



3. Sammeln Sie `netstat -anob output` eine vom Server. Die netstat-Ausgabe zeigt eine große Anzahl von Einträgen für den TIME_WAIT-Status für eine einzelne PID.

```
TCP    10.94.160.76:53396     40.77.226.250:443      TIME_WAIT       1243
TCP    10.94.160.76:53401     104.211.216.33:443     TIME_WAIT       1243
TCP    10.94.160.76:53402     13.76.141.123:443      TIME_WAIT       1243
TCP    10.94.160.76:53403     13.76.141.123:443      TIME_WAIT       1243
TCP    10.94.160.76:53404     117.18.232.200:443     TIME_WAIT       1243
TCP    10.94.160.76:53406     65.55.44.109:443       TIME_WAIT       1243
TCP    10.94.160.76:53407     65.55.44.109:443       TIME_WAIT       1243
TCP    10.94.160.76:53408     13.76.142.215:443      TIME_WAIT       1243
TCP    10.94.160.76:53409     13.76.142.215:443      TIME_WAIT       1243
TCP    10.94.160.76:53410     40.81.31.55:443        TIME_WAIT       1243
TCP    10.94.160.76:53411     40.81.31.55:443        TIME_WAIT       1243
TCP    10.94.160.76:53424     10.151.148.80:80       TIME_WAIT       1243
TCP    10.94.160.76:53434     10.151.148.97:80       TIME_WAIT       1243
TCP    10.94.160.76:53435     10.151.148.97:80       TIME_WAIT       1243
TCP    10.94.160.76:53436     10.151.148.97:80       TIME_WAIT       1243
TCP    10.94.160.76:53445     52.109.124.5:443       TIME_WAIT       1243
TCP    10.94.160.76:53446     52.109.124.5:443       TIME_WAIT       1243
TCP    10.94.160.76:53448     10.151.148.80:80       TIME_WAIT       1243
TCP    10.94.160.76:53460     52.114.128.8:443       TIME_WAIT       1243
TCP    10.94.160.76:53463     52.114.76.37:443       TIME_WAIT       1243
TCP    10.94.160.76:53275     10.151.148.80:443      TIME_WAIT      1243
TCP    10.94.160.76:53383     10.151.148.80:443      TIME_WAIT      1243
TCP    10.94.160.76:53399     10.151.148.80:5985     TIME_WAIT      1243
TCP    10.94.160.76:53414     10.151.148.80:443      TIME_WAIT      1243
TCP    10.94.160.76:53415     10.151.148.80]:443     TIME_WAIT      1243
```

Nach einer ordnungsgemäßen Schließung oder einem abrupten Abschluss einer Sitzung nach einem Zeitraum von 4 Minuten (Standard) wird der verwendete Port vom Prozess oder der Anwendung wieder in den verfügbaren Pool zurückgesetzt. Während dieser 4 Minuten ist der TCP-Verbindungsstatus TIME_WAIT-Zustand. In einer Situation, in der Sie die Port Erschöpfung vermuten, kann eine Anwendung oder ein Prozess nicht alle Ports freigeben, die Sie verbraucht hat, und bleibt im TIME_WAIT-Zustand.

Möglicherweise werden auch CLOSE_WAIT-Zustands Verbindungen in der gleichen Ausgabe angezeigt, allerdings ist CLOSE_WAIT Zustand ein Zustand, wenn eine Seite des TCP-Peers keine zu sendenden Daten mehr hat (FIN gesendet), aber Daten vom anderen Ende empfangen kann. Dieser Zustand zeigt nicht unbedingt Port Erschöpfung an.

> **NOTE**
>
> Wenn Sie über riesige Verbindungen im TIME_WAIT-Zustand verfügen, wird nicht immer angegeben, dass der Server zurzeit nicht in den Anschlüssen vorhanden ist, es sei denn, die ersten beiden Punkte werden überprüft. Wenn viele TIME_WAIT-Verbindungen bestehen, deutet dies darauf hin, dass der Prozess viele TCP-Verbindungen verursacht und eventuell zu Port Erschöpfung führt.
>
> Netstat wurde in Windows 10 mit dem Hinzufügen des Schalters " **-Q** " aktualisiert, um Ports anzuzeigen, die außerhalb der Zeit übergewechselt sind, wie im gebundenen Zustand. Es wurde ein Update für Windows 8,1 und Windows Server 2012 R2 veröffentlicht, das diese Funktion enthält. Das PowerShell- `Get-NetTCPConnection` Cmdlet in Windows 10 zeigt auch diese gebundenen Ports an.
>
> Bis 10/2016 war netstat ungenau. Fehlerbehebungen für netstat, auf 2012 R2 zurückportiert, erlaubten netstat. exe und Get-NetTcpConnection, die TCP-oder UDP-Port Nutzung in Windows Server 2012 R2 ordnungsgemäß zu melden. Weitere Informationen finden Sie unter Windows Server 2012 R2: ephemere Ports -Hotfixes.

1. Öffnen Sie eine Eingabeaufforderung im Administratormodus, und führen Sie den folgenden Befehl aus.

   ```
   Netsh trace start scenario=netconnection capture=yes tracefile=c:\Server.etl
   ```

2. Öffnen Sie die Dateiserver. ETL mit Netzwerk Monitor , und wenden Sie im Abschnitt Filter den Filter **Wscore_MicrosoftWindowsWinsockAFD. _event_bind. Status. LENTStatus. Code = = 0x209**. Einträge, die **STATUS_TOO_MANY_ADDRESSES**sagen, sollten angezeigt werden. Wenn Sie keine Einträge finden, befindet sich der Server noch nicht außerhalb der Ports. Wenn Sie Sie finden, können Sie

bestätigen, dass der Server unter Port Erschöpfung steht.

Problembehandlung bei der Port Erschöpfung

Der Schlüssel besteht darin, zu ermitteln, welcher Prozess oder welche Anwendung alle Ports verwendet. Nachfolgend sind einige der Tools aufgeführt, die Sie zum Isolieren auf einen einzelnen Prozess verwenden können.

Methode 1

Sehen Sie sich zunächst die netstat-Ausgabe an. Wenn Sie Windows 10 oder Windows Server 2016 verwenden, können Sie den Befehl `netstat -anobq` ausführen und auf die Prozess-ID überprüfen, für die maximale Einträge als gebunden gelten. Alternativ können Sie auch den folgenden PowerShell-Befehl ausführen, um den Prozess zu identifizieren:

```
Get-NetTCPConnection | Group-Object -Property State, OwningProcess | Select -Property Count, Name,
@{Name="ProcessName";Expression={(Get-Process -PID ($_.Name.Split(',')[-1].Trim(' '))).Name}}, Group | Sort
Count -Descending
```

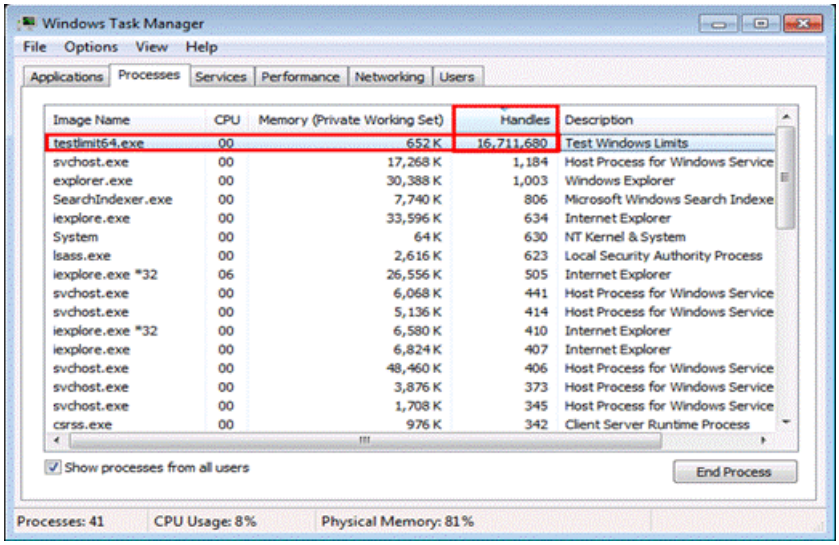
Die meisten Lecks am Port werden durch Benutzermodus-Prozesse verursacht, die die Ports nicht ordnungsgemäß schließen, wenn ein Fehler aufgetreten ist. Auf der Benutzermodus-Ebene sind Ports (eigentlich Sockets) Handles. Sowohl **Task Manager** als auch **ProcessExplorer** sind in der Lage, die Anzahl der Handles anzuzeigen, mit denen Sie ermitteln können, welcher Prozess alle Ports beansprucht.

Für Windows 7 und Windows Server 2008 R2 können Sie Ihre PowerShell-Version so aktualisieren, dass Sie das obige Cmdlet enthält.

Methode 2

Wenn Methode 1 Ihnen nicht hilft, den Prozess zu identifizieren (vor Windows 10 und Windows Server 2012 R2), sehen Sie sich den Task-Manager an:

1. Fügen Sie unter Details/Prozesse eine Spalte mit dem Namen "Handles" hinzu.
2. Sortieren Sie die Spaltenziehpunkte, um den Prozess mit der höchsten Anzahl von Handles zu identifizieren. In der Regel kann der Prozess mit Handles, die größer als 3000 sind, der Täter sein, mit Ausnahme von Prozessen wie System, LSASS. exe, Store. exe, SQLSVR. exe.



3. Wenn ein anderer Prozess als dieser eine höhere Zahl aufweist, beenden Sie diesen Prozess, und versuchen Sie dann, sich mit Domänenanmeldeinformationen anzumelden und zu überprüfen, ob er erfolgreich ist.

Methode 3

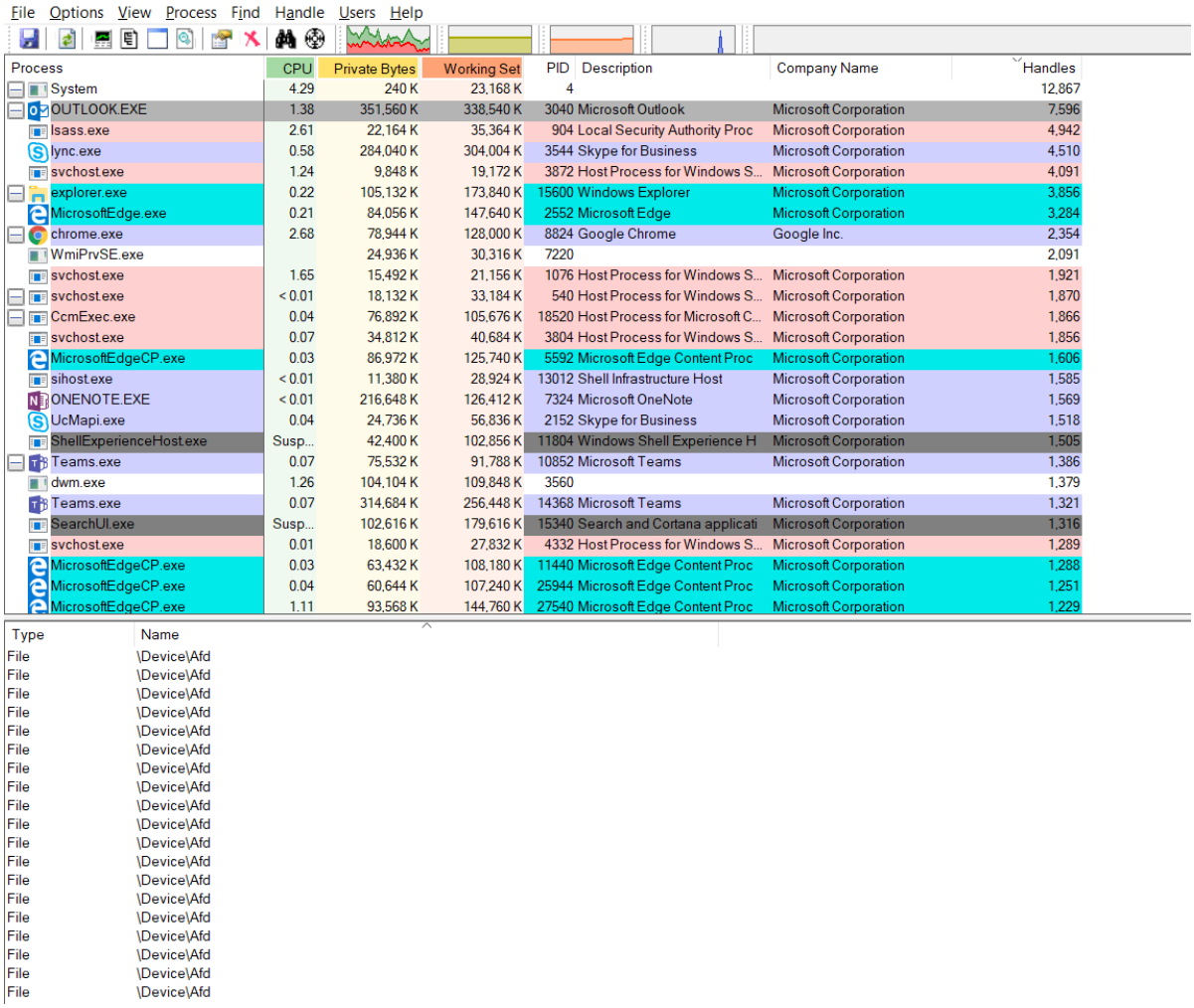
Wenn der Task-Manager Sie nicht bei der Identifizierung des Prozesses unterstützt hat, verwenden Sie den

Prozess-Explorer, um das Problem zu untersuchen.

Schritte zur Verwendung des Prozess-Explorers:

1. Laden Sie Process Explorer herunter , und führen Sie es mit **erhöhten Rechten**aus.
2. Alt + Klicken Sie auf die Spaltenüberschrift, wählen Sie **Spalten auswählen**aus, und fügen Sie auf der Registerkarte **Prozessleistung** die **Anzahl**der Handles hinzu.
3. Wählen Sie **Ansicht \ unteren Bereich anzeigen**aus.
4. Wählen Sie **Ansicht \ untere Bereichsansicht \ Handles**aus.
5. Klicken Sie **** auf die Spalte Handles, um nach diesem Wert zu sortieren.
6. Untersuchen Sie die Prozesse mit einer höheren Anzahl von Handles als die anderen (wahrscheinlich über 10.000, wenn Sie keine ausgehenden Verbindungen herstellen können).
7. Klicken Sie hier, um einen der Prozesse mit einer großen Anzahl von Handles hervorzuheben.
8. Im unteren Bereich sind die Handles wie folgt aufgeführt: Sockets. (Sockets sind technisch Dateihandles).

   Datei \Device\AFD



9. Einige sind normal, aber eine große Anzahl von Ihnen ist nicht (Hunderte bis Tausende). Schließen Sie den fraglichen Prozess. Wenn dadurch ausgehende Konnektivität wiederhergestellt wird, haben Sie weiter bewiesen, dass die APP die Ursache ist. Wenden Sie sich an den Hersteller dieser app.

Wenn die oben genannten Methoden Ihnen nicht helfen, den Prozess zu isolieren, empfehlen wir, dass Sie ein vollständiges Speicherabbild des Computers im Problemzustand sammeln. Der Dump gibt an, welche Prozesse die maximalen Ziehpunkte aufweisen.

Um dieses Problem zu umgehen, wird der Computer im normalen Zustand wieder gestartet, und Sie können das Problem vorerst beheben. Wenn ein Neustart jedoch nicht praktikabel ist, können Sie auch die Anzahl der Ports auf dem Computer mithilfe der folgenden Befehle erhöhen:

```
netsh int ipv4 set dynamicport tcp start=10000 num=1000
```

Dadurch wird der dynamische Portbereich so eingestellt, dass er bei Port 10000 beginnt und bei Port 10999 (1000-Ports) endet. Der Mindest-Portbereich, der festzulegen ist, ist 255. Der minimale startport, der festgesetzt werden kann, ist 1025. Der maximale End-Port (basierend auf dem konfigurierten Bereich) darf 65535 nicht überschreiten.

> **NOTE**
> Beachten Sie, dass die Vergrößerung des dynamischen Portbereichs keine dauerhafte, sondern nur vorübergehende Lösung ist. Sie müssen ermitteln, welche Prozesse/Prozessoren die maximale Anzahl von Ports verbrauchen, und wie Sie in diesem Prozess die Ursache für die Verwendung einer derart großen Anzahl von Ports beheben können.

Für Windows 7 und Windows Server 2008 R2 können Sie das folgende Skript verwenden, um die netstat-Ausgabe mit definierter Häufigkeit zu erfassen. Über die Ausgänge können Sie den Trend zur Portierungs Nutzung sehen.

```
@ECHO ON
set v=%1
:loop
set /a v+=1
ECHO %date% %time% >> netstat.txt
netstat -ano >> netstat.txt

PING 1.1.1.1 -n 1 -w 60000 >NUL

goto loop
```

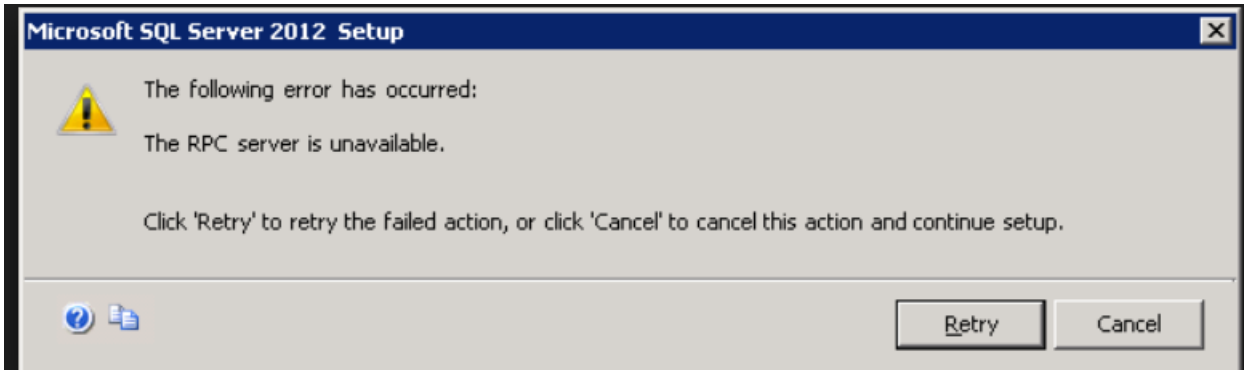
Nützliche Links

- Port Erschöpfung und Sie! – in diesem Artikel werden die netstat-Zustände detailliert erläutert, und Sie erfahren, wie Sie den Portstatus mithilfe der netstat-Ausgabe ermitteln können.
- Erkennung ephemerer Port Erschöpfung: Dieser Artikel enthält ein Skript, das in einer Schleife ausgeführt wird, um den Portstatus zu melden. (Anwendbar für Windows 2012 R2, Windows 8, Windows 10)

Problembehandlung für Remote Procedure Call (RPC)-Fehler

07.08.2019 • 7 minutes to read

Beim Herstellen einer Verbindung mit Windows-Verwaltungsinstrumentation (WMI), SQL Server, während einer Remoteverbindung oder bei einigen MMC-Snap-Ins (Microsoft Management Console) kann der Fehler **RPC-Server nicht verfügbar** sein. Die folgende Abbildung zeigt ein Beispiel für einen RPC-Fehler.



Hierbei handelt es sich um eine häufig auftretende Fehlermeldung in der Netzwerkwelt, und man kann die Hoffnung sehr schnell verlieren, ohne viel zu verstehen, was "unter der Haube" passiert.

Bevor Sie sich mit der Problem *Behandlung des nicht verfügbaren** RPC-Servers vertraut machen, sollten Sie zunächst die Grundlagen des Fehlers verstehen. Es gibt einige wichtige Begriffe, die Sie verstehen müssen:

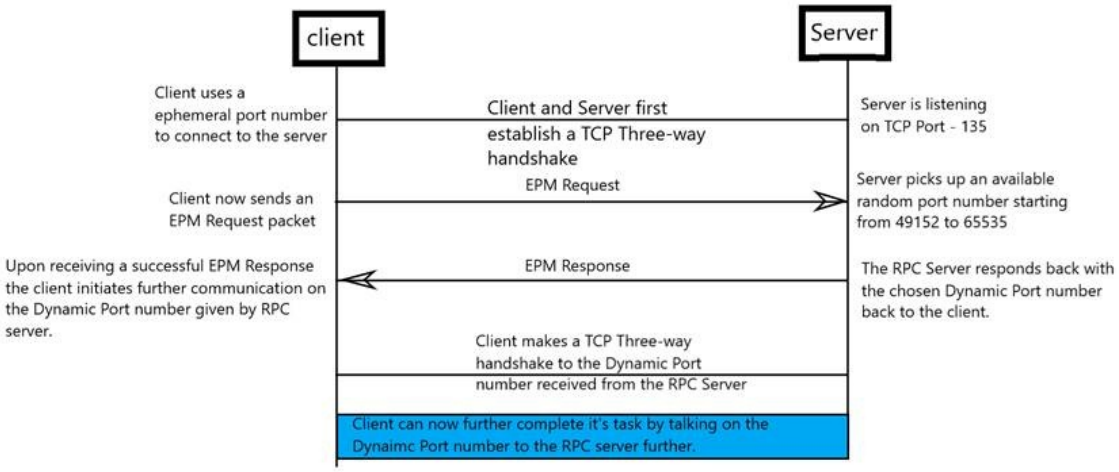
- Endpunktzuordnung – ein Dienst, der den Server überwacht, der Client-apps nach Port und UUID zu Server-apps führt.
- Tower – beschreibt das RPC-Protokoll, um dem Client und dem Server die Aushandlung einer Verbindung zu ermöglichen.
- Floor – der Inhalt eines Turms mit bestimmten Daten wie Ports, IP-Adressen und Bezeichnern.
- UUID – eine bekannte GUID, die die RPC-Anwendung identifiziert. Die UUID ist das, was Sie zum Anzeigen einer bestimmten Art von RPC-Anwendungs Unterhaltung verwenden, da wahrscheinlich viele vorhanden sind.
- Nummer – der Bezeichner einer Funktion, die vom Client vom Server ausgeführt werden soll. Es ist nur eine hexadezimale Zahl, aber ein guter Netzwerkanalysator über setzt die Funktion für Sie. Wenn dies nicht der Fall ist, muss Ihnen der Anwendungsanbieter mitgeteilt werden.
- Port – die Kommunikationsendpunkte für die Client-und Serveranwendungen.
- Stubdaten – die Informationen zu Funktionen und Daten, die zwischen dem Client und dem Server ausgetauscht werden. Hierbei handelt es sich um die Nutzlast, den wichtigen Teil.

> **NOTE**
>
> Viele der oben genannten Informationen werden bei der Problembehandlung verwendet, das wichtigste ist die dynamische RPC-Portnummer, die Sie beim Gespräch mit EPM erhalten.

Funktionsweise der Verbindung

Client a möchte einige Funktionen ausführen oder einen Dienst verwenden, der auf dem Remoteserver ausgeführt wird, wobei zunächst die Verbindung mit dem Remoteserver hergestellt wird, indem ein dreiseitiger

Handshake durchgeführt wird.



RPC-Ports können auch aus einem bestimmten Bereich angegeben werden.

Konfigurieren der dynamischen RPC-Portzuweisung

Die dynamische Portzuweisung (Remote Procedure Call, RPC) wird von Serveranwendungen und Remoteverwaltungsanwendungen wie Dynamic Host Configuration Protocol (DHCP)-Manager, Windows Internet Name Service (WINS)-Manager usw. verwendet. Die dynamische RPC-Portzuweisung weist das RPC-Programm an, basierend auf der Implementierung des verwendeten Betriebssystems einen bestimmten Random-Port in dem für TCP und UDP konfigurierten Bereich zu verwenden.

Kunden, die Firewalls verwenden, möchten möglicherweise steuern, welche Ports RPC verwendet, damit der Firewall-Router so konfiguriert werden kann, dass nur diese TCP-und UDP-Ports weitergeleitet werden. Mit vielen RPC-Servern in Windows können Sie den Serverport in benutzerdefinierten Konfigurationselementen wie Registrierungseinträgen angeben. Wenn Sie einen dedizierten Serverport angeben können, wissen Sie, welcher Datenverkehr zwischen den Hosts über die Firewall fließt, und Sie können festlegen, welcher Datenverkehr auf eine gezieltere Weise zulässig ist.

Wählen Sie als Serverport einen Port außerhalb des Bereichs aus, den Sie unten angeben möchten. Eine umfassende Liste der Serverports, die in Windows und wichtigen Microsoft-Produkten verwendet werden, finden Sie im Artikel Dienstübersicht und Netzwerkportanforderungen für Windows. Der Artikel listet auch die RPC-Server auf, und welche RPC-Server für die Verwendung von benutzerdefinierten Server Anschlüssen konfiguriert werden können, die über die von der RPC-Laufzeit angebotenen Funktionen hinausgehen

Einige Firewalls ermöglichen auch die UUID-Filterung, wenn Sie von einer RPC-Endpunkt Zuordnungsanforderung für eine RPC-Schnittstellen UUID erfahren. Die Antwort hat die Server-Portnummer, und eine nachfolgende RPC-Bindung an diesem Port kann dann übergeben werden.

Mit dem Registrierungs-Editor können Sie die folgenden Parameter für RPC ändern. Die unten besprochenen RPC-Port Schlüsselwerte befinden sich alle im folgenden Schlüssel in der Registrierung:

HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet-Eintragsname (Datentyp)

Ports REG_MULTI_SZ

- Gibt einen Satz von IP-Portbereichen an, bestehend aus allen Ports, die über das Internet verfügbar sind, oder aus allen Anschlüssen, die nicht im Internet verfügbar sind. Jede Zeichenfolge steht für einen einzelnen Port oder einen inklusiven Satz von Ports. Beispielsweise kann ein einzelner Port durch **5984**dargestellt werden, und eine Reihe von Ports kann durch **5000-5100**dargestellt werden. Wenn Einträge außerhalb des Bereichs von 0 bis 65535 liegen oder eine Zeichenfolge nicht interpretiert werden kann, behandelt die RPC-Laufzeit die gesamte Konfiguration als ungültig.

PortsInternetAvailable REG_SZ Y oder N (Groß-/Kleinschreibung wird nicht beachtet)

- Wenn Y, sind die Ports, die in der Ports-Taste aufgelistet sind, alle Internet-verfügbaren Ports auf diesem Computer. Wenn N, sind die Ports, die im Port-Schlüssel aufgeführt sind, alle Ports, die nicht Internet-verfügbar sind.

UseInternetPorts REG_SZ) Y oder N (Groß-/Kleinschreibung wird nicht beachtet)

- Gibt die Standardrichtlinie für das System an.
- Wenn Y, werden die Prozesse, die den Standard verwenden, Ports aus dem Satz der Internet-verfügbaren Ports zugewiesen, wie zuvor definiert.
- Wenn N, werden die Prozesse, die den Standard verwenden, Ports aus der Gruppe von nur-Intranet-Ports zugewiesen.

Beispiel:

In diesem Beispiel wurden Ports 5000 bis einschließlich 6000 willkürlich ausgewählt, um zu veranschaulichen, wie der neue Registrierungsschlüssel konfiguriert werden kann. Hierbei handelt es sich nicht um eine Empfehlung einer Mindestanzahl von Ports, die für ein bestimmtes System benötigt werden.

1. Fügen Sie den Internet Schlüssel unter: HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc
2. Fügen Sie unter dem Internet Schlüssel die Werte "Ports" (MULTI_SZ), "PortsInternetAvailable" (REG_SZ) und "UseInternetPorts" (REG_SZ) hinzu.

   Beispielsweise wird der neue Registrierungsschlüssel wie folgt angezeigt: Ports: REG_MULTI_SZ: 5000-6000 PortsInternetAvailable: REG_SZ: y UseInternetPorts: REG_SZ: y
3. Starten Sie den Server erneut. Alle Anwendungen, die die dynamische RPC-Portzuweisung verwenden, verwenden Ports 5000 bis einschließlich 6000.

Sie sollten einen Portbereich oberhalb von Port 5000 öffnen. Port Nummern unter 5000 werden möglicherweise bereits von anderen Anwendungen verwendet und können Konflikte mit ihrer DCOM-Anwendung (en) verursachen. Darüber hinaus zeigt die bisherige Vorgehensweise, dass eine Mindestzahl von 100-Ports geöffnet werden sollte, da mehrere Systemdienste davon abhängen, dass diese RPC-Ports miteinander kommunizieren.

> **NOTE**
> Die Mindestanzahl der erforderlichen Ports kann von Computer zu Computer unterschiedlich sein. Bei Computern mit höherer Datenverkehr kann es zu einer Port Erschöpfung kommen, wenn die dynamischen RPC-Ports eingeschränkt sind. Berücksichtigen Sie dies, wenn Sie den Portbereich einschränken.

> **WARNING**
> Wenn ein Fehler in der Portkonfiguration vorliegt oder unzureichende Ports im Pool vorhanden sind, kann der Endpunktzuordnungsdienst keine RPC-Server mit dynamischen Endpunkten registrieren. Wenn ein Konfigurationsfehler vorliegt, wird der Fehlercode 87 (0x57) ERROR_INVALID_PARAMETER. Dies kann sich auch auf Windows-RPC-Server wie Netlogon auswirken. In diesem Fall wird das Ereignis 5820 protokolliert:
>
> Protokoll Name: System Quelle: Netlogon-Ereignis-ID: 5820-Ebene: Fehler Schlüsselwörter: klassische Beschreibung: der Netlogon-Dienst konnte die Authz-RPC-Schnittstelle nicht hinzufügen. Der Dienst wurde beendet. Der folgende Fehler ist aufgetreten: "der Parameter ist falsch."

Wenn Sie einen tief greifenden Einblick in die Funktionsweise des IT-Unternehmens haben möchten, lesen Sie RPC über IT/pro.

Problembehandlung bei RPC-Fehler

PortQuery

Die beste Methode, um RPC-Probleme immer zu beheben, bevor Sie sich selbst in die Ablaufverfolgungen einbringen, ist die Verwendung von Tools wie **PortQry**. Sie können schnell feststellen, ob Sie eine Verbindung herstellen können, indem Sie den folgenden Befehl ausführen:

```
Portqry.exe -n <ServerIP> -e 135
```

Dies würde Ihnen viel ausgeben, aber Sie sollten nach * *ip_tcp*-und der Portnummer in den Klammern suchen, die angibt, ob Sie erfolgreich einen dynamischen Port von EPM erhalten und auch eine Verbindung dazu herstellen konnten. Wenn dies nicht der Fall ist, können Sie in der Regel gleichzeitige Netzwerkablaufverfolgungen sammeln. Etwas ähnliches aus der Ausgabe von "Portqry":

```
Portqry.exe -n 169.254.0.2 -e 135
```

Teilausgabe unten:

> Abfrage Zielsystem namens: 169.254.0.2 versucht, die IP-Adresse in einen Namen aufzulösen... IP-Adresse in RPCServer.contoso.com Abfrage aufgelöst... TCP-Port 135 (EPMAP-Dienst): Überwachen der temporären Quell Port Abfrage Endpunkt Zuordnungsdatenbank... Antwort des Servers: uuid: d95afe70-a6d5-4259-822e-2c84da1ddb0d ncacn_ip_tcp: 169.254.0.10**[49664]**

Der Fett gedruckte Wert ist die temporäre Portnummer, mit der Sie eine Verbindung zu einem erfolgreichen Verbindungsaufbau hergestellt haben.

Netsh

Sie können die folgenden Befehle ausführen, um Windows-integrierte Netsh-Aufnahmen zu nutzen, um eine gleichzeitige Ablaufverfolgung zu erfassen. Denken Sie daran, die folgenden auf einem "admin cmd" auszuführen, es erfordert Elevation.

- Auf dem Client

  ```
  Netsh trace start scenario=netconnection capture=yes tracefile=c:\client_nettrace.etl maxsize=512
  overwrite=yes report=yes
  ```

- Auf dem Server

  ```
  Netsh trace start scenario=netconnection capture=yes tracefile=c:\server_nettrace.etl maxsize=512
  overwrite=yes report=yes
  ```

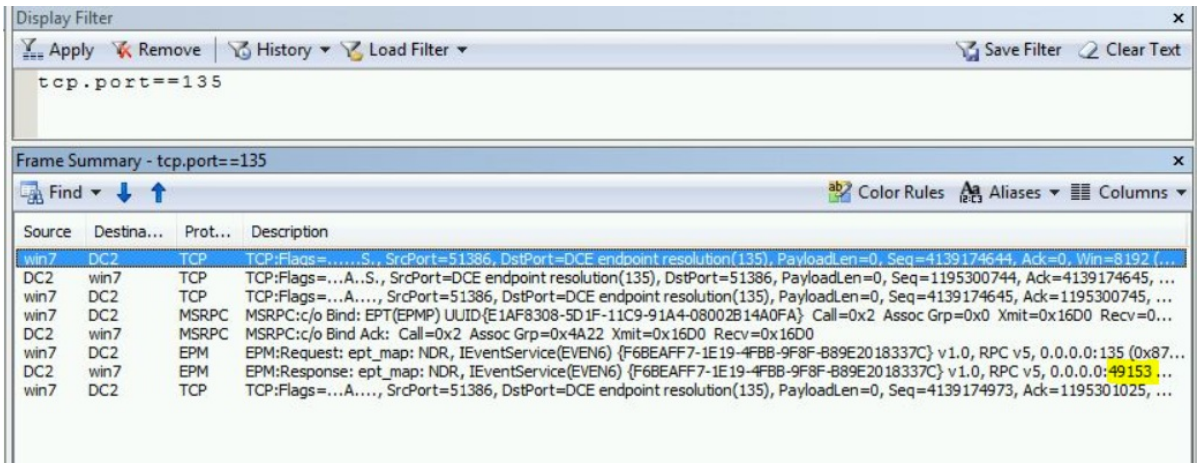
Versuchen Sie nun, Ihr Problem vom Clientcomputer zu reproduzieren, und sobald Sie der Meinung sind, dass das Problem wiedergegeben wurde, können Sie die Ablaufverfolgungen mithilfe des Befehls beenden.

```
Netsh trace stop
```

Öffnen Sie die Ablaufverfolgungen in Microsoft Network Monitor 3,4 oder Message Analyzer, und Filtern Sie die Ablaufverfolgung nach

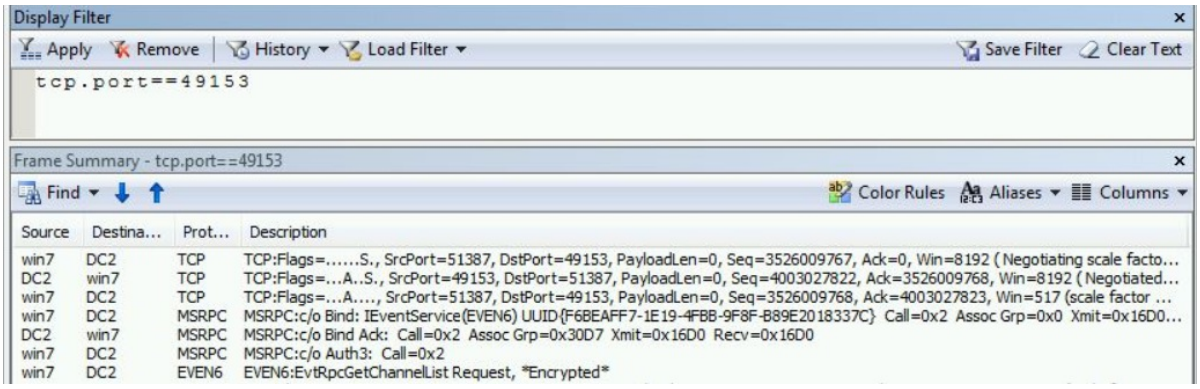
- `Ipv4.address==<client-ip>` und `ipv4.address==<server-ip>` und `tcp.port==135` oder einfach `tcp.port==135` nur helfen.
- Suchen Sie unter der Spalte "Protokoll" nach dem "EPM"-Protokoll.

- Überprüfen Sie jetzt, ob Sie eine Antwort vom Server erhalten. Wenn Sie eine Antwort erhalten, notieren Sie sich die dynamische Portnummer, die Sie für die Verwendung reserviert haben.



- Überprüfen Sie, ob wir erfolgreich eine Verbindung mit diesem dynamischen Port hergestellt haben.

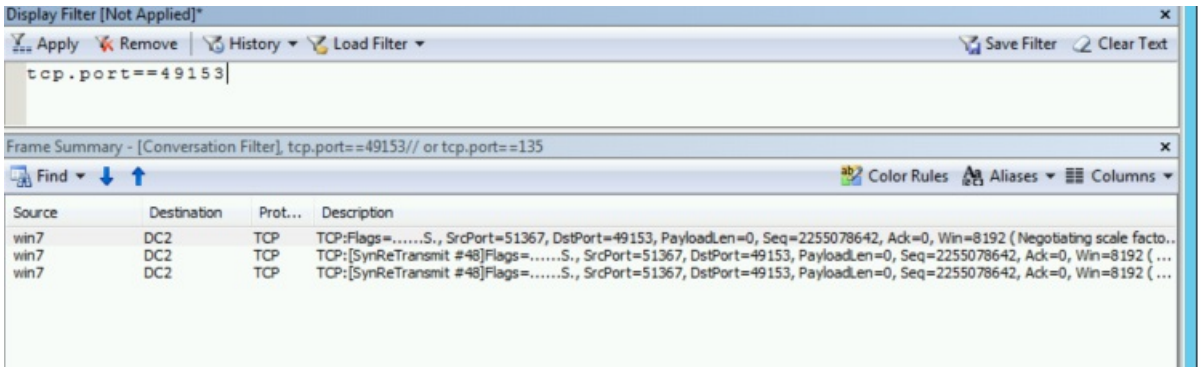
- Der Filter sollte ungefähr so aussehen: `tcp.port==<dynamic-port-allocated>` und `ipv4.address==<server-ip>`



Dies sollte Ihnen dabei helfen, die Konnektivität zu überprüfen und zu isolieren, wenn Netzwerkprobleme angezeigt werden.

Port nicht erreichbar

Der häufigste Grund, warum der RPC-Server nicht zur Verfügung steht, ist der, wenn der dynamische Port, zu dem der Client eine Verbindung herzustellen versucht, nicht erreichbar ist. Auf der clientseitigen Ablaufverfolgung wird dann TCP SYN-erneute Übertragungen für den dynamischen Port angezeigt.



Der Port kann aufgrund eines der folgenden Gründe nicht erreichbar sein:

- Der dynamische Portbereich ist auf der Firewall in der Umgebung blockiert.
- Auf einem mittleren Gerät fallen die Pakete ab.
- Der Zielserver löscht die Pakete (WFP Drop/NIC Drop/Filter Driver usw.).

Erweiterte Problembehandlung für Windows-Startprobleme

11.02.2020 • 2 minutes to read

In diesen Themen erfahren Sie, wie Sie häufige Probleme im Zusammenhang mit dem Windows-Start beheben können.

Funktionsweise

Wenn Microsoft Windows eine Bedingung erlebt, die den sicheren Systembetrieb beeinträchtigt, wird das System angehalten. Diese Windows-Startprobleme werden in den folgenden Gruppen kategorisiert:

- Fehlerüberprüfung: wird auch häufig als Systemabsturz, Kernelfehler oder Abbruchfehler bezeichnet.
- Kein Start: das System erzeugt möglicherweise keine Fehlerüberprüfung, kann aber nicht in Windows gestartet werden.
- Freeze: wird auch als "Systemabsturz" bezeichnet.

Bewährte Methoden

Wenn Sie die zugrunde liegenden Ursachen von Windows-Startproblemen verstehen möchten, ist es wichtig, dass das System ordnungsgemäß konfiguriert ist. Im folgenden finden Sie einige bewährte Methoden für die Konfiguration:

Seitendatei Einstellungen

- Einführung einer Seitendatei
- Bestimmen der geeigneten Auslagerungsdateigröße für 64-Bit-Versionen von Windows

Speicherabbildeinstellungen

- Konfigurieren von Systemausfall- und Wiederherstellungsoptionen in Windows
- Generieren eines Kernels oder eines vollständigen Absturzabbilds

Problembehandlung

In diesen Artikeln finden Sie Informationen zu den Ressourcen, die Sie zur Behandlung von Problemen mit dem Windows-Start benötigen:

- Erweiterte Problembehandlung für Windows-Startprobleme
- Erweiterte Problembehandlung für Abbruchfehler oder Bluescreen-Fehler
- Erweiterte Problembehandlung für Windows-basierte Computer, die einfrieren
- Der Abbruchfehler tritt auf, wenn Sie den in-Box-Broadcom-Netzwerkadaptertreiber aktualisieren.

Bestimmen der geeigneten Auslagerungsdateigröße für 64-Bit-Versionen von Windows

06.03.2020 • 8 minutes to read

Die Größenanpassung von Seiten Dateien hängt von den Einstellungen des Systemabsturz Dumps und der höchst Auslastung oder der erwarteten Spitzenauslastung des System Commits ab. Beide Aspekte sind für jedes System eindeutig, selbst für Systeme, die identisch sind. Das bedeutet, dass die Größe von Seiten Dateien auch für jedes System eindeutig ist und nicht generalisiert werden kann.

Ermitteln der geeigneten Seitendatei Größe

Verwenden Sie die folgenden Überlegungen zur Größenänderung von Seiten Dateien für alle Versionen von Windows und Windows Server.

Absturz-Dump-Einstellung

Wenn während eines Systemabsturzes eine Absturzspeicherabbild Datei erstellt werden soll, muss eine Auslagerungsdatei oder eine dedizierte Dumpdatei vorhanden sein, die groß genug ist, um die Einstellung für das Absturzspeicherabbild des Systems zu sichern. Andernfalls wird keine Systemspeicher Abbilddatei erstellt.

Weitere Informationen finden Sie unter Support für Systemabsturz-Dumps (Abschnitt).

Höchstbetrag des System Commits

Der System Commit-Betrag darf das System Commit-Limit nicht überschreiten. Dieser Grenzwert ist die Summe aus physischem Arbeitsspeicher (RAM) und allen Seiten Dateien kombiniert. Wenn keine Seiten Dateien vorhanden sind, ist das System Commit-Limit etwas kleiner als der installierte physikalische Speicher. Peak-Systemgebundene Speichernutzung kann zwischen Systemen stark variieren. Daher variieren auch der physikalische Arbeitsspeicher und die Größe von Seiten Dateien.

Anzahl selten aufgerufener Seiten

Der Zweck einer Auslagerungsdatei ist das *zurück* (unterstützen) seltener Zugriff auf geänderte Seiten, sodass Sie aus dem physikalischen Speicher entfernt werden können. Dadurch steht mehr verfügbarer Speicherplatz für häufiger zugängliche Seiten zur Verfügung. Der Leistungsindikator "\Memory\Modified page list Bytes" misst teilweise die Anzahl der selten aufgerufenen geänderten Seiten, die für die Festplatte bestimmt sind. Beachten Sie jedoch, dass nicht der gesamte Arbeitsspeicher auf der geänderten Seitenliste auf die Festplatte geschrieben wird. In der Regel bleiben mehrere hundert Megabyte speicherresident in der geänderten Liste. Daher sollten Sie eine Auslagerungsdatei erweitern oder hinzufügen, wenn die folgenden Bedingungen zutreffen:

- Mehr verfügbarer physikalischer Arbeitsspeicher (\Memory\Available MBytes) ist erforderlich.
- Die geänderte Seitenliste enthält eine beträchtliche Menge an Arbeitsspeicher.
- Die vorhandenen Seiten Dateien sind relativ voll (\Paging-Dateien (*) % Verwendung).

Unterstützung für Systemabsturz-Dumps

Ein Systemabsturz (auch bekannt als "Fehlerüberprüfung" oder "Abbruchfehler") tritt auf, wenn das System nicht ordnungsgemäß ausgeführt werden kann. Die aus diesem Ereignis erstellte Dumpdatei wird als Systemabsturz-Dump bezeichnet. Eine Auslagerungsdatei oder eine dedizierte Speicherabbilddatei wird verwendet, um eine Absturzspeicherabbild Datei (Memory. dmp) auf den Datenträger zu schreiben. Daher muss eine Auslagerungsdatei oder eine dedizierte Dumpdatei groß genug sein, um die Art des ausgewählten Absturz Dumps

zu unterstützen. Andernfalls kann das System die Absturzspeicherabbild Datei nicht erstellen.

> **NOTE**
> Während des Starts werden System verwaltete Seiten Dateien entsprechend den Systemabsturz-Speicherabbildeinstellungen angepasst. Es wird davon ausgegangen, dass genügend freier Speicherplatz vorhanden ist.

SYSTEM ABSTURZ-DUMP-EINSTELLUNG	MINIMALE ANFORDERUNG FÜR SEITENDATEI GRÖSSE
Kleiner Speicherauszug (256 KB)	1 MB
Kernel Speicherabbild	Abhängig vom virtuellen Speicherverbrauch des Kernels
Vollständiges Speicherabbild	1 x RAM plus 257 MB *
Automatisches Speicherabbild	Hängt von der Verwendung des virtuellen Kernelspeichers ab. Ausführliche Informationen finden Sie unter automatischer Speicherauszug.

\ * 1 MB für Kopfzeilendaten und Gerätetreiber können 256 MB sekundärer Absturzspeicherabbild Daten insgesamt betragen.

Die Einstellung für das **Automatische Speicherabbild** ist standardmäßig aktiviert. Hierbei handelt es sich um eine Einstellung anstelle einer Art von Absturz Speicher. Diese Einstellung wählt automatisch die beste Seitendatei Größe aus, abhängig von der Häufigkeit von Systemabstürzen.

Das Feature für das automatische Speicherabbild wählt zunächst eine kleine Auslagerungsdateigröße aus. Es würde den Kernelspeicher in den meisten Zeiten aufnehmen. Wenn das System innerhalb von vier Wochen erneut abstürzt, legt das Feature für das automatische Speicherabbild die Größe der Auslagerungsdatei entweder als RAM-Größe oder 32 GB fest, je nachdem, was kleiner ist.

Kernelspeicher Absturz-Dumps erfordern genügend Speicherplatz für die Auslagerungsdatei oder dedizierten Speicherplatz für den Kernelmodus, um die Nutzung des virtuellen Speichers zu ermöglichen. Wenn das System innerhalb von vier Wochen nach dem vorherigen Absturz erneut abstürzt, wird beim Neustart ein vollständiges Speicherabbild ausgewählt. Dies erfordert eine Auslagerungsdatei oder eine dedizierte Dumpdatei mit mindestens der Größe des physikalischen Speichers (RAM) plus 1 MB für Kopfzeileninformationen Plus 256 MB für potenzielle Treiber Daten, um alle potenziellen Daten zu unterstützen, die aus dem Speicher gedumpten werden. Auch hier wird die vom System verwaltete Auslagerungsdatei so erweitert, dass diese Art von Absturz Speicher zurückgesetzt wird. Wenn das System so konfiguriert ist, dass es eine Auslagerungsdatei oder eine dedizierte Dumpdatei mit einer bestimmten Größe aufweist, stellen Sie sicher, dass die Größe ausreicht, um die Einstellung für das Absturzspeicherabbild zu sichern, die in der Tabelle weiter oben in diesem Abschnitt zusammen mit und dem Höchstwert für das System für den Höchstbetrag aufgeführt ist.

Dedizierte Speicherabbilddateien

Computern, auf denen Microsoft Windows oder Microsoft Windows Server ausgeführt wird, muss in der Regel eine Auslagerungsdatei vorhanden sein, um einen Systemabsturz Dump zu unterstützen. System Administratoren haben jetzt die Möglichkeit, stattdessen eine dedizierte Speicherabbilddatei zu erstellen.

Eine dedizierte Speicherabbilddatei ist eine Auslagerungsdatei, die nicht für Paging verwendet wird. Stattdessen ist es "dediziert", um eine Systemabsturz-Dumpdatei (Memory. dmp) zurückzugeben, wenn ein Systemabsturz eintritt. Dedizierte Dumpdateien können auf allen Datenträgern gespeichert werden, die eine Auslagerungsdatei unterstützen können. Wir empfehlen, dass Sie eine dedizierte Dumpdatei verwenden, wenn Sie ein Systemabsturz-Dump verwenden möchten, aber keine Auslagerungsdatei wünschen.

Vom System verwaltete Seiten Dateien

Standardmäßig werden Seiten Dateien vom System verwaltet. Das bedeutet, dass die Seiten Dateien basierend auf zahlreichen Faktoren, wie etwa der Größe des installierten physikalischen Speichers, dem Prozess der Aufnahme des System Commits und dem Prozess der Aufnahme eines Systemabsturz Dumps, zunehmen und verringert werden.

Wenn beispielsweise der System Commit-Betrag mehr als 90 Prozent des System Commit-Limits überschreitet, wird die Auslagerungsdatei auf "zurück" erhöht. Dies tritt weiterhin auf, bis die Auslagerungsdatei dreimal so groß wie physischer Arbeitsspeicher oder 4 GB ist, je nachdem, welcher Wert größer ist. Dabei wird davon ausgegangen, dass der logische Datenträger, der die Auslagerungsdatei hostet, groß genug ist, um dem Wachstum gerecht zu werden.

In der folgenden Tabelle sind die Mindest-und Höchstwerte für Seiten Dateien von System verwalteten Seiten Dateien in Windows 10 aufgelistet.

MINIMALE SEITENDATEI GRÖSSE	MAXIMALE SEITENDATEI GRÖSSE
Variiert basierend auf dem Seitendatei-Nutzungsverlauf, der Arbeitsspeichermenge (RAM ÷ 8, Max 32 GB) und den Einstellungen für das Absturzspeicherabbild.	3 × RAM oder 4 GB, je nachdem, welcher Wert größer ist. Dies ist dann auf die Volumegröße ÷ 8 limitiert. Wenn dies für Crash Dump-Einstellungen erforderlich ist, kann Sie jedoch auf maximal 1 GB freien Speicherplatz auf dem Datenträger anwachsen.

Leistungsindikatoren

Verschiedene Leistungsindikatoren sind mit Seiten Dateien verbunden. In diesem Abschnitt werden die Indikatoren und ihre Measures beschrieben.

\ Arbeitsspeicher \ Seite/Sek. und andere Fehlerindikatoren für harte Seiten

Die folgenden Leistungsindikatoren messen harte Seitenfehler (einschließlich, aber nicht darauf beschränkend, Seitendatei Lesevorgänge):

- \ Arbeitsspeicher \ Seite/Sek.
- \Memory\Page-Lesevorgänge/Sek.
- \Memory\Page-Eingaben/Sek.

Die folgenden Leistungsindikatoren messen eine Auslagerungsdatei:

- \Memory\Page-Schreibvorgänge/Sek.
- \Memory\Page-Ausgabe/Sek.

Harte Seitenfehler sind Fehler, die durch Abrufen der Daten vom Datenträger aufgelöst werden müssen. Solche Daten können Teile von DLLs, exe-Dateien, Arbeitsspeicher zugeordnete Dateien und Seiten Dateien umfassen. Diese Fehler sind möglicherweise mit einer Auslagerungsdatei oder mit einem Zustand mit geringem Arbeitsspeicher verbunden. Harte Seitenfehler sind eine Standardfunktion des Betriebssystems. Sie treten auf, wenn die folgenden Elemente gelesen werden:

- Teile von Bilddateien (dll-und exe-Dateien) während der Verwendung
- Speicher zugeordnete Dateien
- Eine Seitendatei

Hohe Werte für diese Leistungsindikatoren (übermäßiges Paging) zeigen den Datenträgerzugriff in der Regel 4 KB pro Seitenfehler auf x86-und x64-Versionen von Windows und Windows Server an. Dieser Datenträgerzugriff ist

möglicherweise mit einer Auslagerungsdatei Aktivität verbunden, kann aber zu einer schlechten Festplattenleistung beitragen, die systemweite Verzögerungen verursachen kann, wenn die zugehörigen Datenträger überlastet sind.

Daher empfiehlt es sich, die Datenträgerleistung der logischen Datenträger zu überwachen, die eine Auslagerungsdatei in Korrelation mit diesen Leistungsindikatoren hosten. Beachten Sie, dass ein System, das über eine dauerhafte 100-fehlerhafte Seitenfehler pro Sekunde verfügt, 400 KB pro Sekunde Festplatten Übertragungen erlebt. Bei den meisten 7.200-rpm-Laufwerken können ca. 5 MB pro Sekunde bei einer IO-Größe von 16 KB oder 800 KB pro Sekunde bei einer IO-Größe von 4 KB verarbeitet werden. Kein Leistungsindikator misst direkt den logischen Datenträger, für den die hart Seitenfehler aufgelöst werden.

\Paging-Datei (*) % Verwendung

Der \Paging-Datei (*) % Usage PerformanceCounter misst den Prozentsatz der Nutzung jeder Auslagerungsdatei. die Verwendung einer Auslagerungsdatei in 100 Prozent deutet nicht auf ein Leistungsproblem hin, solange das System Commit-Limit nicht durch das System Commit-Entgelt erreicht wird und wenn eine beträchtliche Menge an Arbeitsspeicher nicht darauf wartet, in eine Auslagerungsdatei geschrieben zu werden.

> **NOTE**
> Die Größe der geänderten Seitenliste (Bytes der \Memory\Modified-Seitenliste) ist die Summe der geänderten Daten, die darauf warten, auf den Datenträger geschrieben zu werden.

Wenn die geänderte Seitenliste (eine Liste der Seiten, auf denen der physische Arbeitsspeicher am wenigsten häufig zugegriffen wird) viel Arbeitsspeicher enthält und wenn der **% Usage** -Wert aller Seiten Dateien größer als 90 ist, können Sie mehr physikalischen Speicher für häufigere Zugriffsseiten verfügbar machen, indem Sie eine Auslagerungsdatei erhöhen oder hinzufügen.

> **NOTE**
> Nicht der gesamte Arbeitsspeicher der geänderten Seitenliste wird auf den Datenträger geschrieben. In der Regel bleiben mehrere hundert Megabyte speicherresident in der geänderten Liste.

Überlegungen zu mehreren Seiten Dateien und Datenträgern

Wenn ein System so konfiguriert ist, dass es mehr als eine Seitendatei enthält, ist die Seitendatei, die zuerst antwortet, diejenige, die verwendet wird. Das bedeutet, dass Seiten Dateien, die sich auf schnelleren Datenträgern befinden, häufiger verwendet werden. Darüber hinaus ist es wichtig, ob Sie eine Auslagerungsdatei auf einen "schnellen" oder "langsamen" Datenträger setzen, nur, wenn häufig auf die Auslagerungsdatei zugegriffen wird und der Datenträger, der die jeweilige Auslagerungsdatei hostet, überlastet ist. Beachten Sie, dass die Verwendung der tatsächlichen Seitendatei stark von der Größe des geänderten Speichers abhängt, den das System verwaltet. Das bedeutet, dass Dateien, die bereits auf einem Datenträger vorhanden sind (wie txt, doc, dll und exe), nicht in eine Auslagerungsdatei geschrieben werden. Nur geänderte Daten, die noch nicht auf dem Datenträger vorhanden sind (beispielsweise nicht gespeicherter Text in Editor), sind Speicher, der möglicherweise von einer Auslagerungsdatei unterstützt wird. Nachdem die nicht gespeicherten Daten als Datei auf dem Datenträger gespeichert wurden, wird Sie vom Datenträger und nicht von einer Auslagerungsdatei gesichert.

Generieren eines Kernels oder eines vollständigen Absturz Dumps

11.10.2019 • 3 minutes to read

Ein Systemabsturz (auch bekannt als "Fehlerüberprüfung" oder "Abbruchfehler") tritt auf, wenn Windows nicht ordnungsgemäß ausgeführt werden kann. Die aus diesem Ereignis erstellte Dumpdatei wird als Systemabsturz-Dump bezeichnet.

Eine manuelle Kernel-oder vollständige Speicherabbilddatei ist hilfreich, wenn Sie mehrere Probleme beheben, da der Prozess zum Zeitpunkt des Absturzes einen Datensatz des Systemspeichers erfasst.

Einrichten von Seiten Dateien

Weitere Informationen finden Sie unter Unterstützung für Systemabsturz Abbilder für die Auslagerungsdateigröße für Systemabsturz Dump.

Einstellung ' Speicherabbild aktivieren '

Sie müssen als Administrator oder als Mitglied der Gruppe Administratoren angemeldet sein, um dieses Verfahren ausführen zu können. Wenn Ihr Computer mit einem Netzwerk verbunden ist, verhindern Sie möglicherweise, dass die Netzwerkrichtlinieneinstellungen diesen Vorgang abschließen.

Führen Sie die folgenden Schritte aus, um die Speicherabbild Einstellung zu aktivieren:

1. Wählen Sie in der System **Steuerung System und Sicherheits** > **System**aus.
2. Wählen Sie **Erweiterte Systemeinstellungen**aus, und wählen Sie dann die Registerkarte **erweitert** aus.
3. Wählen Sie im Bereich **Start und Wiederherstellung** die Option **Einstellungen**aus.
4. Stellen Sie sicher, dass unter **Debuginformationen schreiben**das **Kernel Speicherabbild** oder das **vollständige Speicherabbild** ausgewählt ist.
5. Starten Sie den Computer neu.

> **NOTE**
>
> Sie können den Pfad der Speicherabbilddatei ändern, indem Sie das Feld **Dumpdatei** bearbeiten. Anders ausgedrückt: Sie können den Pfad von%SystemRoot%\Memory.dmp so ändern, dass er auf ein lokales Laufwerk zeigt, das über genügend Speicherplatz verfügt, beispielsweise E:\Memory.dmp.

Tipps zum Generieren von Speicherabbildern

Wenn der Computer abstürzt und neu gestartet wird, wird der Inhalt des physikalischen Arbeitsspeichers in die Auslagerungsdatei geschrieben, die sich auf der Partition befindet, auf der das Betriebssystem installiert ist.

Je nach der Geschwindigkeit der Festplatte, auf der Windows installiert ist, kann das Dumping von mehr als 2 GB Speicherplatz viel Zeit in Anspruch nehmen. Auch wenn die Speicherabbilddatei so konfiguriert ist, dass Sie sich auf einer anderen lokalen Festplatte befindet, wird eine beträchtliche Datenmenge gelesen und auf die Festplatten geschrieben. Dies kann zu einem längeren Serverausfall führen.

> **NOTE**
> Verwenden Sie diese Methode, um vollständige Speicherabbilddateien mit Vorsicht zu generieren. Im Idealfall sollten Sie dies nur dann tun, wenn Sie vom Microsoft-Support Techniker ausdrücklich dazu aufgefordert werden. Alle Kernel-oder vollständigen Speicherabbild-Datei Debuggen sollten der letzte Ausweg sein, nachdem alle standardmäßigen Methoden zur Problembehandlung vollständig erschöpft sind.

Manuelles Erstellen einer Speicherabbilddatei

Verwenden des NotMyFault-Tools

Wenn Sie sich während des Auftretens des Problems anmelden können, können Sie das Microsoft Sysinternals-Tool NotMyFault verwenden. Gehen Sie hierzu folgendermaßen vor:

1. Laden Sie das NotMyFault -Tool herunter.
2. Wählen Sie **Start**aus, und wählen Sie dann **Eingabeaufforderung**aus.
3. Führen Sie in der Befehlszeile den folgenden Befehl aus:

```
notMyfault.exe /crash
```

> **NOTE**
> Dieser Vorgang generiert eine Speicherabbilddatei und einen D1-Stopp-Fehler.

Verwenden von NMI

Auf einigen Computern können Sie keine Absturzspeicherabbild Datei mithilfe der Tastatur erstellen. So werden beispielsweise Hewlett-Packard (HP) c Blade Systeme-Server aus dem Hewlett-Packard-Entwicklungsunternehmen über eine browserbasierte grafische Benutzeroberfläche (Graphical User Interface, GUI) verwaltet. Eine Tastatur ist nicht mit dem HP c Blade Systeme-Server verbunden.

In diesen Fällen müssen Sie eine vollständige Absturzspeicherabbild Datei oder eine Kernel Absturz-Dumpdatei generieren, indem Sie den nicht maskierten Interrupt (NMI)-Schalter verwenden, der einen NMI auf dem Systemprozessor verursacht.

Gehen Sie hierzu folgendermaßen vor:

> **IMPORTANT**
> Führen Sie die Schritte in diesem Abschnitt sorgfältig aus. Wird die Registrierung falsch angepasst, können schwerwiegende Probleme auftreten. Bevor Sie ihn ändern, Sichern Sie die Registrierung für die Wiederherstellung , falls Probleme auftreten.

1. Suchen Sie im Registrierungs-Editor den folgenden Registrierungsunterschlüssel: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl**
2. Klicken Sie mit der rechten Maustaste auf **CrashControl**, zeigen Sie auf **neu**, und klicken Sie dann auf **DWORD-Wert**.
3. Geben Sie NMICrashDump ein, und drücken Sie dann die EINGABETASTE.
4. Klicken Sie mit der rechten Maustaste auf **NMICrashDump**, und wählen Sie dann **ändern**aus.
5. Geben Sie im Feld **Wertdaten den Wert 1 ein**, und wählen Sie dann **OK**aus.

6. Starten Sie den Computer neu.

7. Hardware Anbieter wie HP, IBM und Dell stellen möglicherweise eine automatische System Wiederherstellungsfunktion (Automatic System Recovery, ASR) bereit. Sie sollten dieses Feature während der Problembehandlung deaktivieren. Wenn beispielsweise das Feature HP und Compaq ASR im BIOS aktiviert ist, deaktivieren Sie dieses Feature, während Sie die Problembehandlung ausführen, um eine vollständige Datei "Memory. dmp" zu generieren. Die genauen Schritte erhalten Sie von Ihrem Hardwareanbieter.

8. Aktivieren Sie den NMI-Schalter im BIOS oder über die integrierte Lights Out (ILO)-Weboberfläche.

> **NOTE**
>
> Die genauen Schritte finden Sie im BIOS-Referenzhandbuch, oder wenden Sie sich an Ihren Hardwareanbieter.

9. Testen Sie diese Methode auf dem Server, indem Sie die NMI-Option verwenden, um eine Speicherabbilddatei zu generieren. Sie sehen eine Fehlfunktion der 0x00000080-Hardware.

Verwenden der Tastatur

Erzwingen eines System Absturzes über die Tastatur

Verwenden des Debuggers

Erzwingen eines System Absturzes vom Debugger

Einführung in Seiten Dateien

06.03.2020 • 2 minutes to read

Eine Auslagerungsdatei (auch als "Auslagerungsdatei" bezeichnet) ist eine optionale versteckte System Datei auf einer Festplatte.

Funktion

Seiten Dateien weisen die folgenden Funktionalitäten auf:

Physische Erweiterung des Arbeitsspeichers

Seiten Dateien ermöglichen es dem System, selten aufgerufene geänderte Seiten aus dem physikalischen Speicher zu entfernen, damit das System den physikalischen Speicher für häufiger zugängliche Seiten effizienter nutzen kann.

Anforderungen an Anwendungen

Einige Produkte oder Dienstleistungen erfordern eine Auslagerungsdatei aus verschiedenen Gründen. Spezifische Informationen finden Sie in der Produktdokumentation.

Die folgenden Windows-Server erfordern beispielsweise Seiten Dateien:

- Windows Server-Domänencontroller (DCS)
- DFS-Replikation (DFS-R) Server
- Zertifikatserver
- Adam/LDS-Server

Der Grund dafür ist, dass der Algorithmus des Datenbankcaches für die erweiterbare Speichermodul (ESENT oder ESE in Microsoft Exchange Server) vom Leistungsmonitorindikator "\Memory\Transition Pages purposed/sec" abhängt. Eine Auslagerungsdatei ist erforderlich, um sicherzustellen, dass der Datenbankcache Speicher freigeben kann, wenn andere Dienste oder Anwendungen Arbeitsspeicher anfordern.

Für Windows Server 2012 Hyper-v und Windows Server 2012 R2 Hyper-v sollte die Auslagerungsdatei des Verwaltungsbetriebssystems (gemeinhin als Hostbetriebssystem bezeichnet) standardmäßig auf "System verwaltet" festgelegt werden.

Unterstützung für Systemabsturz-Dumps

Seiten Dateien können verwendet werden, um Systemabsturz Abbilder zu "zurück" (oder zu unterstützen) und zu erweitern, wie viel vom System zugesicherter Speicher (auch bekannt als "virtueller Speicher"), den ein System unterstützenkann.

Weitere Informationen zu Systemabsturz Abbildern finden Sie unter Systemabsturz-Dump-Optionen.

Seiten Dateien in Windows mit großem physikalischen Speicher

Wenn großer physikalischer Arbeitsspeicher installiert ist, ist möglicherweise eine Auslagerungsdatei nicht erforderlich, um die System Commit-Belastung während der Spitzenauslastung zu unterstützen. Beispielsweise unterstützen 64-Bit-Versionen von Windows und Windows Server mehr physikalischen Arbeitsspeicher (RAM) als die Unterstützung von 32-Bit-Versionen. Der verfügbare physische Speicher kann allein groß genug sein.

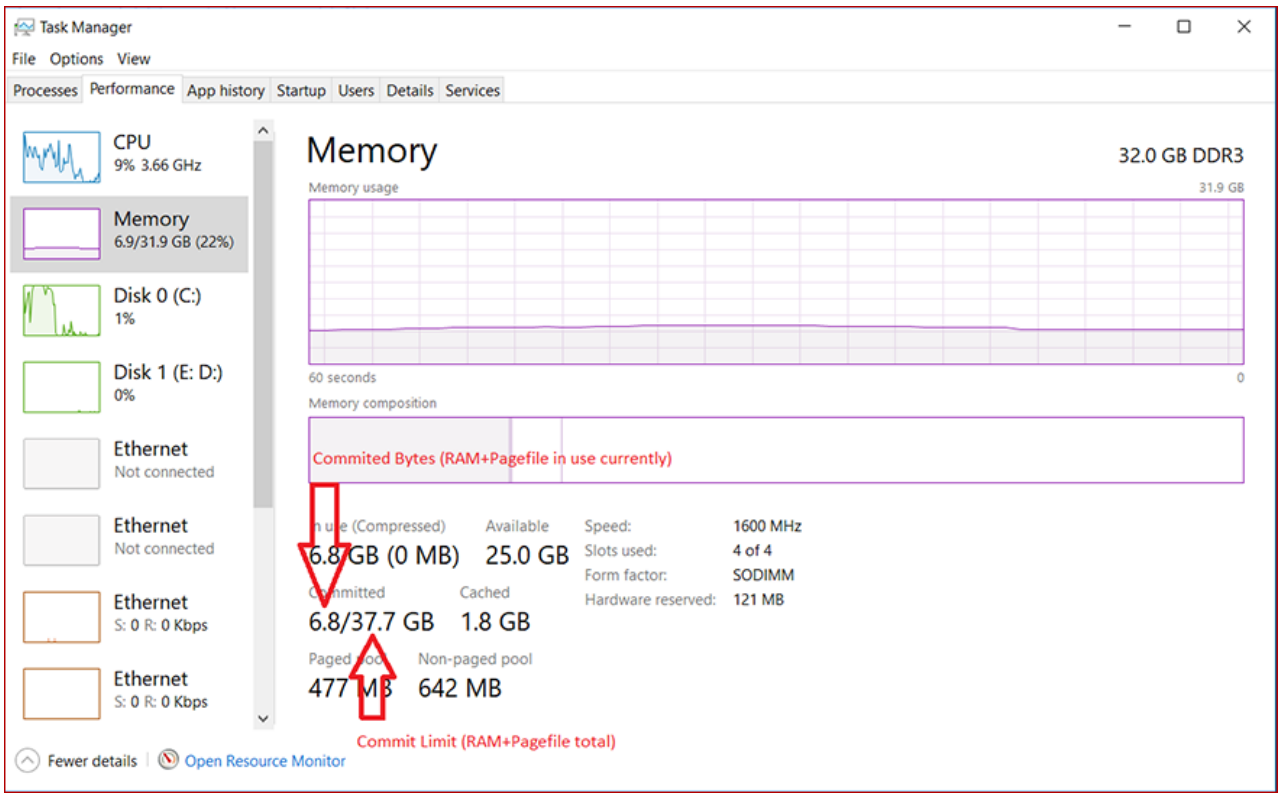
Der Grund für die Konfiguration der Seitendatei Größe hat sich jedoch nicht geändert. Es ging immer um die Unterstützung eines Systemabsturz Dumps, falls dies erforderlich ist, oder um die Erweiterung des System Commit-Limits, falls dies erforderlich ist. Wenn beispielsweise viel physischer Arbeitsspeicher installiert ist, ist es

möglich, dass eine Auslagerungsdatei nicht erforderlich ist, um die System Begehung während der Spitzenauslastung zu sichern. Der verfügbare physische Speicher kann allein groß genug sein, um dies zu tun. Es ist jedoch möglich, dass eine Auslagerungsdatei oder eine dedizierte Dumpdatei zum Zurücksetzen eines Systemabsturz Dumps erforderlich ist.

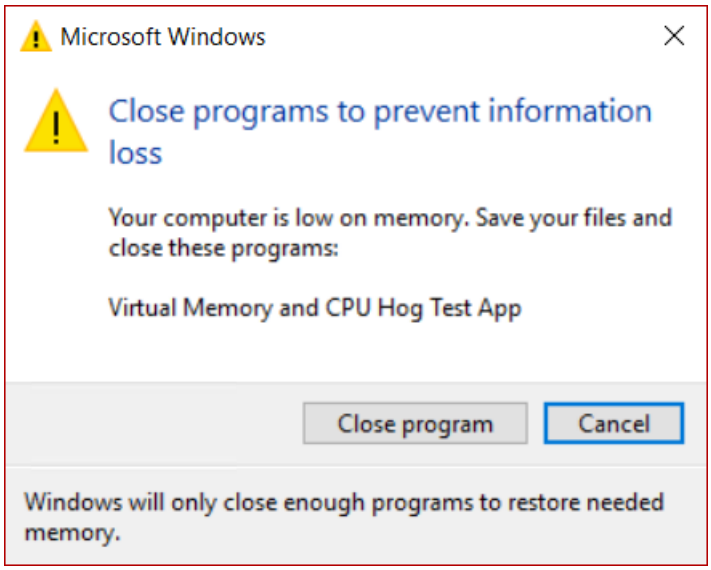
System zugesicherter Speicher

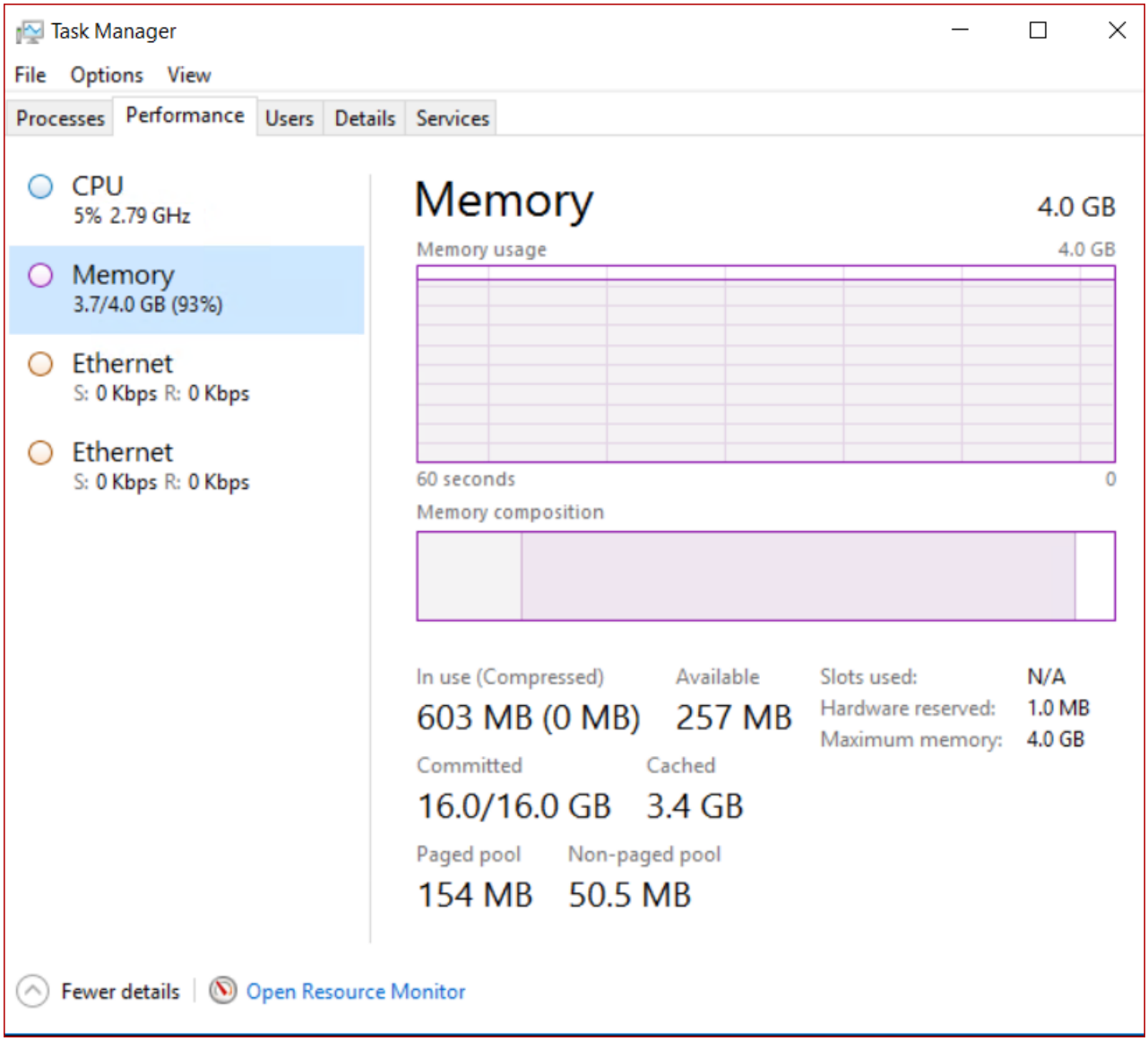
Seiten Dateien verlängern, wie viel "zugesicherter Speicher" (auch bekannt als "virtueller Speicher") zum Speichern geänderter Daten verwendet wird.

Der Speichergrenzwert des System Commits ist die Summe aus physikalischem Arbeitsspeicher und allen Seiten Dateien kombiniert. Sie stellt den maximalen, vom System zugesicherten Speicher (auch als "System Commit Charge" bezeichnet) dar, den das System unterstützenkann.



Das System-Commit-Entgelt ist der gesamte zugesicherte oder "versprochene" Speicher des gesamten zugesicherten virtuellen Speichers im System. Wenn die System Commit-Belastung das System Commit-Limit erreicht, erhalten das System und die Prozesse möglicherweise keinen zugesicherten Speicher. Diese Bedingung kann zu einem Einfrieren, Absturz und anderen Störungen führen. Stellen Sie daher sicher, dass Sie das System Commit-Limit hoch genug festlegen, um die System Commit-Belastung während der Spitzenauslastung zu unterstützen.





Das System Committed Charge-und System Committed-Limit kann auf der Registerkarte **Leistung** im Task-Manager oder mithilfe der Leistungsindikatoren "\Memory\Committed Bytes" und "\Memory\Commit Limit" gemessen werden. Der Leistungsindikator \Memory% Committed Bytes in use ist ein Verhältnis von \Memory\Committed Bytes zu \Memory\Commit Grenzwerten.

NOTE

Vom System verwaltete Seiten Dateien werden automatisch bis zu dreimal so groß wie der physikalische Arbeitsspeicher oder 4 GB (je nachdem, welcher Wert größer ist), wenn die System Commit-Belastung 90 Prozent des System Commit-Limits erreicht. Dabei wird davon ausgegangen, dass genügend freier Speicherplatz für das Wachstum verfügbar ist.

Konfigurieren von Systemausfall- und Wiederherstellungsoptionen in Windows

06.03.2020 • 7 minutes to read

In diesem Artikel wird beschrieben, wie Sie die Aktionen konfigurieren, die Windows ausführt, wenn ein Systemfehler (auch als Fehlerüberprüfung, Systemabsturz, schwerwiegender Systemfehler oder Abbruchfehler bezeichnet) eintritt. Sie können die folgenden Aktionen konfigurieren:

- Schreiben Sie ein Ereignis in das System Protokoll.
- Benachrichtigen Sie Administratoren (wenn Sie Administratorbenachrichtigungen eingerichtet haben).
- Fügen Sie den Systemspeicher in eine Datei ein, die erfahrene Benutzer zum Debuggen verwenden können.
- Starten Sie den Computer automatisch neu.

> **NOTE**
> Sie müssen als Administrator oder als Mitglied der Gruppe Administratoren angemeldet sein, um dieses Verfahren ausführen zu können. Wenn Ihr Computer mit einem Netzwerk verbunden ist, verhindern Sie möglicherweise, dass die Netzwerkrichtlinieneinstellungen diesen Vorgang abschließen.

Konfigurieren von Systemfehler-und Wiederherstellungsoptionen

> **IMPORTANT**
> Führen Sie die Schritte in diesem Abschnitt sorgfältig aus. Wird die Registrierung falsch angepasst, können schwerwiegende Probleme auftreten. Bevor Sie ihn ändern, Sichern Sie die Registrierung für die Wiederherstellung , falls Probleme auftreten.

Die Optionen sind im Dialogfeld **Start und Wiederherstellung** verfügbar. Sie können auch die folgenden Methoden verwenden:

- Ändern Sie die Werte unter dem folgenden Registrierungsunterschlüssel:

  HKEY_LOCAL_MACHINE \system\currentcontrolset\control\crashcontrol

- Wenn Sie die Option auf dem lokalen Computer ändern möchten, verwenden Sie das Befehlszeilendienstprogramm (WMIC. exe) für den Zugriff auf die Windows-Verwaltungsinstrumentation (WMI).

Führen Sie die folgenden Schritte aus, um die Optionen für **Start und Wiederherstellung**anzuzeigen. (Der Registrierungswert und die WMIC-Befehle werden auch für jede Option aufgelistet.)

1. Wählen Sie in der Systemsteuerung **System und Sicherheit > System**aus.
2. Wählen Sie **Erweiterte Systemeinstellungen**aus, wählen Sie die Registerkarte **erweitert** aus, und wählen Sie im **Start-und Wiederherstellungs** Bereich **Einstellungen** aus.

Unter "System Fehler"

Aktivieren Sie die Kontrollkästchen für die Aktionen, die Windows ausführen soll, wenn ein Systemfehler auftritt.

Schreiben eines Ereignisses in das System Protokoll

Mit dieser Option wird angegeben, dass Ereignisinformationen im System Protokoll aufgezeichnet werden. Diese Option ist standardmäßig aktiviert.

Um diese Option zu deaktivieren, führen Sie den folgenden Befehl aus, oder ändern Sie den Registrierungswert:

```
wmic recoveros set WriteToSystemLog = False
```

- Setzen Sie den **LogEvent** -DWORD-Wert auf **0**.

Senden einer administrativen Benachrichtigung

Die Option gibt an, dass Administratoren über den Systemfehler benachrichtigt werden, wenn Sie Administratorbenachrichtigungen konfiguriert haben. Diese Option ist standardmäßig aktiviert.

Um diese Option zu deaktivieren, führen Sie den folgenden Befehl aus, oder ändern Sie den Registrierungswert:

```
wmic recoveros set SendAdminAlert = False
```

- Setzen Sie den **SendAlert** -DWORD-Wert auf **0**.

Automatisch neu starten

Die Option gibt an, dass Windows Ihren Computer automatisch neu startet. Diese Option ist standardmäßig aktiviert.

Um diese Option zu deaktivieren, führen Sie den folgenden Befehl aus, oder ändern Sie den Registrierungswert:

```
wmic recoveros set AutoReboot = False
```

- Setzen Sie den DWORD-Wert " **AutoReboot** " auf " **0**".

Unter "Debuginformationen schreiben"

Wählen Sie einen der folgenden Informationstypen aus, die Windows in einer Speicherabbilddatei aufzeichnen soll, wenn der Computer unerwartet beendet wird:

(keine)

Die Option zeichnet keine Informationen in einer Speicherabbilddatei auf.

Wenn Sie angeben möchten, dass Windows keine Informationen in einer Speicherabbilddatei aufzeichnen soll, führen Sie den folgenden Befehl aus, oder ändern Sie den Registrierungswert:

- `cmd wmic recoveros set DebugInfoType = 0`
- Setzen Sie den **CrashDumpEnabled** -DWORD-Wert auf **0**.

Kleiner Speicherauszug

Die Option zeichnet die kleinste Menge an Informationen auf, um das Problem zu erkennen. Diese Option erfordert eine Auslagerungsdatei mit mindestens 2 Megabyte (MB) auf dem Startvolume Ihres Computers und gibt an, dass Windows jedesmal eine neue Datei erstellt, wenn das System unerwartet beendet wird. Ein Verlauf dieser Dateien wird in dem Ordner gespeichert, der unter kleines Speicherabbild Verzeichnis (%SystemRoot%\Minidump) aufgeführt ist. Unter Windows XP und Windows Server 2003 wird die kleine Speicherabbilddatei zusammen mit dem Windows-Feature zur Fehlerberichterstattung verwendet.

Um anzugeben, dass Sie eine kleine Speicherabbilddatei verwenden möchten, führen Sie den folgenden Befehl aus, oder ändern Sie den Registrierungswert:

```
wmic recoveros set DebugInfoType = 3
```

- Stellen Sie den **CrashDumpEnabled** -DWORD-Wert auf **3**ein.

Um anzugeben, dass Sie einen Ordner als kleines Speicherabbild Verzeichnis verwenden möchten, führen Sie den folgenden Befehl aus, oder ändern Sie den Registrierungswert:

```
wmic recoveros set MiniDumpDirectory = <folderpath>
```

- Setzen Sie den Wert der **MinidumpDir** -Erweiterungs Zeichenfolge auf \ <folderPath \ >.

Kernel Speicherabbild

Die Option zeichnet nur den Kernelspeicher auf. Diese Option speichert mehr Informationen als eine kleine Speicherabbilddatei, aber es dauert weniger Zeit als eine vollständige Speicherabbilddatei. Die Datei wird standardmäßig in%SystemRoot%\Memory.dmp gespeichert, und alle vorherigen Kernel-oder vollständigen Speicherabbilddateien werden überschrieben, wenn das Kontrollkästchen **vorhandene Datei überschreiben** aktiviert ist. Wenn Sie diese Option aktivieren, müssen Sie über eine ausreichend große Auslagerungsdatei auf dem Startvolume verfügen. Die erforderliche Größe hängt von der Größe des Arbeitsspeichers auf Ihrem Computer ab, aber der maximale Speicherplatz, der für ein Kernelspeicherabbild auf einem 32-Bit-System verfügbar sein muss, beträgt 2 GB plus 16 MB. Bei einem 64-Bit-System ist der maximale Speicherplatz, der für einen Kernelspeicher Auszug verfügbar sein muss, die Größe des RAM plus 128 MB. In der folgenden Tabelle finden Sie Richtlinien für die Größe der Auslagerungsdatei:

RAM-GRÖSSE	DIE AUSLAGERUNGSDATEI SOLLTE NICHT KLEINER ALS SEIN
256 MB – 1373 MB	1,5 Mal die RAM-Größe
1.374 MB oder höher	32-Bit-System: 2 GB plus 16 MB 64-Bit-System: Größe des RAM plus 128 MB

Führen Sie den folgenden Befehl aus, um anzugeben, dass Sie eine Kernelspeicherabbild Datei verwenden möchten, oder ändern Sie den Registrierungswert:

```
wmic recoveros set DebugInfoType = 2
```

- Setzen Sie den **CrashDumpEnabled** -DWORD-Wert auf **2**.

Um anzugeben, dass Sie eine Datei als Speicherabbilddatei verwenden möchten, führen Sie den folgenden Befehl aus, oder ändern Sie den Registrierungswert:

```
wmic recoveros set DebugFilePath = <filepath>
```

- Setzen Sie den Wert für die erweiterbare **Dumpdatei** -Zeichenfolge auf \ <filePath \ >.

Um anzugeben, dass Sie keine vorherigen Kernel-oder vollständigen Speicherabbilddateien überschreiben möchten, führen Sie den folgenden Befehl aus, oder ändern Sie den Registrierungswert:

```
wmic recoveros set OverwriteExistingDebugFile = 0
```

- Setzen Sie den DWORD-Wert **overwrite** auf **0**.

Vollständiges Speicherabbild

Die Option zeichnet den Inhalt des Systemspeichers auf, wenn der Computer unerwartet beendet wird. Diese Option steht auf Computern mit mindestens 2 GB Arbeitsspeicher nicht zur Verfügung. Wenn Sie diese Option auswählen, muss auf dem Startvolume eine Auslagerungsdatei vorhanden sein, die ausreicht, um den gesamten physikalischen Arbeitsspeicher Plus 1 MB zu speichern. Die Datei wird standardmäßig in%SystemRoot%\Memory.dmp gespeichert.

Das zusätzliche Megabyte ist für eine vollständige Speicherabbilddatei erforderlich, da Windows zusätzlich zum dumpen des Speicherinhalts eine Kopfzeile schreibt. Der Header enthält eine Crash Dump-Signatur und gibt die Werte einiger Kernel Variablen an. Die Headerinformationen erfordern kein vollständiges Megabyte an Speicherplatz, aber Windows passt Ihre Auslagerungsdatei in Schritten von Megabyte an.

Führen Sie den folgenden Befehl aus, um anzugeben, dass Sie eine vollständige Speicherabbilddatei verwenden möchten, oder ändern Sie den Registrierungswert:

```
wmic recoveros set DebugInfoType = 1
```

- Stellen Sie den **CrashDumpEnabled** -DWORD-Wert auf **1 ein**.

Um anzugeben, dass Sie eine Datei als Speicherabbilddatei verwenden möchten, führen Sie den folgenden Befehl aus, oder ändern Sie den Registrierungswert:

```
wmic recoveros set DebugFilePath = <filepath>
```

- Setzen Sie den Wert für die erweiterbare Dumpdatei-Zeichenfolge auf \ <filePath \ >.

Um anzugeben, dass Sie keine vorherigen Kernel-oder vollständigen Speicherabbilddateien überschreiben möchten, führen Sie den folgenden Befehl aus, oder ändern Sie den Registrierungswert:

```
wmic recoveros set OverwriteExistingDebugFile = 0
```

- Setzen Sie den DWORD-Wert **overwrite** auf **0**.

> **NOTE**
> Wenn Sie sich an den Microsoft-Support zu einem Stoppfehler wenden, werden Sie möglicherweise nach der Speicherabbilddatei gefragt, die von der Option Debuginformationen schreiben generiert wird.

Wenn Sie die Systemfehler-und Wiederherstellungseinstellungen für Ihren lokalen Computer anzeigen möchten, geben Sie **WMIC Recoverys** an einer Eingabeaufforderung ein, und drücken Sie dann die EINGABETASTE. Wenn Sie die Systemfehler-und Wiederherstellungseinstellungen für einen Remotecomputer in Ihrem lokalen Netzwerk anzeigen möchten, geben Sie **WMIC/Node: <computer_name> wiederherstellen** an einer Eingabeaufforderung ein, und drücken Sie dann die EINGABETASTE.

> **NOTE**
> Um diese WMIC. exe-Befehlszeilenbeispiele erfolgreich verwenden zu können, müssen Sie mit einem Benutzerkonto angemeldet sein, das über Administratorrechte auf dem Computer verfügt. Wenn Sie nicht mit einem Benutzerkonto angemeldet sind, das über Administratorrechte auf dem Computer verfügt, verwenden Sie die Optionen **/User: user_name** und **/Password: Kennwort** .

Tipps

- Um das Feature "Dumpdatei" nutzen zu können, muss sich Ihre Auslagerungsdatei auf dem Startvolume befinden. Wenn Sie die Auslagerungsdatei auf ein anderes Volume verschoben haben, müssen Sie Sie auf das Startvolume zurück verschieben, bevor Sie dieses Feature verwenden.
- Wenn Sie das Kernel Speicherabbild oder die Option Vollständiges Speicherabbild festlegen und das Kontrollkästchen **vorhandene Datei überschreiben** aktivieren, schreibt Windows immer denselben Dateinamen. Wenn Sie einzelne Speicherabbilddateien speichern möchten, deaktivieren Sie das Kontrollkästchen **vorhandene Datei überschreiben** , und ändern Sie dann den Dateinamen nach jedem Abbruchfehler.
- Sie können Speicherplatz sparen, wenn Sie auf das Kontrollkästchen **Ereignis in das Systemprotokoll schreiben** und **administrative Benachrichtigung senden** klicken. Der Speicher, den Sie speichern, hängt vom Computer ab, aber diese Features erfordern in der Regel etwa 60 bis 70 KB.

Verweise

Varianten von Speicherabbilddateien im Kernel Modus

Erweiterte Problembehandlung für Windows-Startprobleme

08.01.2020 • 11 minutes to read

NOTE

Dieser Artikel ist für die Verwendung durch Support-Mitarbeiter und IT-Experten vorgesehen. Wenn Sie nach weiteren allgemeinen Informationen zu Wiederherstellungsoptionen suchen, lesen Sie Wiederherstellungsoptionen in Windows 10.

Zusammenfassung

Es gibt mehrere Gründe, warum ein Windows-basierter Computer während des Starts möglicherweise Probleme aufweist. Ermitteln Sie zum Beheben von Startproblemen zunächst, in welcher der folgenden Phasen der Computer hängen bleibt:

PHASE	STARTVORGANG	BIOS	UEFI
1	Preboot	MBR/PBR (Bootstrap-Code)	UEFI-Firmware
2	Windows-Start-Manager	%SystemDrive%\bootmgr	\EFI\Microsoft\Boot\bootmgfw.efi
3	Windows-Betriebssystem-Loader	%SystemRoot%\system32\winload.exe	%SystemRoot%\system32\winload.efi
4	Windows NT-Betriebssystem Kernel	%SystemRoot%\system32\ntoskrnl.exe	

1. Preboot

Die PC-Firmware initiiert einen Einschalt selbst Test (Post) und lädt die Firmware-Einstellungen. Dieser Pre-Boot-Prozess endet, wenn ein gültiger Systemdatenträger erkannt wird. Firmware liest den Master Boot Record (MBR) und startet dann den Windows-Start-Manager.

2. Windows-Start-Manager

Windows-Start-Manager findet und startet das Windows-Ladeprogramm (Winload. exe) auf der Windows-Startpartition.

3. Loader für Windows-Betriebssystem

Wichtige Treiber, die für den Start des Windows-Kernels erforderlich sind, werden geladen, und der Kernel wird ausgeführt.

4. Windows NT-Betriebssystem Kernel

Der Kernel lädt die Systemregistrierungsstruktur und zusätzliche Treiber, die als BOOT_START gekennzeichnet sind, in den Arbeitsspeicher.

Der Kernel übergibt die Steuerung an den Sitzungs-Manager-Prozess (SMS. exe), der die Systemsitzung initialisiert, und lädt und startet die Geräte und Treiber, die nicht BOOT_START gekennzeichnet sind.

Nachfolgend finden Sie eine Zusammenfassung der Startsequenz, was auf dem Bildschirm zu sehen ist, und typische Startprobleme an diesem Punkt in der Sequenz. Bevor Sie mit der Problembehandlung beginnen, müssen Sie sich mit der Gliederung des Startprozesses und dem Anzeigestatus vertraut machen, um sicherzustellen, dass das Problem zu Beginn des Projekts richtig erkannt wurde.

Klicken und vergrößern

Jede Phase hat einen anderen Ansatz bei der Problembehandlung. Dieser Artikel enthält Problembehandlungstechniken für Probleme, die während der ersten drei Phasen auftreten.

> **NOTE**
>
> Wenn der Computer wiederholt zu den Wiederherstellungsoptionen bootet, führen Sie an einer Eingabeaufforderung den folgenden Befehl aus, um den Zyklus zu unterbrechen:
>
> ```
> Bcdedit /set {default} recoveryenabled no
> ```
>
> Wenn die F8-Optionen nicht funktionieren, führen Sie den folgenden Befehl aus:
>
> ```
> Bcdedit /set {default} bootmenupolicy legacy
> ```

BIOS-Phase

Führen Sie die folgenden Schritte aus, um zu ermitteln, ob das System die BIOS-Phase überschritten hat:

1. Wenn externe Peripheriegeräte an den Computer angeschlossen sind, trennen Sie Sie.
2. Überprüfen Sie, ob die Festplatten Leuchte auf dem physikalischen Computer funktioniert. Wenn dies nicht der Fall ist, deutet dies darauf hin, dass der Startvorgang in der BIOS-Phase hängen bleibt.
3. Drücken Sie die Taste Num, um festzustellen, ob die Anzeigeleuchte ein-und ausgeschaltet wird. Wenn dies nicht der Fall ist, weist dies darauf hin, dass der Startvorgang beim BIOS hängen bleibt.

Wenn das System in der BIOS-Phase hängen bleibt, liegt möglicherweise ein Hardwareproblem vor.

Boot-Loader-Phase

Wenn der Bildschirm komplett schwarz ist, mit Ausnahme eines blinkenden Cursors, oder wenn Sie einen der folgenden Fehlercodes erhalten, deutet dies darauf hin, dass der Startvorgang in der Phase des Bootloaders fest steht:

- Startkonfigurationsdaten (BCD) fehlen oder sind beschädigt
- Boot-Datei oder MBR-fehlerhaft
- Betriebssystem fehlt
- Boot Sektor fehlt oder ist beschädigt
- Nicht vorhanden oder fehlerhaft
- Aufgrund fehlender oder fehlerhafter Systemstruktur kann nicht gestartet werden

Um dieses Problem zu beheben, verwenden Sie Windows-Installationsmedien, um den Computer zu starten, drücken Sie UMSCHALT + F10 für eine Eingabeaufforderung, und verwenden Sie dann eine der folgenden Methoden.

Methode 1: Tool zum Starten der Reparatur

Das Startreparatur Tool behebt automatisch viele häufige Probleme. Darüber hinaus können Sie mit dem Tool komplexere Startprobleme schnell diagnostizieren und beheben. Wenn der Computer ein Startproblem erkennt, startet der Computer das Tool zum Starten der Reparatur. Wenn das Tool gestartet wird, wird eine Diagnose durchgeführt. Diese Diagnose umfasst das Analysieren von Startprotokolldateien, um die Ursache des Problems zu ermitteln. Wenn das Tool zum Starten der Reparatur die Ursache ermittelt, versucht das Tool, das Problem automatisch zu beheben.

Folgen Sie dazu thesesteps.

> **NOTE**
> Weitere Methoden zum Starten von WinRE finden Sie unter Windows-Wiederherstellungsumgebung (Windows RE).

1. Starten Sie das System auf dem Installationsdatenträger für die installierte Version von Windows. Weitere Informationen finden Sie unter Erstellen von Installationsmedien für Windows.
2. Wählen Sie auf dem Bildschirm **Windows installieren** die Option **weiter** > **Reparatur Ihres Computers**aus.
3. Wählen Sie auf dem Bildschirm **System Wiederherstellungsoptionen** die Option **nächste** > **Eingabeaufforderung**aus.
4. Klicken Sie nach dem Start der Reparatur auf **Herunterfahren**, und aktivieren Sie dann Ihren PC, um festzustellen, ob Windows ordnungsgemäß booten kann.

Das Tool zum Starten der Reparatur generiert eine Protokolldatei, die Ihnen hilft, die Startprobleme und die vorgenommenen Reparaturen zu verstehen. Sie finden die Protokolldatei an folgendem Speicherort:

%windir%\System32\LogFiles\Srt\Srttrail.txt

Weitere Informationen finden Sie unter Stoppfehler oder der Computer reagiert nicht mehr, wenn Sie versuchen, Windows Vista oder Windows 7 zu starten .

Methode 2: Reparieren von Start Codes

Führen Sie zum Reparieren von Startcodes den folgenden Befehl aus:

```
BOOTREC /FIXMBR
```

Führen Sie zum Reparieren des Startsektors den folgenden Befehl aus:

```
BOOTREC /FIXBOOT
```

> **NOTE**
> Wenn **BOOTREC** zusammen mit **fixmbr** ausgeführt wird, wird nur der Masterstartcode überschrieben. Wenn sich die Beschädigung im MBR auf die Partitionstabelle auswirkt, kann das Problem durch Ausführen von **fixmbr** möglicherweise nicht behoben werden.

Methode 3: Beheben von BCD-Fehlern

Wenn BCD-Fehler auftreten, führen Sie die folgenden Schritte aus:

1. Suchen Sie nach allen installierten Systemen. Geben Sie zu diesem Zweck folgenden Befehl ein:

```
Bootrec /ScanOS
```

2. Starten Sie den Computer neu, um zu überprüfen, ob das Problem behoben ist.

3. Wenn das Problem nicht behoben ist, führen Sie den folgenden Befehl aus:

```
Bootrec /rebuildbcd
```

4. Möglicherweise erhalten Sie eine der folgenden Ausgänge:

```
Scanning all disks for Windows installations. Please wait, since this may take a while ...
Successfully scanned Windows installations. Total identified Windows installations: 0
The operation completed successfully.
```

```
Scanning all disks for Windows installations. Please wait, since this may take a while ...
Successfully scanned Windows installations. Total identified Windows installations: 1
D:\Windows
Add installation to boot list? Yes/No/All:
```

Wenn die Ausgabe die **Windows-Installation zeigt: 0**, führen Sie die folgenden Befehle aus:

```
bcdedit /export c:\bcdbackup

attrib c:\\boot\\bcd -r –s -h

ren c:\\boot\\bcd bcd.old

bootrec /rebuildbcd
```

Nachdem Sie den Befehl ausgeführt haben, wird die folgende Ausgabe angezeigt:

```
Scanning all disks for Windows installations. Please wait, since this may take a while ...
Successfully scanned Windows installations. Total identified Windows installations: 1
{D}:\Windows
Add installation to boot list? Yes/No/All: Y
```

1. Versuchen Sie, das System neu zu starten.

Methode 4: Ersetzen Sie einen anderen.

Wenn das Problem durch die Methoden 1, 2 und 3 nicht behoben werden kann, ersetzen Sie die Start-Datei von Laufwerk C in die reservierte Partition des Systems. Gehen Sie hierzu folgendermaßen vor:

1. Ändern Sie an einer Eingabeaufforderung das Verzeichnis in die reservierte Partition des Systems.

2. Führen Sie den Befehl **Attribute** aus, um die Datei einzublenden:

```
attrib -r -s -h
```

3. Führen Sie den gleichen **Attribut** Befehl auf dem Windows-Systemlaufwerk aus:

```
attrib -r -s -h
```

4. Benennen Sie die Datei "ein" als "ein":

```
ren c:\bootmgr bootmgr.old
```

5. Navigieren Sie zum Systemlaufwerk.
6. Kopieren Sie die Datei, und fügen Sie Sie dann in die reservierte Partition des Systems ein.
7. Starten Sie den Computer neu.

Methode 5: Wiederherstellen der System Struktur

Wenn Windows die Systemregistrierungsstruktur nicht in den Arbeitsspeicher laden kann, müssen Sie die Systemstruktur wiederherstellen. Verwenden Sie dazu die Windows-Wiederherstellungsumgebung, oder verwenden Sie Notfalldiskette (Notfalldiskette), um die Dateien aus dem C:\Windows\System32\config\RegBack in C:\Windows\System32\config. zu kopieren.

Wenn das Problem weiterhin besteht, möchten Sie möglicherweise die Systemstatussicherung an einem anderen Speicherort wiederherstellen und dann die zu ersetzenden Registrierungsstrukturen abrufen.

Kernel Phase

Wenn das System während der Kernel Phase hängen bleibt, treten mehrere Symptome auf, oder es werden mehrere Fehlermeldungen angezeigt. Dazu gehören, aber nicht nur die folgenden:

- Nach dem Begrüßungsbildschirm (Windows-Logo-Bildschirm) wird ein Stopp-Fehler angezeigt.
- Spezifischer Fehlercode wird angezeigt. Beispielsweise "0x00000C2", "0x0000007B", "Unzugängliches Startgerät" usw.
  - Erweiterte Problembehandlung für Stoppfehler 7B oder Inaccessible_Boot_Device
  - Erweiterte Problembehandlung für die Ereignis-ID 41 "das System wurde neu gestartet, ohne dass es zuerst sauber heruntergefahren wurde"
- Der Bildschirm bleibt auf dem Symbol "rotierendes Rad" (Rolling dots) "System busy" hängen.
- Hinter dem Begrüßungsbildschirm wird ein schwarzer Bildschirm angezeigt.

Um diese Probleme zu beheben, versuchen Sie die folgenden Wiederherstellungs Startoptionen nacheinander.

Szenario 1: versuchen Sie, den Computer im abgesicherten Modus oder letzte als funktionierend bekannte Konfiguration zu starten.

Versuchen Sie auf dem Bildschirm **Erweiterte Startoptionen** , den Computer im **abgesicherten Modus** oder im **abgesicherten Modus mit Netzwerk**zu starten. Wenn eine dieser Optionen funktioniert, verwenden Sie die Ereignisanzeige, um die Ursache des Startproblems zu ermitteln und zu diagnostizieren. Führen Sie die folgenden Schritte aus, um in den Ereignisprotokollen aufgezeichnete Ereignisse anzuzeigen:

1. Verwenden Sie eine der folgenden Methoden, um die Ereignisanzeige zu öffnen:
   - Klicken Sie auf **Start**, zeigen Sie auf **Verwaltung**, und klicken Sie dann auf **Ereignisanzeige**.
   - Starten Sie das Ereignisanzeige-Snap-in in der Microsoft Management Console (MMC).
2. Erweitern Sie in der Konsolenstruktur die Ereignisanzeige, und klicken Sie dann auf das Protokoll, das Sie anzeigen möchten. Klicken Sie beispielsweise auf **System Protokoll** oder **Anwendungsprotokoll**.
3. Doppelklicken Sie im Detailbereich auf das Ereignis, das Sie anzeigen möchten.
4. Klicken Sie im Menü **Bearbeiten** auf **Kopieren**, öffnen Sie ein neues Dokument in dem Programm, in dem Sie das Ereignis einfügen möchten (beispielsweise Microsoft Word), und klicken Sie dann auf **Einfügen**.
5. Verwenden Sie die nach-oben-oder nach-unten-Taste, um die Beschreibungder des vorhergehenden oder

nächsten Ereignisses zu Logistikkettenim.

Sauberen Start

Wenn Sie Probleme beheben möchten, die sich auf Dienste auswirken, führen Sie einen sauberen Neustart mithilfe der System Konfiguration (MSCONFIG) durch. Wählen Sie **selektiver Start** aus, um die Dienste einzeln zu testen, um zu ermitteln, welches Problem verursacht wird. Wenn Sie die Ursache nicht finden können, versuchen Sie, die Systemdienste einzubinden. In den meisten Fällen ist der problematische Dienst jedoch Drittanbieter.

Deaktivieren Sie alle fehlerhaften Dienste, und versuchen Sie, den Computer erneut zu starten, indem Sie **Normaler Start**auswählen.

Ausführliche Anweisungen finden Sie unter Ausführen eines sauberen Starts in Windows.

Wenn der Computer im Modus "Treibersignatur deaktivieren" gestartet wird, starten Sie den Computer unter "Treibersignatur Erzwingung deaktivieren", und führen Sie dann die im folgenden Artikel beschriebenen Schritte aus, um zu ermitteln, welche Treiber oder Dateien die Treibersignatur Erzwingung erfordern: Problem Behandlung beim Startproblem verursachte bymissing-Treibersignatur (x64)

> **NOTE**
>
> Wenn es sich bei dem Computer um einen Domänencontroller handelt, versuchen Sie es mit dem Verzeichnisdienste-Wiederherstellungsmodus.
>
> Diese Methode ist ein wichtiger Schritt, wenn Sie auf Abbruchfehler "0xC00002E1" oder "0xC00002E2" stoßen.

Beispiele

> **WARNING**
>
> Wenn Sie die Registrierung mithilfe des Registrierungs-Editors oder einer anderen Methode falsch ändern, kann dies zu schwerwiegenden Problemen führen. Für diese Probleme kann es erforderlich sein, dass Sie das Betriebssystem neu installieren. Microsoft kann nicht garantieren, dass diese Probleme gelöst werden können. Das Ändern der Registrierung erfolgt auf eigenes Risiko.

Fehlercode INACCESSIBLE_BOOT_DEVICE (Beenden von 0x7B)

Führen Sie die folgenden Schritte zum Filtern der Treiber aus, um diesen Abbruchfehler zu beheben:

1. Wechseln Sie zur Windows-Wiederherstellungsumgebung (WinRE), indem Sie eine ISO-Diskette des Systems in das Laufwerk einfügen. Die ISO sollte dieselbe Version von Windows oder eine neuere Version aufweisen.
2. Öffnen Sie die Registrierung.
3. Laden Sie die Systemstruktur, und nennen Sie Sie als "Test".
4. Überprüfen Sie unter dem folgenden Registrierungsunterschlüssel nach niedrigeren Filter-und oberen Filterelementen für nicht-Microsoft-Treiber:

   HKEY_LOCAL_MACHINE \system\controlset001\control\class
5. Klicken Sie für jeden von Ihnen gefundenen Drittanbietertreiber auf den oberen oder unteren Filter, und löschen Sie dann die Wertdaten.
6. Durchsuchen Sie die gesamte Registrierung nach ähnlichen Elementen. Als geeignetes Verfahren aus, und Entladen Sie dann die Registrierungsstruktur.
7. Starten Sie den Server im normalen Modus neu.

Weitere Schritte zur Problembehandlung finden Sie in den folgenden Artikeln:

- Erweiterte Problembehandlung für Stoppfehler 7B oder Inaccessible_Boot_Device

Wenn Sie Probleme beheben möchten, die nach der Installation von Windows-Updates auftreten, überprüfen Sie anhand der folgenden Schritte auf ausstehende Updates:

1. Öffnen Sie ein Eingabeaufforderungsfenster in WinRE.
2. Führen Sie den folgenden Befehl aus:

   ```
   DISM /image:C:\ /get-packages
   ```

3. Wenn es ausstehende Updates gibt, deinstallieren Sie Sie, indem Sie die folgenden Befehle ausführen:

   ```
   DISM /image:C:\ /remove-package /packagename: name of the package
   ```

   ```
   DISM /Image:C:\ /Cleanup-Image /RevertPendingActions
   ```

Versuchen Sie, den Computer zu starten.

Wenn der Computer nicht gestartet wird, führen Sie die folgenden Schritte aus:

1. Öffnen Sie ein Eingabeaufforderungsfenster in WinRE, und starten Sie einen Text-Editor wie Editor.
2. Navigieren Sie zum Systemlaufwerk, und suchen Sie nach windows\winsxs\pending.Xml.
3. Wenn die ausstehende XML-Datei gefunden wird, benennen Sie die Datei als "Ausstehend. Xml. old" um.
4. Öffnen Sie die Registrierung, und laden Sie dann die Komponentenstruktur in HKEY_LOCAL_MACHINE als Test.
5. Markieren Sie die geladene Teststruktur, und suchen Sie dann nach dem **PendingXmlIdentifier** -Wert.
6. Wenn der Wert **PendingXmlIdentifier** vorhanden ist, löschen Sie den Wert.
7. Entladen Sie die Teststruktur.
8. Laden Sie die Systemstruktur, und nennen Sie Sie "Test".
9. Navigieren Sie zum folgenden Unterschlüssel:

   HKEY_LOCAL_MACHINE \system\controlset001\services\trustedinstaller

10. Ändern des **Start** Werts von **1** in **4**
11. Entladen Sie die Struktur.
12. Versuchen Sie, den Computer zu starten.

Wenn der Abbruchfehler verspätet beim Startvorgang auftritt oder wenn der Abbruchfehler weiterhin generiert wird, können Sie ein Speicherabbild aufzeichnen. Ein gutes Speicherabbild kann helfen, die Ursache für den Abbruchfehler zu ermitteln. Ausführliche Informationen finden Sie in den folgenden Artikeln:

- Generieren eines Kernels oder eines vollständigen Absturzabbilds

Weitere Informationen zu Seitendatei Problemen in Windows 10 oder Windows Server 2016 finden Sie in den folgenden Themen:

- Einführung in Seiten Dateien

Weitere Informationen zu Abbruchfehlern finden Sie im folgenden Knowledge Base-Artikel:

- Erweiterte Problembehandlung für Stoppfehler und Bluescreens

Wenn in der Dumpdatei ein Fehler angezeigt wird, der sich auf einen Treiber bezieht (Wenn beispielsweise windows\system32\drivers\stcvsm.sys fehlt oder beschädigt ist), folgen Sie den folgenden Richtlinien:

- Überprüfen Sie die Funktionalität, die vom Treiber bereitgestellt wird. Wenn es sich bei dem Treiber um einen Drittanbieter-Start Treiber handelt, stellen Sie sicher, dass Sie wissen, was er tut.
- Wenn der Treiber nicht wichtig ist und keine Abhängigkeiten aufweist, laden Sie die Systemstruktur, und deaktivieren Sie dann den Treiber.
- Wenn der Abbruchfehler die System Dateibeschädigung angibt, führen Sie die Systemdateiprüfung im Offlinemodus aus.
  - Öffnen Sie dazu WinRE, öffnen Sie eine Eingabeaufforderung, und führen Sie dann den folgenden Befehl aus:

    ```
    SFC /Scannow /OffBootDir=C:\ /OffWinDir=E:\Windows
    ```

    Weitere Informationen finden Sie unter Verwenden von System File Checker (SFC) zum Beheben von Problemen
  - Wenn die Datenträgerbeschädigung vorhanden ist, führen Sie den Befehl Datenträger überprüfen aus:

    ```
    chkdsk /f /r
    ```
  - Wenn der Stopp-Fehler auf allgemeine Registrierungsbeschädigung hindeutet, oder wenn Sie der Meinung sind, dass neue Treiber oder Dienste installiert wurden, führen Sie die folgenden Schritte aus:

    1. Starten Sie WinRE, und öffnen Sie ein Eingabeaufforderungsfenster.
    2. Starten Sie einen Text-Editor wie Editor.
    3. Navigieren zu C:\Windows\System32\Config.
    4. Benennen Sie die alle fünf Hives um, indem Sie ". old" an den Namen anfügen.
    5. Kopieren Sie alle Hives aus dem Ordner "Regback", fügen Sie Sie in den Ordner "config" ein, und versuchen Sie dann, den Computer im normalen Modus zu starten.

Erweiterte Problembehandlung für Windows-basierte Computer, die einfrieren

06.03.2020 • 11 minutes to read

In diesem Artikel wird beschrieben, wie Probleme mit dem fixieren auf Windows-basierten Computern und Servern behoben werden können. Außerdem werden Methoden zum Sammeln von Daten bereitgestellt, die Administratoren oder Softwareentwicklern dabei helfen, diese Probleme zu diagnostizieren, zu identifizieren und zu beheben.

> **NOTE**
>
> Die Produkte von Drittanbietern, die in diesem Artikel behandelt werden, werden von Unternehmen hergestellt, die unabhängig von Microsoft sind. Microsoft übernimmt keine Garantie, weder konkludent noch anderweitig, für die Leistung oder Zuverlässigkeit dieser Produkte.

Ermitteln des Problems

- Welcher Computer friert? (Beispiel: der betroffene Computer ist ein physischer Server, virtueller Server usw.)
- Welcher Vorgang wurde ausgeführt, als das Einfrieren erfolgte? (Beispiel: dieses Problem tritt auf, wenn Sie die GUI Herunterfahren, einen oder mehrere Vorgänge ausführen usw.)
- Wie oft treten die Fehler auf? (Beispiel: dieses Problem tritt jeden Abend um 19.00 Uhr auf, jeden Tag um 7.00 Uhr usw.)
- Auf wie vielen Computern tritt dies auf? (Beispiel: alle Computer, nur einen Computer, 10 Computer usw.)

Behandeln von Problemen mit dem fixieren

Wenn Sie Probleme mit dem fixieren beheben möchten, überprüfen Sie den aktuellen Status Ihres Computers, und führen Sie eine der folgenden Methoden aus.

Für den Computer, der noch in einem fixierten Zustand ausgeführt wird

Wenn der physikalische Computer oder der virtuelle Computer weiterhin einfriert, verwenden Sie eine oder mehrere der folgenden Methoden für die Problembehandlung:

- Versuchen Sie, auf den Computer über Remote Desktop, Citrix usw. zuzugreifen.
- Verwenden Sie das Domänenkonto oder lokales Administratorkonto, um sich auf dem Computer mithilfe einer der Remotefunktionen für den Zugriff auf physische Konsolen zu anmelden, wie etwa Dell Remote Access Card (DRAC), HP Integrated Lights-Out (iLo) oder IBM Remote Supervisor-Adapter (RSA).
- Testen Sie Ping auf den Computer. Das Herunterfallen von Paketen und eine starke Netzwerklatenz können beobachtet werden.
- Zugriff auf administrative Freigaben (\ \ \ *Servername*\c $).
- Drücken Sie STRG + ALT + ENTF, und überprüfen Sie die Antwort.
- Versuchen Sie, Remoteverwaltungstools wie Computer Verwaltung, Remote Server-Manager und wmimgmt.msc zu verwenden.

Für den Computer, der nicht mehr fixiert ist

Verwenden Sie eine oder mehrere der folgenden Methoden für die Problembehandlung, wenn der physikalische Computer oder der virtuelle Computer eingefroren ist, aber jetzt in einem guten Zustand ausgeführt wird.

Für einen physikalischen Computer

- Überprüfen Sie die System-und Anwendungsprotokolle von dem Computer, auf dem das Problem auftritt. Überprüfen Sie die Ereignisprotokolle auf die relevante Ereignis-ID:
  - Anwendungsereignisprotokoll: Anwendungsfehler (schlägt Absturz oder relevanter System Prozess vor)
  - System Ereignisprotokolle, Fehlerereignis-IDs des Dienststeuerungs-Managers für wichtige Systemdienste
  - Fehlerereignis-IDs 2019/2020 mit Quelle SRV/Server
- Generieren Sie einen System Diagnosebericht, indem Sie den Befehl Perfmon/Report ausführen.

Für einen virtuellen Computer

- Überprüfen Sie die System-und Anwendungsprotokolle von dem Computer, auf dem das Problem auftritt.
- Generieren Sie einen System Diagnosebericht, indem Sie den Befehl Perfmon/Report ausführen.
- Überprüfen Sie den Verlauf in den Tools für die virtuelle Verwaltungsüberwachung.

Sammeln von Daten für das Fixieren von Problemen

Wenn Sie Daten für einen Server Einfrieren sammeln möchten, überprüfen Sie die folgende Tabelle, und verwenden Sie eine oder mehrere der vorgeschlagenen Methoden.

COMPUTERTYP UND-ZUSTAND	DATEN SAMMLUNGSMETHODE
Ein physischer Computer, der in einem fixierten Zustand ausgeführt wird	Verwenden Sie eine Speicherabbilddatei, um Daten zu sammeln. Oder verwenden Sie Methode 2, 3 oder 4. Diese Methoden sind weiter unten in diesem Abschnitt aufgeführt.
Ein nicht mehr fixierter physischer Computer	Verwenden Sie Methode 1, 2, 3 oder 4. Diese Methoden sind weiter unten in diesem Abschnitt aufgeführt. Und verwenden Sie den Pool Monitor, um Daten zu sammeln.
Ein virtueller Computer, der in einem fixierten Zustand ausgeführt wird	Hyper-V oder VMware: verwenden Sie eine Speicherabbilddatei zum Sammeln von Daten für den virtuellen Computer, der in einem fixierten Zustand ausgeführtwird. XenServer: Verwenden Sie die Methode 1, 2, 3 oder 4. Diese Methoden sind weiter unten in diesem Abschnitt aufgeführt.
Eine virtuelle Maschine, die nicht mehr fixiert ist	Verwenden Sie Methode 1, 2, 3 oder 4. Diese Methoden sind weiter unten in diesem Abschnitt aufgeführt.

Methode 1: Speicherabbild

> **NOTE**
> Führen Sie die Schritte in diesem Abschnitt sorgfältig aus. Wird die Registrierung falsch angepasst, können schwerwiegende Probleme auftreten. Bevor Sie ihn ändern, Sichern Sie die Registrierung für die Wiederherstellung , falls Probleme auftreten.

Eine vollständige Speicherabbilddatei zeichnet alle Inhalte des Systemspeichers auf, wenn der Computer unerwartet beendet wird. Eine vollständige Speicherabbilddatei kann Daten aus Prozessen enthalten, die beim Sammeln der Speicherabbilddatei ausgeführt wurden.

Wenn der Computer nicht mehr fixiert ist und jetzt in einem guten Zustand ausgeführt wird, führen Sie die folgenden Schritte aus, um das Speicherabbild zu aktivieren, damit Sie Speicherabbilder sammeln können, wenn das Problem beim fixieren erneut auftritt. Wenn der virtuelle Computer weiterhin in einem fixierten Zustand ausgeführt wird, führen Sie die folgenden Schritte aus, um das Speicherabbild zu aktivieren und zu sammeln.

> **NOTE**
> Wenn Sie über ein auf dem Computer aktiviertes Neustart Feature verfügen, wie beispielsweise das Feature Automatischer System Neustart (ASR) in Compaq-Computern, deaktivieren Sie es. Diese Einstellung ist in der Regel im BIOS zu finden. Wenn dieses Feature aktiviert ist und das BIOS keinen Heartbeat vom Betriebssystem erkennt, wird der Computer neu gestartet. Der Neustart kann den dumpprozess unterbrechen.

1. Stellen Sie sicher, dass der Computer eingerichtet ist, um eine vollständige Speicherabbilddatei zu erhalten. Gehen Sie hierzu folgendermaßen vor:

   a. Wechseln Sie zu **Ausführen** , `Sysdm.cpl` und geben Sie Sie ein, und drücken Sie dann die EINGABETASTE.

   b. Wählen Sie in **System Eigenschaften**auf der Registerkarte **erweitert** die Option **Leistungs** > **Einstellungen** > **erweitert**aus, und überprüfen oder ändern Sie den virtuellen Speicher, indem Sie auf **ändern**klicken.

   c. Wechseln Sie zurück zu den**erweiterten** > **Einstellungen** für **System Eigenschaften** > in **Start und Wiederherstellung**.

   d. Wählen Sie im Abschnitt **Debuginformationen schreiben** die Option **vollständiges Speicherabbild**aus.

   > **NOTE**
   > Für Windows-Versionen, die älter als Windows 8 oder Windows Server 2012 sind, steht der vollständige Speicherabbildtyp nicht in der GUI zur Verfügung. Sie müssen Sie im Registrierungs-Editor ändern. Ändern Sie dazu den Wert des folgenden **CrashDumpEnabled** -Registrierungseintrags in **1** (REG_DWORD): **HKEY_LOCAL_MACHINE \system\currentcontrolset\control\crashcontrol\crashdumpenabled**

   e. Wählen Sie **vorhandene Datei überschreiben**aus.

   f. Stellen Sie sicher, dass auf dem Systemlaufwerk eine Auslagerungsdatei (pagefile. sys) vorhanden ist und mindestens 100 Megabyte (MB) über dem installierten RAM (Initial und maximale Größe) sind.

      Darüber hinaus können Sie die Problemumgehung für Speicherplatzeinschränkungen auf dem Systemlaufwerk in Windows Server 2008verwenden.

   g. Stellen Sie sicher, dass auf dem Systemlaufwerk mehr verfügbarer Speicherplatz als physischer Arbeitsspeicher verfügbar ist.

2. Aktivieren Sie den Registrierungswert CrashOnCtrlScroll erstellen, damit das System eine Speicherabbilddatei mithilfe der Tastatur generieren kann. Gehen Sie hierzu folgendermaßen vor:

   a. Wechseln Sie zum Registrierungs-Editor, und suchen Sie dann die folgenden Registrierungsschlüssel:

      - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters`
      - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kbdhid\Parameters`

   b. Erstellen Sie den folgenden CrashOnCtrlScroll erstellen-Registrierungseintrag in den beiden Registrierungsschlüsseln:

      - **Name des Werts**: `CrashOnCtrlScroll`
      - **Datentyp**: `REG_DWORD`
      - **Wert**: `1`

   c. Beenden Sie den Registrierungs-Editor.

d. Starten Sie den Computer neu.

3. Auf einigen physikalischen Computern können Sie eine nicht vernetzte Unterbrechung (NMI) vom webschnittstelles Feature (wie DRAC, iLo und RSA) generieren. Standardmäßig wird diese Einstellung jedoch das System beenden, ohne ein Speicherabbild zu erstellen.

   Damit das Betriebssystem eine Speicherabbilddatei bei einer NMI-Unterbrechung generieren kann, legen Sie den Wert des Registrierungseintrags NMICrashDump `1` auf (REG_DWORD). Starten Sie den Computer dann neu, um diese Änderung anzuwenden.

   > **NOTE**
   > Dies gilt nur für Windows 7, Windows Server 2008 R2 und frühere Versionen von Windows. Für Windows 8 Windows Server 2012 und höhere Versionen von Windows ist der NMICrashDump-Registrierungsschlüssel nicht mehr erforderlich, und eine NMI-Unterbrechung führt zu einem Abbruchfehler, der auf eine Speicherabbild Datensammlung folgt.

4. Wenn der Computer das Problem aufweist, halten Sie die Rechte **STRG** -Taste gedrückt, und drücken Sie zwei Mal die **Scroll-Sperr** Taste, um eine Speicherabbilddatei zu generieren.

   > **NOTE**
   > Standardmäßig befindet sich die Speicherabbilddatei im folgenden Pfad:
   > %SystemRoot%\Memory. DMP

Methode 2: Daten Plausibilitätsprüfung

Verwenden Sie das Dienstprogramm Dump-Überprüfung (Dumpchk. exe), um eine Speicherabbilddatei zu lesen oder zu überprüfen, ob die Datei ordnungsgemäß erstellt wurde. Sie können das Tool Microsoft DumpChk (Crash Dump File Checker) verwenden, um sicherzustellen, dass die Speicherabbilddateien nicht beschädigt oder ungültig sind.

- Verwenden von DumpChk
- DumpCheck herunterladen

Erfahren Sie, wie Sie Dumpchk. exe verwenden, um Ihre Dumpdateien zu überprüfen:

Methode 3: System Monitor

Sie können den Windows-System Monitor verwenden, um zu untersuchen, wie sich die ausgeführten Programme auf die Leistung Ihres Computers auswirken, sowohl in Echtzeit als auch durch das Sammeln von Protokolldaten für die spätere Analyse. Führen Sie die folgenden Befehle an einer Eingabeaufforderung als Administrator aus, um Leistungsindikator-und Ereignisablaufverfolgungsprotokoll Sammlungen auf lokalen und Remotesystemen zu erstellen:

```
Logman create counter LOGNAME_Long -u DOMAIN\USERNAME * -f bincirc -v mmddhhmm -max 500 -c
"\\COMPUTERNAME\LogicalDisk(*)\*" "\\COMPUTERNAME\Memory\*" "\\COMPUTERNAME\Network Interface(*)\*"
"\\COMPUTERNAME\Paging File(*)\*" "\\COMPUTERNAME\PhysicalDisk(*)\*" "\\COMPUTERNAME\Process(*)\*"
"\\COMPUTERNAME\Redirector\*" "\\COMPUTERNAME\Server\*" "\\COMPUTERNAME\System\*" "\\COMPUTERNAME\Terminal
Services\*" "\\COMPUTERNAME\Processor(*)\*" "\\COMPUTERNAME\Cache\*" -si 00:05:00
```

```
Logman create counter LOGNAME_Short -u DOMAIN\USERNAME * -f bincirc -v mmddhhmm -max 500 -c
"\\COMPUTERNAME\LogicalDisk(*)\*" "\\COMPUTERNAME\Memory\*" "\\COMPUTERNAME\Network Interface(*)\*"
"\\COMPUTERNAME\Paging File(*)\*" "\\COMPUTERNAME\PhysicalDisk(*)\*" "\\COMPUTERNAME\Process(*)\*"
"\\COMPUTERNAME\Redirector\*" "\\COMPUTERNAME\Server\*" "\\COMPUTERNAME\System\*" "\\COMPUTERNAME\Terminal
Services\*" "\\COMPUTERNAME\Processor(*)\*" "\\COMPUTERNAME\Cache\*" -si 00:00:10
```

Anschließend können Sie das Protokoll starten oder beenden, indem Sie die folgenden Befehle ausführen:

```
logman start LOGNAME_Long / LOGNAME_Short
logman stop LOGNAME_Long / LOGNAME_Short
```

Das System Monitor Protokoll befindet sich im Pfad: C:\PERFLOGS

Methode 4: Microsoft-Support Diagnose

1. Geben Sie im Suchfeld des Microsoft Support Diagnostics Self-Help-PortalsWindows-Leistungsdiagnostik ein.
2. Wählen Sie in den Suchergebnissen **Windows-Leistungsdiagnostik**aus, und klicken Sie dann auf **Erstellen**.
3. Führen Sie die Schritte der Diagnose aus.

Weitere Methoden zum Sammeln von Daten

Verwenden des Speicherabbilds zum Sammeln von Daten für den physikalischen Computer, der in einem fixierten Zustand ausgeführt wird

> **WARNING**
> Führen Sie die Schritte in diesem Abschnitt sorgfältig aus. Wird die Registrierung falsch angepasst, können schwerwiegende Probleme auftreten. Bevor Sie ihn ändern, Sichern Sie die Registrierung für die Wiederherstellung , falls Probleme auftreten.

Wenn der physikalische Computer weiterhin in einem fixierten Zustand ausgeführt wird, führen Sie die folgenden Schritte aus, um das Speicherabbild zu aktivieren und zu sammeln:

1. Stellen Sie sicher, dass der Computer eingerichtet ist, um eine vollständige Speicherabbilddatei abzurufen, und dass Sie über das Netzwerk darauf zugreifen können. Gehen Sie hierzu folgendermaßen vor:

   > **NOTE**
   > Wenn es nicht möglich ist, auf den betroffenen Computer über das Netzwerk zuzugreifen, versuchen Sie, eine Speicherabbilddatei über die NMI-Unterbrechung zu generieren. Das Ergebnis der Aktion kann keine Speicherabbilddatei sammeln, wenn einige der folgenden Einstellungen nicht qualifiziert sind.

   a. Versuchen Sie, auf den Desktop des Computers zuzugreifen.

   > **NOTE**
   > Wenn der Zugriff auf das Betriebssystem nicht möglich ist, versuchen Sie, den Registrierungs-Editor auf dem Computer remote zuzugreifen, um den Typ der Speicherabbilddatei und die Auslagerungsdatei zu überprüfen, mit der der Computer derzeit konfiguriert ist.

   b. Wechseln Sie von einem Remotecomputer, der sich vorzugsweise im gleichen Netzwerk und Subnetz befindet, zum **Registrierungs-Editor** > **Connect Network Registry**. Stellen Sie dann eine Verbindung mit dem betreffenden Computer her, und überprüfen Sie die folgenden Einstellungen:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnabled`

  Stellen Sie sicher, dass der Registrierungseintrag `1` "CrashDumpEnabled" lautet.

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\NMICrashDump`

  Wenn der Registrierungseintrag "NMICrashDump" auf einigen physischen Servern vorhanden und sein Wert `1` ist, können Sie die NMI von den Remoteverwaltungsfunktionen (wie DRAC, iLo und RSA) nutzen.

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PagingFiles and ExistingPageFiles`

  Wenn der Wert des Registrierungseintrags " **Pagefile** " System verwaltet ist, wird die Größe nicht in der Registrierung widergespiegelt (Beispielwert:?: \ Pagefile. sys).

  Wenn die Auslagerungsdatei angepasst wird, wird die Größe in der Registrierung widergespiegelt, wie "?: \ Pagefile. sys 1024 1124 ' wobei 1024 die ursprüngliche Größe und 1124 die maximale Größe ist.

  > **NOTE**
  > Wenn die Größe nicht in der Registrierung widergespiegelt wird, versuchen Sie, auf eine administrative Freigabe zuzugreifen, in der sich die Auslagerungsdatei befindet (beispielsweise \ \ \ *Servername*\c $).

c. Stellen Sie sicher, dass auf dem Systemlaufwerk des Computers eine Auslagerungsdatei (pagefile. sys) vorhanden ist, die mindestens 100 MB über dem installierten Arbeitsspeicher beträgt.

d. Stellen Sie sicher, dass auf den Festplatten des Computers mehr freier Speicherplatz vorhanden ist, als physischer Arbeitsspeicher vorhanden ist.

2. Aktivieren Sie den Registrierungswert **CrashOnCtrlScroll erstellen** auf dem Computer, damit das System eine Speicherabbilddatei mithilfe der Tastatur generieren kann. Gehen Sie hierzu folgendermaßen vor:

   a. Wechseln Sie von einem Remotecomputer, der sich vorzugsweise im gleichen Netzwerk und Subnetz befindet, zum Registrierungs-Editor \ > Netzwerkregistrierung verbinden. Stellen Sie eine Verbindung mit dem betreffenden Computer her, und suchen Sie die folgenden Registrierungsschlüssel:

   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters`
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kbdhid\Parameters`

   b. Erstellen Sie den folgenden CrashOnCtrlScroll erstellen-Registrierungseintrag in den beiden Registrierungsschlüsseln:

   Name des Werts: `CrashOnCtrlScroll`
   Datentyp: `REG_DWORD`
   Wert: `1`

   c. Beenden Sie den Registrierungs-Editor.

   d. Starten Sie den Computer neu.

3. Wenn der Computer das Problem aufweist, halten Sie die Rechte **STRG** -Taste gedrückt, und drücken Sie zwei Mal die **Scroll-Sperr** Taste, um einen Speicherauszug zu generieren.

> **NOTE**
> Standardmäßig befindet sich die Speicherabbilddatei im Pfad:%SystemRoot%\Memory. DMP

Verwenden des Pool Monitors zum Sammeln von Daten für den physikalischen Computer, der nicht mehr fixiert ist

Der Pool Monitor zeigt die Anzahl der Zuweisungen und die ausstehenden Bytes der Zuteilung nach Pooltyp und die Kategorie an, die an ExAllocatePoolWithTag-Aufrufe übergeben wird.

Erfahren Sie, wie Sie den Pool Monitor verwenden und wie Sie die Daten zur Problembehandlung von Pool Lecks verwendenkönnen.

Verwenden des Speicherabbilds zum Sammeln von Daten für den virtuellen Computer, der in einem fixierten Zustand ausgeführt wird

Verwenden Sie eine der folgenden Methoden für die Anwendung, auf der der virtuelle Computer ausgeführt wird.

Microsoft Hyper-V

Wenn auf dem virtuellen Computer Windows 8, Windows Server 2012 oder eine neuere Version von Windows unter Microsoft Hyper-V Server 2012 ausgeführt wird, können Sie das integrierte NMI-Feature über ein Debug-VM- Cmdlet verwenden, um ein Speicherabbild zu Debuggen und abzurufen.

Führen Sie das folgende Cmdlet in Windows PowerShell aus, um die virtuellen Computer unter Hyper-V zu Debuggen:

```
Debug-VM -Name "VM Name" -InjectNonMaskableInterrupt -ComputerName Hostname
```

> **NOTE**
> Diese Methode ist nur für Windows 8, Windows Server 2012 und höhere Versionen von virtuellen Windows-Computern anwendbar. Informationen zu früheren Versionen von Windows finden Sie unter Methoden 1 bis 4, die weiter oben in diesem Abschnitt beschrieben werden.

VMware

Sie können VMware-Schnappschüsse verwenden oder den Zustand suspendieren und eine Speicherabbilddatei extrahieren, die einer vollständigen Speicherabbilddatei entspricht. Mithilfe von Checkpoint to Core Tool (vmss2core)können Sie sowohl Suspend (. vmss)-und Snapshot-Zustands Dateien (Vmsn) in eine Speicherabbilddatei konvertieren und dann die Datei mithilfe der standardmäßigen Windows-Debugging-Tools analysieren.

Citrix XenServer

Der Speicherabbild Vorgang erfolgt durch Drücken der Tastenkombination Strg + Scroll Lock + Scroll Lock, die in Methode 1 und auf der Citrix-Websitebeschrieben wird.

Speicherplatzeinschränkungen auf dem Systemlaufwerk in Windows Server 2008

Unter Windows Server 2008 haben Sie möglicherweise nicht genügend freien Speicherplatz, um eine vollständige Speicherabbilddatei auf dem Systemdatenträger zu generieren. Es gibt einen Hotfix , der die Datensammlung ermöglicht, auch wenn nicht genügend Speicherplatz auf dem Systemlaufwerk vorhanden ist, um die Speicherabbilddatei zu speichern.

Darüber hinaus gibt es unter Windows Server 2008 Service Pack (SP2) eine zweite Option, wenn auf dem Systemlaufwerk nicht genügend Speicherplatz zur Verfügung steht. Sie können nämlich den Registrierungseintrag

DedicatedDumpFile verwenden. Informationen zur Verwendung des Registrierungseintrags finden Sie unter neues Verhalten in Windows Vista und Windows Server 2008.

Weitere Informationen finden Sie unter so wird es gemacht: Verwenden des Registrierungswerts "DedicatedDumpFile", um die Speicherplatzeinschränkungen auf dem Systemlaufwerk zu überwinden.

Erweiterte Problembehandlung für Stoppfehler und Bluescreens

22.02.2020 • 19 minutes to read

NOTE

Wenn Sie kein Support-Mitarbeiter oder IT-Experte sind, finden Sie weitere hilfreiche Informationen zu Abbruchfehlern ("Blue Screen")-Meldungen unter Beheben von Bluescreen-Fehlern.

Was sind die Ursachen für Abbruchfehler?

Ein Stopp-Fehler wird als blauer Bildschirm angezeigt, der den Namen des fehlerhaften Treibers enthält, wie beispielsweise die folgenden Beispieltreiber:

- `atikmpag.sys`
- `igdkmd64.sys`
- `nvlddmkm.sys`

Es gibt keine einfache Erläuterung für die Ursache von Abbruchfehlern (auch bekannt als Bluescreen-Fehler oder Fehler Prüfungsfehler). Viele verschiedene Faktoren können einbezogen werden. Verschiedene Studien deuten jedoch darauf hin, dass Abbruchfehler in der Regel nicht von Microsoft Windows-Komponenten verursacht werden. Stattdessen beziehen sich diese Fehler im Allgemeinen auf fehlerhafte Hardwaretreiber oder Treiber, die von Software von Drittanbietern installiert werden. Dazu gehören Videokarten, Drahtlosnetzwerkkarten, Sicherheitsprogramme usw.

Unsere Analyse der Ursachen von Abstürzen gibt Folgendes an:

- 70 Prozent werden durch Treibercode von Drittanbietern verursacht
- 10 Prozent werden durch Hardwareprobleme verursacht
- 5 Prozent werden durch Microsoft-Code verursacht
- 15 Prozent haben unbekannte Ursachen (weil der Arbeitsspeicher zu fehlerhaft ist, um analysiert zu werden).

Allgemeine Schritte zur Problembehandlung

Führen Sie die folgenden allgemeinen Schritte aus, um Fehlermeldungen in Abbruch zu beheben:

1. Überprüfen Sie den STOPP-Fehlercode, den Sie in den Ereignisprotokollen finden. Suchen Sie online nach den spezifischen Stoppfehler Codes, um festzustellen, ob es bekannte Probleme, Lösungen oder Problemumgehungen für das Problem gibt.
2. Als bewährte Methode empfehlen wir, dass Sie die folgenden Schritte ausführen:

   a. Stellen Sie sicher, dass Sie die neuesten Updates für Windows-Updates, kumulative Updates und Rollups installieren. Wenn Sie den Updatestatus überprüfen möchten, lesen Sie den entsprechenden Updateverlauf für Ihr System:

   - Windows10, Version1809
   - Windows10, Version1803
   - Windows10, Version 1709
   - Windows10, Version1703

- Windows Server 2016 und Windows 10, Version 1607
- Windows10, Version1511
- Windows Server 2012 R2 und Windows 8.1
- Windows Server 2008 R2 und Windows 7 SP1

b. Stellen Sie sicher, dass das BIOS und die Firmware auf dem neuesten Stand sind.

c. Führen Sie relevante Hardware-und Speichertests aus.

3. Führen Sie das Windows-Diagnosepaket " Machine memory dump Collector " aus. Dieses Diagnosetool wird verwendet, um Speicherabbilddateien des Computers zu erfassen und auf bekannte Lösungen zu überprüfen.

4. Führen Sie den Microsoft Safety Scanner oder ein anderes virenerkennungsprogramm aus, das die Überprüfung des Master-Boot-Eintrags für Infektionen umfasst.

5. Stellen Sie sicher, dass genügend freier Speicherplatz auf der Festplatte vorhanden ist. Die genaue Anforderung ist unterschiedlich, aber wir empfehlen 10 – 15 Prozent freien Speicherplatz.

6. Wenden Sie sich an den jeweiligen Hardware-oder Softwarehersteller, um die Treiber und Anwendungen in den folgenden Szenarien zu aktualisieren:

   - Die Fehlermeldung weist darauf hin, dass ein bestimmter Treiber das Problem verursacht.
   - Es wird ein Hinweis auf einen Dienst angezeigt, der gestartet oder beendet wird, bevor der Absturz aufgetreten ist. Ermitteln Sie in dieser Situation, ob das Dienstverhalten für alle Instanzen des Absturzes konsistent ist.
   - Sie haben Software-oder Hardwareänderungen vorgenommen.

   > **NOTE**
   >
   > Wenn für einen bestimmten Hersteller keine Updates verfügbar sind, wird empfohlen, den zugehörigen Dienst zu deaktivieren.
   >
   > Informationen dazu finden Sie unter so wird es gemacht: Ausführen eines sauberen Starts in Windows
   >
   > Sie können einen Treiber deaktivieren, indem Sie die Schritte unter vorübergehende Deaktivierung des Kernelmodus-Filtertreibers in Windowsausführen.
   >
   > Möglicherweise möchten Sie auch die Option zum Zurücksetzen von Änderungen oder zum Wiederherstellen des letzten bekannten Arbeits Zustands in Frage stellen. Weitere Informationen finden Sie unter Zurücksetzen eines Gerätetreibers auf eine vorherige Version.

Speicherabbild Sammlung

Führen Sie die folgenden Schritte aus, um das System für Speicherabbilddateien zu konfigurieren:

1. DumpConfigurator-Tool herunterladen.
2. Extrahieren Sie die ZIP-Datei, und navigieren Sie zum Ordner " **Quell Code** ".
3. Führen Sie das Tool DumpConfigurator. hta aus, und wählen Sie dann **diese HTA erweitern**aus.
4. Wählen Sie **Auto config Kernel**aus.
5. Starten Sie den Computer neu, damit die Einstellung wirksam wird.
6. Beenden und deaktivieren Sie automatische System Neustart Dienste (ASR), um zu verhindern, dass Dumpdateien geschrieben werden.
7. Wenn der Server virtualisiert ist, deaktivieren Sie den automatischen Neustart, nachdem die Speicherabbilddatei erstellt wurde. Auf diese Weise können Sie eine Momentaufnahme des Serverzustands aufnehmen und auch dann, wenn das Problem erneut auftritt.

Die Speicherabbilddatei wird an den folgenden Speicherorten gespeichert:

DUMP-DATEITYP	PFAD
(keine)	%SystemRoot%\Memory. DMP (inaktiv oder abgeblendet)
Kleine Speicherabbilddatei (256 KB)	%SystemRoot%\Minidump
Kernel-Speicherabbilddatei	%SystemRoot%\Memory. DMP
Vollständige Speicherabbilddatei	%SystemRoot%\Memory. DMP
Automatische Speicherabbilddatei	%SystemRoot%\Memory. DMP
Aktive Speicherabbilddatei	%SystemRoot%\Memory. DMP

Sie können das Tool Microsoft DumpChk (Crash Dump File Checker) verwenden, um sicherzustellen, dass die Speicherabbilddateien nicht beschädigt oder ungültig sind. Weitere Informationen finden Sie im folgenden Video:

Weitere Informationen zur Verwendung von Dumpchk. exe zum Überprüfen Ihrer Dumpdateien:

- Verwenden von DumpChk
- DumpCheck herunterladen

Einstellungen für Auslagerungsdatei

- Einführung einer Auslagerungsdatei im lang Zeitdienst Kanal und halbjährlicher Kanal von Windows
- Bestimmen der geeigneten Auslagerungsdateigröße für 64-Bit-Versionen von Windows
- Erstellen eines Kernels oder einer vollständigen Speicherabbilddatei in Windows Server 2008 und Windows Server 2008 R2

Speicherabbild Analyse

Die Ursache für den Absturz zu finden, ist möglicherweise nicht einfach. Hardware Probleme sind besonders schwer zu diagnostizieren, da Sie zu unregelmäßigen und unvorhersehbaren Verhaltensweisen führen können, die sich in verschiedenen Symptomen manifestieren können.

Wenn ein Abbruchfehler auftritt, sollten Sie zunächst die problematischen Komponenten isolieren und dann versuchen, den Abbruchfehler erneut auszulösen. Wenn Sie das Problem replizieren können, können Sie die Ursache in der Regel ermitteln.

Sie können die Tools wie Windows Software Development Kit (SDK) und Symbole verwenden, um Dump-Protokolle zu diagnostizieren. Im nächsten Abschnitt wird die Verwendung dieses Tools erläutert.

Erweiterte Schritte zur Problembehandlung

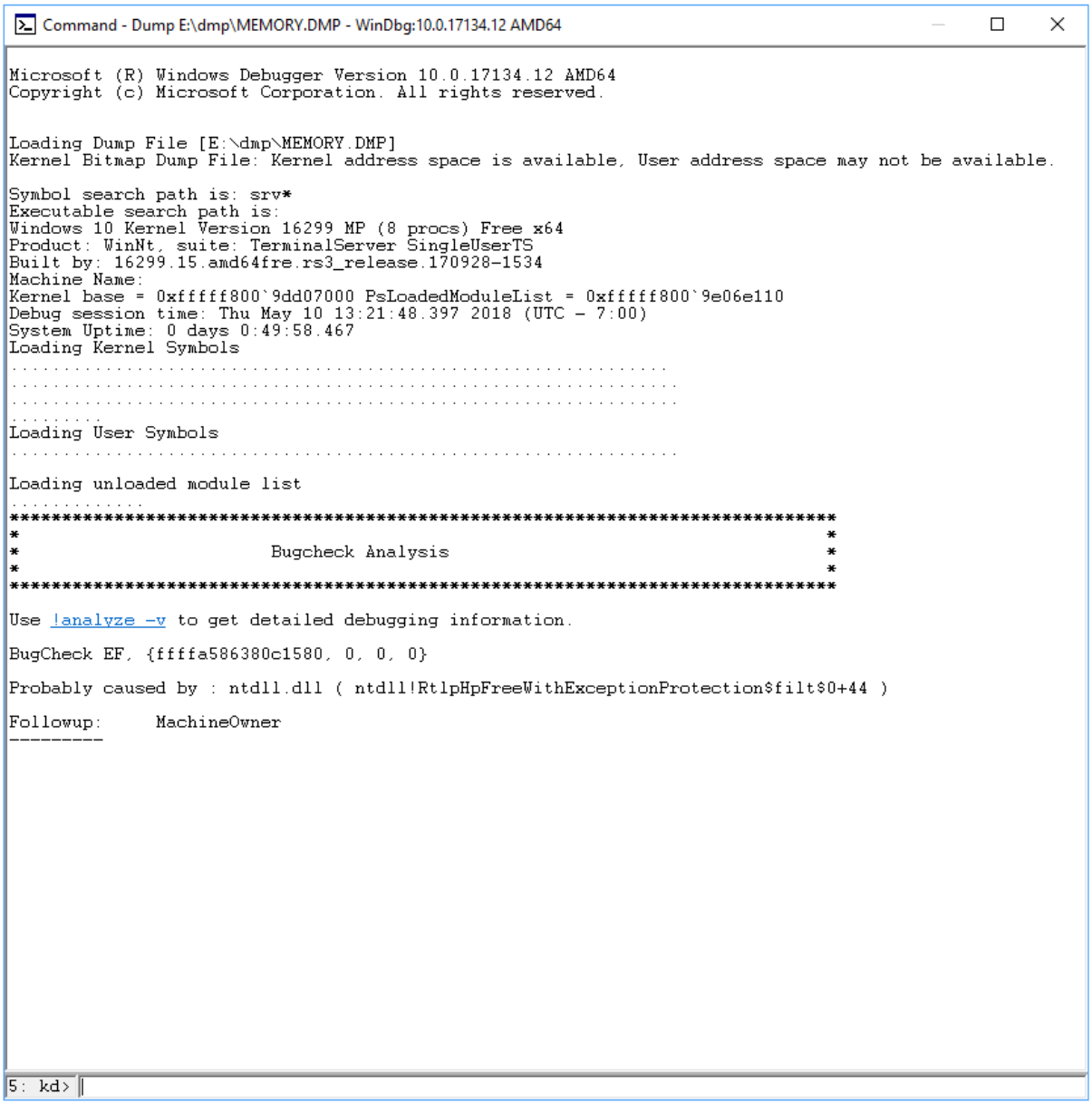
> **NOTE**
>
> Die erweiterte Problembehandlung für Absturzabbilder kann sehr schwierig sein, wenn Sie nicht mit der Programmierung und internen Windows-Mechanismen vertraut sind. Wir haben versucht, einen kurzen Einblick in einige der verwendeten Techniken zu geben, darunter einige Beispiele. Damit Sie bei der Problembehandlung eines Absturz Speichers wirklich effektiv sein können, sollten Sie sich mit den erweiterten Debugging-Techniken vertraut machen. Eine Video Übersicht finden Sie unter Erweitertes Windows-Debuggen und Debuggen des Kernel Modus stürzt ab und hängt ab. Lesen Sie auch die unten aufgeführten erweiterten Verweise.

Erweiterte Debugging-Verweise

Erweitertes Windows-Debugging
Debugging-Werkzeuge für Windows (WinDbg KD, CDB, NTSD)

Schritte zum Debuggen

1. Stellen Sie sicher, dass der Computer zum Generieren einer vollständigen Speicherabbilddatei eingerichtet ist, wenn ein Absturz eintritt. Weitere Informationen finden Sie hier .
2. Suchen Sie die Datei "Memory. dmp" in Ihrem Windows-Verzeichnis auf dem Computer, der abstürzt, und kopieren Sie die Datei auf einen anderen Computer.
3. Laden Sie auf dem anderen Computer das Windows 10 SDKherunter.
4. Starten Sie die Installation, und wählen Sie **Debugging Tools für Windows**aus. Dadurch wird das WinDbg-Tool installiert.
5. Öffnen Sie das WinDbg-Tool, und legen Sie den Symbolpfad auf, indem Sie auf **Datei** und dann auf **Symbol Dateipfad**klicken.
   a. Wenn der Computer mit dem Internet verbunden ist, geben Sie den öffentlichen Microsoft-Symbolserver ein (https://msdl.microsoft.com/download/symbols) und klicken Sie auf **OK**. Dies ist die empfohlene Methode.
   b. Wenn der Computer nicht mit dem Internet verbunden ist, müssen Sie einen lokalen Symbolpfadangeben.
6. Klicken Sie auf **Crash Dump öffnen**, und öffnen Sie dann die Datei Memory. dmp, die Sie kopiert haben. Sehen Sie sich das Beispiel unten an.



7. Es sollte einen Link geben, der besagt **! analyze-v** unter **BugCheck-Analyse**. Klicken Sie auf diesen Link.

Dadurch wird der Befehl! Analyze-v in der Eingabeaufforderung unten auf der Seite angezeigt.

8. Eine detaillierte BugCheck-Analyse wird angezeigt. Sehen Sie sich das Beispiel unten an.

```
Command - Dump E:\dmp\MEMORY.DMP - WinDbg:10.0.17134.12 AMD64

Followup:     MachineOwner
---------

5: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

CRITICAL_PROCESS_DIED (ef)
        A critical system process died
Arguments:
Arg1: ffffa586380c1580, Process object or thread object
Arg2: 0000000000000000, If this is 0, a process died. If this is 1, a thread died.
Arg3: 0000000000000000
Arg4: 0000000000000000

Debugging Details:
------------------


KEY_VALUES_STRING: 1


TIMELINE_ANALYSIS: 1


DUMP_CLASS: 1

DUMP_QUALIFIER: 401

BUILD_VERSION_STRING:  16299.15.amd64fre.rs3_release.170928-1534

SYSTEM_MANUFACTURER:  Dell Inc.

SYSTEM_PRODUCT_NAME:  XPS 8700

SYSTEM_SKU:  0x05B7

BIOS_VENDOR:  Dell Inc.

BIOS_VERSION:  A12

BIOS_DATE:  02/05/2018

BASEBOARD_MANUFACTURER:  Dell Inc.

BASEBOARD_PRODUCT:  0KWVT8

BASEBOARD_VERSION:  A02

DUMP_TYPE:  1

BUGCHECK_P1: ffffa586380c1580

BUGCHECK_P2: 0

5: kd>
```

9. Scrollen Sie nach unten zu dem Abschnitt, in dem **STACK_TEXT**steht. Es gibt Zeilen mit Zahlen mit jeder Zeile, gefolgt von einem Doppelpunkt und etwas Text. Dieser Text sollte Ihnen mitteilen, welche DLL den Absturz verursacht, und ggf., welcher Dienst die dll abstürzt.
10. Details zum Interpretieren der STACK_TEXT Ausgabe finden Sie unter Verwenden der! analyze-Erweiterung .

Es gibt viele mögliche Ursachen für einen BugCheck, und jeder Fall ist eindeutig. Im obigen Beispiel sind die wichtigen Zeilen, die aus dem STACK_TEXT identifiziert werden können, 20, 21 und 22:

(Hier werden Hex-Daten entfernt, und Zeilen werden zur Übersichtlichkeit nummeriert)

```
1  : nt!KeBugCheckEx
2  : nt!PspCatchCriticalBreak+0xff
3  : nt!PspTerminateAllThreads+0x1134cf
4  : nt!PspTerminateProcess+0xe0
5  : nt!NtTerminateProcess+0xa9
6  : nt!KiSystemServiceCopyEnd+0x13
7  : nt!KiServiceLinkage
8  : nt!KiDispatchException+0x1107fe
9  : nt!KiFastFailDispatch+0xe4
10 : nt!KiRaiseSecurityCheckFailure+0x3d3
11 : ntdll!RtlpHpFreeWithExceptionProtection$filt$0+0x44
12 : ntdll!_C_specific_handler+0x96
13 : ntdll!RtlpExecuteHandlerForException+0xd
14 : ntdll!RtlDispatchException+0x358
15 : ntdll!KiUserExceptionDispatch+0x2e
16 : ntdll!RtlpHpVsContextFree+0x11e
17 : ntdll!RtlpHpFreeHeap+0x48c
18 : ntdll!RtlpHpFreeWithExceptionProtection+0xda
19 : ntdll!RtlFreeHeap+0x24a
20 : FWPolicyIOMgr!FwBinariesFree+0xa7c2
21 : mpssvc!FwMoneisDiagEdpPolicyUpdate+0x1584f
22 : mpssvc!FwEdpMonUpdate+0x6c
23 : ntdll!RtlpWnfWalkUserSubscriptionList+0x29b
24 : ntdll!RtlpWnfProcessCurrentDescriptor+0x105
25 : ntdll!RtlpWnfNotificationThread+0x80
26 : ntdll!TppExecuteWaitCallback+0xe1
27 : ntdll!TppWorkerThread+0x8d0
28 : KERNEL32!BaseThreadInitThunk+0x14
29 : ntdll!RtlUserThreadStart+0x21
```

Das Problem liegt hier bei **mpssvc** , einer Komponente der Windows-Firewall. Das Problem wurde behoben, indem die Firewall vorübergehend deaktiviert und dann die Firewall-Richtlinien zurückgesetzt werden.

Weitere Beispiele finden Sie im Abschnitt Debugging examples am Ende dieses Artikels.

Video Ressourcen

Die folgenden Videos veranschaulichen verschiedene Techniken zur Problembehandlung bei der Analyse von Dumpdateien.

- Speicherabbilddatei analysieren
- Installieren des Debugging-Tools für Windows (x64 und x86)
- Debuggen des Kernelmodus-Absturz Speicher Dumps
- Spezieller Pool

Erweiterte Problembehandlung mithilfe der Treiberüberprüfung

Wir schätzen, dass etwa 75 Prozent aller Abbruchfehler durch fehlerhafte Treiber verursacht werden. Das Tool für die Treiberüberprüfung bietet verschiedene Methoden, die Ihnen bei der Problembehandlung helfen. Dazu gehören die Ausführung von Treibern in einem isolierten Speicherpool (ohne Freigabe von Arbeitsspeicher mit anderen Komponenten), wodurch extremer Speicherdruck und die Überprüfung von Parametern generiert werden. Wenn das Tool Fehler bei der Ausführung des Treiber Codes findet, erstellt es proaktiv eine Ausnahme, um zu ermöglichen, dass ein Teil des Codes weiter untersucht wird.

WARNING

Die Treiberüberprüfung beansprucht viele CPUs und kann den Computer erheblich verlangsamen. Möglicherweise werden auch weitere Abstürze auftreten. Die Überprüfung deaktiviert fehlerhafte Treiber, nachdem ein Stoppfehler aufgetreten ist, und wird weiterhin ausgeführt, bis Sie das System erfolgreich neu starten und auf den Desktop zugreifen können. Sie können auch davon ausgehen, dass mehrere Dumpdateien erstellt wurden.

Versuchen Sie nicht, alle Treiber gleichzeitig zu überprüfen. Dies kann die Leistung beeinträchtigen und das System unbrauchbar machen. Dies schränkt auch die Effektivität des Tools ein.

Verwenden Sie die folgenden Richtlinien, wenn Sie die Treiberüberprüfung verwenden:

- Testen Sie alle "verdächtigen" Treiber (Treiber, die kürzlich aktualisiert wurden oder bekanntermaßen problematisch sind).
- Wenn weiterhin nicht-analysierbar Abstürze auftreten, versuchen Sie, die Überprüfung auf alle Drittanbieter- und nicht signierten Treiber zu aktivieren.
- Aktivieren Sie die gleichzeitige Überprüfung für Gruppen von 10 – 20 Treibern.
- Darüber hinaus können Sie das Tool deaktivieren, indem Sie im abgesicherten Modus starten, wenn der Computer aufgrund der Treiberüberprüfung nicht in den Desktop gestartet werden kann. Dies liegt daran, dass das Tool nicht im abgesicherten Modus ausgeführt werden kann.

Weitere Informationen finden Sie unter Driver Verifier.

Häufige Windows-Stoppfehler

Dieser Abschnitt enthält keine Liste aller Fehlercodes, doch da viele Fehlercodes die gleichen potenziellen Auflösungen aufweisen, sollten Sie die folgenden Schritte ausführen, um die Fehlerbehandlung zu beheben.

In der folgenden Tabelle sind die allgemeinen Problembehandlungsverfahren für häufige Abbruchfehler Codes aufgeführt.

BEENDEN VON FEHLERMELDUNGEN UND CODE	ABHILFEMASSNAHMEN
VIDEO_ENGINE_TIMEOUT_DETECTED oder VIDEO_TDR_TIMEOUT_DETECTED Beenden des Fehlercodes 0x00000141 oder 0x00000117	Wenden Sie sich an den Anbieter des aufgelisteten Bildschirmtreibers, um ein entsprechendes Update für diesen Treiber zu erhalten.
DRIVER_IRQL_NOT_LESS_OR_EQUAL Abbruchfehler Code 0x0000000D1	Wenden Sie die neuesten Updates für den Treiber an, indem Sie die neuesten kumulativen Updates für das System über die Microsoft Update-katalogwebsite anwenden. Aktualisieren eines veralteten NIC-Treibers. Virtualisierte VMware-Systeme führen häufig "Intel (R) pro/1000 MT-Netzwerkverbindung" (e1g6032e. sys). Dieser Treiber steht unter http://downloadcenter.intel.com. Wenden Sie sich an den Hardwarehersteller, um den NIC-Treiber für eine Lösung zu aktualisieren. Verwenden Sie für VMware-Systeme den integrierten VMware-NIC-Treiber (Typen VMXNET oder VMXNET2, VMXNET3 kann verwendet werden) anstelle von Intel e1g6032e. sys.

BEENDEN VON FEHLERMELDUNGEN UND CODE	ABHILFEMASSNAHMEN
PAGE_FAULT_IN_NONPAGED_AREA Abbruchfehler Code 0x000000050	Wenn ein Treiber in der Stop-Fehlermeldung identifiziert wird, wenden Sie sich an den Hersteller, um ein Update zu erhalten. Wenn keine Updates verfügbar sind, deaktivieren Sie den Treiber, und überwachen Sie das System auf Stabilität. Führen Sie chkdsk/f/r aus, um Datenträgerfehler zu erkennen und zu reparieren. Sie müssen das System neu starten, bevor die Datenträgerüberprüfung auf einer Systempartition beginnt. Wenden Sie sich an den Hersteller, um Diagnosetools für das Festplattensubsystem zu erhalten. Versuchen Sie, alle Anwendungen oder Dienste erneut zu installieren, die kürzlich installiert oder aktualisiert wurden. Es ist möglich, dass der Absturz ausgelöst wurde, während das Systemanwendungen startete und die Registrierung für die Einstellungs Einstellungen gelesen hat. Durch eine Neuinstallation der Anwendung können beschädigte Registrierungsschlüssel behoben werden. Wenn das Problem weiterhin besteht und Sie eine aktuelle Systemstatussicherung ausgeführt haben, versuchen Sie, die Registrierungsstrukturen aus der Sicherung wiederherzustellen.
SYSTEM_SERVICE_EXCEPTION Abbruchfehler Code C000021A {schwerwiegender Systemfehler} der Windows-Subsystem-Systemprozess wurde unerwartet mit einem Status von 0xc0000005 beendet. Das System wurde beendet.	Verwenden Sie das Tool für die Systemdateiprüfung, um fehlende oder beschädigte Systemdateien zu reparieren. Mit der Systemdateiprüfung können Benutzer nach Beschädigungen in Windows-Systemdateien suchen und beschädigte Dateien wiederherstellen. Weitere Informationen finden Sie unter Verwenden des System Datei-Überprüfungstools.
NTFS_FILE_SYSTEM Abbruchfehler Code 0x000000024	Dieser Abbruchfehler wird häufig durch Beschädigungen im NTFS-Dateisystem oder fehlerhafte Blöcke (Sektoren) auf der Festplatte verursacht. Beschädigte Treiber für Festplatten (SATA oder IDE) können sich auch negativ auf die Lese-und Schreibfähigkeit des Systems auf dem Datenträger auswirken. Führen Sie alle Hardwarediagnosen aus, die vom Hersteller des Speichersubsystems bereitgestellt werden. Verwenden Sie das Tool zum Überprüfen von Datenträgern, um sicherzustellen, dass keine Dateisystemfehler vorliegen. Klicken Sie dazu mit der rechten Maustaste auf das Laufwerk, das Sie scannen möchten, wählen Sie Eigenschaften aus, wählen Sie Extras und dann die Schaltfläche jetzt überprüfen aus. Wir empfehlen außerdem, den NTFS-Dateisystemtreiber (NTFS. sys) zu aktualisieren und die neuesten kumulativen Updates für das aktuelle Betriebssystem anzuwenden, bei dem das Problem auftritt.

BEENDEN VON FEHLERMELDUNGEN UND CODE	ABHILFEMASSNAHMEN
KMODE_EXCEPTION_NOT_HANDLED Abbruchfehler Code 0x0000001E	Wenn ein Treiber in der Stop-Fehlermeldung identifiziert wird, deaktivieren oder entfernen Sie diesen Treiber. Deaktivieren oder entfernen Sie alle Treiber oder Dienste, die vor kurzem hinzugefügt wurden. Wenn der Fehler während der Startsequenz auftritt und die Systempartition mithilfe des NTFS-Dateisystems formatiert ist, können Sie den Treiber im Geräte-Manager möglicherweise mithilfe des abgesicherten Modus deaktivieren. Gehen Sie hierzu folgendermaßen vor: Wechseln Sie zu **Einstellungen > & Update Security > Recovery**. Wählen Sie unter **Erweiterter Start**die Option **jetzt neu starten**aus. Wählen Sie nach dem Neustart des PCs auf dem Bildschirm **Option auswählen** die **Option > Problembehandlung > bei den > Start Einstellungen für erweiterte Optionen**aus. Nachdem der Computer neu gestartet wurde, wird eine Liste mit Optionen angezeigt. Drücken Sie **4** oder **F4** , um den Computer im abgesicherten Modus zu starten. Wenn Sie beabsichtigen, das Internet im abgesicherten Modus zu verwenden, drücken Sie **5** oder **F5** für den abgesicherten Modus mit Netzwerk Option.
DPC_WATCHDOG_VIOLATION Abbruchfehler Code 0x00000133	Dieser Abbruchfehler Code wird durch einen fehlerhaften Treiber verursacht, der seine Arbeit unter bestimmten Bedingungen nicht innerhalb des zugeteilten Zeitrahmens abschließt. Damit wir diesen Fehler vermeiden können, sammeln Sie die Speicherabbilddatei aus dem System, und verwenden Sie dann den Windows-Debugger, um den fehlerhaften Treiber zu finden. Wenn ein Treiber in der Stop-Fehlermeldung identifiziert wird, deaktivieren Sie den Treiber, um das Problem zu isolieren. Erkundigen Sie sich beim Hersteller nach Treiberupdates. Überprüfen Sie das Systemprotokoll in der Ereignisanzeige auf weitere Fehlermeldungen, die möglicherweise dazu beitragen, das Gerät oder den Treiber zu identifizieren, der den Abbruchfehler 0x133 verursacht. Überprüfen Sie, ob die installierte neue Hardware mit der installierten Windows-Version kompatibel ist. So können Sie beispielsweise Informationen zur erforderlichen Hardware unter Windows 10-Spezifikationen abrufen. Wenn der Windows-Debugger installiert ist und Sie Zugriff auf öffentliche Symbole haben, können Sie die c:\WINDOWS\MEMORY.dmp-Datei in den Debugger laden und dann auf Ermitteln der Quelle der Fehlerüberprüfung 0x133 (DPC_WATCHDOG_VIOLATION) auf Windows Server 2012 , um den problematischen Treiber aus dem Speicherabbild zu finden.

BEENDEN VON FEHLERMELDUNGEN UND CODE	ABHILFEMASSNAHMEN
USER_MODE_HEALTH_MONITOR Abbruchfehler Code 0x0000009E	Dieser Abbruchfehler weist darauf hin, dass eine Integritätsprüfung im Benutzermodus auf eine Weise fehlgeschlagen ist, die das ordnungsgemäße Herunterfahren verhindert. Daher stellt Windows wichtige Dienste wieder her, indem es neu startet oder das Anwendungsfailover auf andere Server aktiviert. Der Clusterdienst enthält einen Erkennungsmechanismus, der möglicherweise nicht mehr reagiert, wenn sich Benutzermodus-Komponenten befinden. Dieser Abbruchfehler tritt in der Regel in einer Clusterumgebung auf, und der angegebene fehlerhafte Treiber ist "Rs. exe". Überprüfen Sie die Ereignisprotokolle auf Speicherfehler, um den fehlerhaften Prozess zu identifizieren. Versuchen Sie, die Komponente oder den Prozess zu aktualisieren, die in den Ereignisprotokollen angegeben ist. Das folgende Ereignis sollte aufgezeichnet werden: Ereignis-ID: 4870 Quelle: Microsoft-Windows-Failoverclustering Beschreibung: die Überwachung des Benutzermodus-Status hat festgestellt, dass das System nicht mehr reagiert. Der virtuelle Failovercluster-Adapter hat den Kontakt mit dem Cluster Server Prozess mit einer Prozess-ID ' %1 ' für ' %2 ' Sekunden verloren. Die Wiederherstellungsaktion wird ausgeführt. Überprüfen Sie die Cluster Protokolle, um den Prozess zu identifizieren und zu untersuchen, welche Elemente dazu führen können, dass der Prozess hängen bleibt. Weitere Informationen finden Sie unter "Warum wird mein Failover-Clustering-Knoten blaues Screening mit einem Stopp-0x0000009E?" Weitere Informationen finden Sie im folgenden Microsoft-Video was zu tun ist, wenn ein 9E auftritt.

Debugging-Beispiele

Beispiel 1

Dieser BugCheck wird verursacht, wenn ein Treiber während des Upgrades hängen bleibt, was zu einem BugCheck D1 in NDIS. sys (einem Microsoft-Treiber) führt. Im **image_name** wird der Fehler Treiber mitgeteilt, aber da es sich um einen Microsoft-Treiber handelt, kann er nicht ersetzt oder entfernt werden. Die Auflösungsmethode besteht darin, das Netzwerkgerät im Geräte-Manager zu deaktivieren und das Upgrade erneut zu versuchen.

```
2: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

DRIVER_IRQL_NOT_LESS_OR_EQUAL (d1)
An attempt was made to access a pageable (or completely invalid) address at an
interrupt request level (IRQL) that is too high.  This is usually
caused by drivers using improper addresses.
If kernel debugger is available get stack backtrace.
Arguments:
Arg1: 000000000011092a, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000001, value 0 = read operation, 1 = write operation
Arg4: fffff807aa74f4c4, address which referenced memory
Debugging Details:
------------------

KEY_VALUES_STRING: 1
STACKHASH_ANALYSIS: 1
```

```
TIMELINE_ANALYSIS: 1
DUMP_CLASS: 1
DUMP_QUALIFIER: 400
SIMULTANEOUS_TELSVC_INSTANCES:  0
SIMULTANEOUS_TELWP_INSTANCES:  0
BUILD_VERSION_STRING:  16299.15.amd64fre.rs3_release.170928-1534
SYSTEM_MANUFACTURER:  Alienware
SYSTEM_PRODUCT_NAME:  Alienware 15 R2
SYSTEM_SKU:  Alienware 15 R2
SYSTEM_VERSION:  1.2.8
BIOS_VENDOR:  Alienware
BIOS_VERSION:  1.2.8
BIOS_DATE:  01/29/2016
BASEBOARD_MANUFACTURER:  Alienware
BASEBOARD_PRODUCT:  Alienware 15 R2
BASEBOARD_VERSION:  A00
DUMP_TYPE:  2
BUGCHECK_P1: 11092a
BUGCHECK_P2: 2
BUGCHECK_P3: 1
BUGCHECK_P4: fffff807aa74f4c4
WRITE_ADDRESS: fffff80060602380: Unable to get MiVisibleState
Unable to get NonPagedPoolStart
Unable to get NonPagedPoolEnd
Unable to get PagedPoolStart
Unable to get PagedPoolEnd
000000000011092a
CURRENT_IRQL:  2
FAULTING_IP:
NDIS!NdisQueueIoWorkItem+4 [minio\ndis\sys\miniport.c @ 9708]
fffff807`aa74f4c4 48895120        mov     qword ptr [rcx+20h],rdx
CPU_COUNT: 8
CPU_MHZ: a20
CPU_VENDOR:  GenuineIntel
CPU_FAMILY: 6
CPU_MODEL: 5e
CPU_STEPPING: 3
CPU_MICROCODE: 6,5e,3,0 (F,M,S,R)  SIG: BA'00000000 (cache) BA'00000000 (init)
BLACKBOXPNP: 1 (!blackboxpnp)
DEFAULT_BUCKET_ID:  WIN8_DRIVER_FAULT
BUGCHECK_STR:  AV
PROCESS_NAME:  System
ANALYSIS_SESSION_HOST:  SHENDRIX-DEV0
ANALYSIS_SESSION_TIME:  01-17-2019 11:06:05.0653
ANALYSIS_VERSION: 10.0.18248.1001 amd64fre
TRAP_FRAME:  ffffa884c0c3f6b0 -- (.trap 0xffffa884c0c3f6b0)
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=fffff807ad018bf0 rbx=0000000000000000 rcx=000000000011090a
rdx=fffff807ad018c10 rsi=0000000000000000 rdi=0000000000000000
rip=fffff807aa74f4c4 rsp=ffffa884c0c3f840 rbp=000000002408fd00
r8=ffffb30e0e99ea30  r9=0000000001d371c1 r10=0000000020000080
r11=0000000000000000 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na pe nc
NDIS!NdisQueueIoWorkItem+0x4:
fffff807`aa74f4c4 48895120        mov     qword ptr [rcx+20h],rdx ds:00000000`0011092a=????????????????
Resetting default scope

LAST_CONTROL_TRANSFER:  from fffff800603799e9 to fffff8006036e0e0

STACK_TEXT:
ffffa884`c0c3f568 fffff800`603799e9 : 00000000`0000000a 00000000`0011092a 00000000`00000002 00000000`00000001 :
nt!KeBugCheckEx [minkernel\ntos\ke\amd64\procstat.asm @ 134]
ffffa884`c0c3f570 fffff800`60377d7d : fffff78a`4000a150 ffffb30e`03fba001 ffff8180`f0b5d180 00000000`000000ff :
nt!KiBugCheckDispatch+0x69 [minkernel\ntos\ke\amd64\trap.asm @ 2998]
ffffa884`c0c3f6b0 fffff807`aa74f4c4 : 00000000`00000002 ffff8180`f0754180 00000000`00269fb1 ffff8180`f0754180 :
nt!KiPageFault+0x23d [minkernel\ntos\ke\amd64\trap.asm @ 1248]
ffffa884`c0c3f840 fffff800`60256b63 : ffffb30e`0e18f710 ffff8180`f0754180 ffffa884`c0c3fa18 00000000`00000002 :
```

```
NDIS!NdisQueueIoWorkItem+0x4 [minio\ndis\sys\miniport.c @ 9708]
ffffa884`c0c3f870 fffff800`60257bfd : 00000000`00000008 00000000`00000000 00000000`00269fb1 ffff8180`f0754180 :
nt!KiProcessExpiredTimerList+0x153 [minkernel\ntos\ke\dpcsup.c @ 2078]
ffffa884`c0c3f960 fffff800`6037123a : 00000000`00000000 ffff8180`f0754180 00000000`00000000 ffff8180`f0760cc0 :
nt!KiRetireDpcList+0x43d [minkernel\ntos\ke\dpcsup.c @ 1512]
ffffa884`c0c3fb60 00000000`00000000 : ffffa884`c0c40000 ffffa884`c0c39000 00000000`00000000 00000000`00000000 :
nt!KiIdleLoop+0x5a [minkernel\ntos\ke\amd64\idle.asm @ 166]

RETRACER_ANALYSIS_TAG_STATUS:  Failed in getting KPCR for core 2
THREAD_SHA1_HASH_MOD_FUNC:  5b59a784f22d4b5cbd5a8452fe39914b8fd7961d
THREAD_SHA1_HASH_MOD_FUNC_OFFSET:  5643383f9cae3ca39073f7721b53f0c633bfb948
THREAD_SHA1_HASH_MOD:  20edda059578820e64b723e466deea47f59bd675
FOLLOWUP_IP:
NDIS!NdisQueueIoWorkItem+4 [minio\ndis\sys\miniport.c @ 9708]
fffff807`aa74f4c4 48895120        mov     qword ptr [rcx+20h],rdx
FAULT_INSTR_CODE:  20518948
FAULTING_SOURCE_LINE:  minio\ndis\sys\miniport.c
FAULTING_SOURCE_FILE:  minio\ndis\sys\miniport.c
FAULTING_SOURCE_LINE_NUMBER:  9708
FAULTING_SOURCE_CODE:
  9704:     _In_ _Points_to_data_      PVOID                       WorkItemContext
  9705:     )
  9706: {
  9707:
> 9708:     ((PNDIS_IO_WORK_ITEM)NdisIoWorkItemHandle)->Routine = Routine;
  9709:     ((PNDIS_IO_WORK_ITEM)NdisIoWorkItemHandle)->WorkItemContext = WorkItemContext;
  9710:
  9711:     IoQueueWorkItem(((PNDIS_IO_WORK_ITEM)NdisIoWorkItemHandle)->IoWorkItem,
  9712:                     ndisDispatchIoWorkItem,
  9713:                     CriticalWorkQueue,

SYMBOL_STACK_INDEX:  3
SYMBOL_NAME:  NDIS!NdisQueueIoWorkItem+4
FOLLOWUP_NAME:  ndiscore
MODULE_NAME: NDIS
IMAGE_NAME:  NDIS.SYS
DEBUG_FLR_IMAGE_TIMESTAMP:  0
IMAGE_VERSION:  10.0.16299.99
DXGANALYZE_ANALYSIS_TAG_PORT_GLOBAL_INFO_STR:  Hybrid_FALSE
DXGANALYZE_ANALYSIS_TAG_ADAPTER_INFO_STR:  GPU0_VenId0x1414_DevId0x8d_WDDM1.3_Active;
STACK_COMMAND:  .thread ; .cxr ; kb
BUCKET_ID_FUNC_OFFSET:  4
FAILURE_BUCKET_ID:  AV_NDIS!NdisQueueIoWorkItem
BUCKET_ID:  AV_NDIS!NdisQueueIoWorkItem
PRIMARY_PROBLEM_CLASS:  AV_NDIS!NdisQueueIoWorkItem
TARGET_TIME:  2017-12-10T14:16:08.000Z
OSBUILD:  16299
OSSERVICEPACK:  98
SERVICEPACK_NUMBER: 0
OS_REVISION: 0
SUITE_MASK:  784
PRODUCT_TYPE:  1
OSPLATFORM_TYPE:  x64
OSNAME:  Windows 10
OSEDITION:  Windows 10 WinNt TerminalServer SingleUserTS Personal
OS_LOCALE:
USER_LCID:  0
OSBUILD_TIMESTAMP:  2017-11-26 03:49:20
BUILDDATESTAMP_STR:  170928-1534
BUILDLAB_STR:  rs3_release
BUILDOSVER_STR:  10.0.16299.15.amd64fre.rs3_release.170928-1534
ANALYSIS_SESSION_ELAPSED_TIME:  8377
ANALYSIS_SOURCE:  KM
FAILURE_ID_HASH_STRING:  km:av_ndis!ndisqueueioworkitem
FAILURE_ID_HASH:  {10686423-afa1-4852-ad1b-9324ac44ac96}
FAILURE_ID_REPORT_LINK: https://go.microsoft.com/fwlink/?LinkID=397724&FailureHash=10686423-afa1-4852-ad1b-
9324ac44ac96
Followup:     ndiscore
---------
```

Beispiel 2

In diesem Beispiel hat ein nicht-Microsoft-Treiberseiten Fehler verursacht, daher haben wir keine Symbole für diesen Treiber. Wenn Sie jedoch **image_name** und oder **module_name** sehen, gibt es **WwanUsbMP. sys** , die das Problem verursacht hat. Das Trennen des Geräts und das erneute Testen des Upgrades ist eine mögliche Lösung.

```
1: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

PAGE_FAULT_IN_NONPAGED_AREA (50)
Invalid system memory was referenced.  This cannot be protected by try-except.
Typically the address is just plain bad or it is pointing at freed memory.
Arguments:
Arg1: 8ba10000, memory referenced.
Arg2: 00000000, value 0 = read operation, 1 = write operation.
Arg3: 82154573, If non-zero, the instruction address which referenced the bad memory
                address.
Arg4: 00000000, (reserved)

Debugging Details:
------------------

*** WARNING: Unable to verify timestamp for WwanUsbMp.sys
*** ERROR: Module load completed but symbols could not be loaded for WwanUsbMp.sys

KEY_VALUES_STRING: 1
STACKHASH_ANALYSIS: 1
TIMELINE_ANALYSIS: 1
DUMP_CLASS: 1
DUMP_QUALIFIER: 400
BUILD_VERSION_STRING:  16299.15.x86fre.rs3_release.170928-1534
MARKER_MODULE_NAME:  IBM_ibmpmdrv
SYSTEM_MANUFACTURER:  LENOVO
SYSTEM_PRODUCT_NAME:  20AWS07H00
SYSTEM_SKU:  LENOVO_MT_20AW_BU_Think_FM_ThinkPad T440p
SYSTEM_VERSION:  ThinkPad T440p
BIOS_VENDOR:  LENOVO
BIOS_VERSION:  GLET85WW (2.39 )
BIOS_DATE:  09/29/2016
BASEBOARD_MANUFACTURER:  LENOVO
BASEBOARD_PRODUCT:  20AWS07H00
BASEBOARD_VERSION:  Not Defined
DUMP_TYPE:  2
BUGCHECK_P1: ffffffff8ba10000
BUGCHECK_P2: 0
BUGCHECK_P3: ffffffff82154573
BUGCHECK_P4: 0
READ_ADDRESS: 822821d0: Unable to get MiVisibleState
8ba10000
FAULTING_IP:
nt!memcpy+33 [minkernel\crts\crtw32\string\i386\memcpy.asm @ 213
82154573 f3a5            rep movs dword ptr es:[edi],dword ptr [esi]
MM_INTERNAL_CODE:  0
CPU_COUNT: 4
CPU_MHZ: 95a
CPU_VENDOR:  GenuineIntel
CPU_FAMILY: 6
CPU_MODEL: 3c
CPU_STEPPING: 3
```

```
CPU_MICROCODE: 6,3c,3,0 (F,M,S,R)  SIG: 21'00000000 (cache) 21'00000000 (init)
BLACKBOXBSD: 1 (!blackboxbsd)
BLACKBOXPNP: 1 (!blackboxpnp)
DEFAULT_BUCKET_ID:  WIN8_DRIVER_FAULT
BUGCHECK_STR:  AV
PROCESS_NAME:  System
CURRENT_IRQL:  2
ANALYSIS_SESSION_HOST:  SHENDRIX-DEV0
ANALYSIS_SESSION_TIME:  01-17-2019 10:54:53.0780
ANALYSIS_VERSION: 10.0.18248.1001 amd64fre
TRAP_FRAME:  8ba0efa8 -- (.trap 0xffffffff8ba0efa8)
ErrCode = 00000000
eax=8ba1759e ebx=a2bfd314 ecx=00001d67 edx=00000002 esi=8ba10000 edi=a2bfe280
eip=82154573 esp=8ba0f01c ebp=8ba0f024 iopl=0         nv up ei pl nz ac pe nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00010216
nt!memcpy+0x33:
82154573 f3a5            rep movs dword ptr es:[edi],dword ptr [esi]
Resetting default scope
LOCK_ADDRESS:  8226c6e0 -- (!locks 8226c6e0)
Cannot get _ERESOURCE type
Resource @ nt!PiEngineLock (0x8226c6e0)    Available
1 total locks
PNP_TRIAGE_DATA:
                Lock address  : 0x8226c6e0
                Thread Count  : 0
                Thread address: 0x00000000
                Thread wait   : 0x0

LAST_CONTROL_TRANSFER:  from 82076708 to 821507e8

STACK_TEXT:
8ba0ede4 82076708 00000050 8ba10000 00000000 nt!KeBugCheckEx [minkernel\ntos\ke\i386\procstat.asm @ 114]
8ba0ee40 8207771e 8ba0efa8 8ba10000 8ba0eea0 nt!MiSystemFault+0x13c8 [minkernel\ntos\mm\mmfault.c @ 4755]
8ba0ef08 821652ac 00000000 8ba10000 00000000 nt!MmAccessFault+0x83e [minkernel\ntos\mm\mmfault.c @ 6868]
8ba0ef08 82154573 00000000 8ba10000 00000000 nt!_KiTrap0E+0xec [minkernel\ntos\ke\i386\trap.asm @ 5153]
8ba0f024 86692866 a2bfd314 8ba0f094 0000850a nt!memcpy+0x33 [minkernel\crts\crtw32\string\i386\memcpy.asm @
213]
8ba0f040 866961bc 8ba0f19c a2bfd0e8 00000000 NDIS!ndisMSetPowerManagementCapabilities+0x8a
[minio\ndis\sys\miniport.c @ 7969]
8ba0f060 866e1f66 866e1caf adfb9000 00000000 NDIS!ndisMSetGeneralAttributes+0x23d [minio\ndis\sys\miniport.c @
8198]
8ba0f078 ac50c15f a2bfd0e8 0000009f 00000001 NDIS!NdisMSetMiniportAttributes+0x2b7 [minio\ndis\sys\miniport.c @
7184]
WARNING: Stack unwind information not available. Following frames may be wrong.
8ba0f270 ac526f96 adfb9000 a2bfd0e8 8269b9b0 WwanUsbMp+0x1c15f
8ba0f3cc 866e368a a2bfd0e8 00000000 8ba0f4c0 WwanUsbMp+0x36f96
8ba0f410 867004b0 a2bfd0e8 a2bfd0e8 a2be2a70 NDIS!ndisMInvokeInitialize+0x60 [minio\ndis\sys\miniport.c @
13834]
8ba0f7ac 866dbc8e a2acf730 866b807c 00000000 NDIS!ndisMInitializeAdapter+0xa23 [minio\ndis\sys\miniport.c @
601]
8ba0f7d8 866e687d a2bfd0e8 00000000 00000000 NDIS!ndisInitializeAdapter+0x4c [minio\ndis\sys\initpnp.c @ 931]
8ba0f800 866e90bb adfb64d8 00000000 a2bfd0e8 NDIS!ndisPnPStartDevice+0x118 [minio\ndis\sys\configm.c @ 4235]
8ba0f820 866e8a58 adfb64d8 a2bfd0e8 00000000 NDIS!ndisStartDeviceSynchronous+0xbd [minio\ndis\sys\ndispnp.c @
3096]
8ba0f838 866e81df adfb64d8 8ba0f85e 8ba0f85f NDIS!ndisPnPIrpStartDevice+0xb4 [minio\ndis\sys\ndispnp.c @ 1067]
8ba0f860 820a7e98 a2bfd030 adfb64d8 8ba0f910 NDIS!ndisPnPDispatch+0x108 [minio\ndis\sys\ndispnp.c @ 2429]
8ba0f878 8231f07e 8ba0f8ec adf5d4c8 872e2eb8 nt!IofCallDriver+0x48 [minkernel\ntos\io\iomgr\iosubs.c @ 3149]
8ba0f898 820b8569 820c92b8 872e2eb8 8ba0f910 nt!PnpAsynchronousCall+0x9e [minkernel\ntos\io\pnpmgr\irp.c @
3005]
8ba0f8cc 820c9a76 00000000 820c92b8 872e2eb8 nt!PnpSendIrp+0x67 [minkernel\ntos\io\pnpmgr\irp.h @ 286]
8ba0f914 8234577b 872e2eb8 adf638b0 adf638b0 nt!PnpStartDevice+0x60 [minkernel\ntos\io\pnpmgr\irp.c @ 3187]
8ba0f94c 82346cc7 872e2eb8 adf638b0 adf638b0 nt!PnpStartDeviceNode+0xc3 [minkernel\ntos\io\pnpmgr\start.c @
1712]
8ba0f96c 82343c68 00000000 a2bdb3d8 adf638b0 nt!PipProcessStartPhase1+0x4d [minkernel\ntos\io\pnpmgr\start.c @
114]
8ba0fb5c 824db885 8ba0fb80 00000000 00000000 nt!PipProcessDevNodeTree+0x386 [minkernel\ntos\io\pnpmgr\enum.c @
6129]
8ba0fb88 8219571b 85852520 8c601040 8226ba90 nt!PiRestartDevice+0x91 [minkernel\ntos\io\pnpmgr\enum.c @ 4743]
8ba0fbe8 820804af 00000000 00000000 8c601040 nt!PnpDeviceActionWorker+0xdb4b7
```

```
[minkernel\ntos\io\pnpmgr\action.c @ 674]
8ba0fc38 8211485c 85852520 421de295 00000000 nt!ExpWorkerThread+0xcf [minkernel\ntos\ex\worker.c @ 4270]
8ba0fc70 82166785 820803e0 85852520 00000000 nt!PspSystemThreadStartup+0x4a [minkernel\ntos\ps\psexec.c @ 7756]
8ba0fc88 82051e07 85943940 8ba0fcd8 82051bb9 nt!KiThreadStartup+0x15 [minkernel\ntos\ke\i386\threadbg.asm @ 82]
8ba0fc94 82051bb9 8b9cc600 8ba10000 8ba0d000 nt!KiProcessDeferredReadyList+0x17 [minkernel\ntos\ke\thredsup.c @
5309]
8ba0fcd8 00000000 00000000 00000000 00000000 nt!KeSetPriorityThread+0x249 [minkernel\ntos\ke\thredobj.c @ 3881]


RETRACER_ANALYSIS_TAG_STATUS:  Failed in getting KPCR for core 1
THREAD_SHA1_HASH_MOD_FUNC:  e029276c66aea80ba36903e89947127118d31128
THREAD_SHA1_HASH_MOD_FUNC_OFFSET:  012389f065d31c8eedd6204846a560146a38099b
THREAD_SHA1_HASH_MOD:  44dc639eb162a28d47eaeeae4afe6f9eeccced3d
FOLLOWUP_IP:
WwanUsbMp+1c15f
ac50c15f 8bf0            mov     esi,eax
FAULT_INSTR_CODE:  f33bf08b
SYMBOL_STACK_INDEX:  8
SYMBOL_NAME:  WwanUsbMp+1c15f
FOLLOWUP_NAME:  MachineOwner
MODULE_NAME: WwanUsbMp
IMAGE_NAME:  WwanUsbMp.sys
DEBUG_FLR_IMAGE_TIMESTAMP:  5211bb0c
DXGANALYZE_ANALYSIS_TAG_PORT_GLOBAL_INFO_STR:  Hybrid_FALSE
DXGANALYZE_ANALYSIS_TAG_ADAPTER_INFO_STR:
GPU0_VenId0x1414_DevId0x8d_WDDM1.3_NotActive;GPU1_VenId0x8086_DevId0x416_WDDM1.3_Active_Post;
STACK_COMMAND:  .thread ; .cxr ; kb
BUCKET_ID_FUNC_OFFSET:  1c15f
FAILURE_BUCKET_ID:  AV_R_INVALID_WwanUsbMp!unknown_function
BUCKET_ID:  AV_R_INVALID_WwanUsbMp!unknown_function
PRIMARY_PROBLEM_CLASS:  AV_R_INVALID_WwanUsbMp!unknown_function
TARGET_TIME:  2018-02-12T11:33:51.000Z
OSBUILD:  16299
OSSERVICEPACK:  15
SERVICEPACK_NUMBER: 0
OS_REVISION: 0
SUITE_MASK:  272
PRODUCT_TYPE:  1
OSPLATFORM_TYPE:  x86
OSNAME:  Windows 10
OSEDITION:  Windows 10 WinNt TerminalServer SingleUserTS
OS_LOCALE:
USER_LCID:  0
OSBUILD_TIMESTAMP:  2017-09-28 18:32:28
BUILDDATESTAMP_STR:  170928-1534
BUILDLAB_STR:  rs3_release
BUILDOSVER_STR:  10.0.16299.15.x86fre.rs3_release.170928-1534
ANALYSIS_SESSION_ELAPSED_TIME:  162bd
ANALYSIS_SOURCE:  KM
FAILURE_ID_HASH_STRING:  km:av_r_invalid_wwanusbmp!unknown_function
FAILURE_ID_HASH:  {31e4d053-0758-e43a-06a7-55f69b072cb3}
FAILURE_ID_REPORT_LINK: https://go.microsoft.com/fwlink/?LinkID=397724&FailureHash=31e4d053-0758-e43a-06a7-
55f69b072cb3

Followup:     MachineOwner
---------

ReadVirtual: 812d1248 not properly sign extended
```

Verweise

Fehlerüberprüfung-Code Referenz

Erweiterte Problembehandlung für Stoppfehler 7B oder Inaccessible_Boot_Device

04.12.2019 • 8 minutes to read

In diesem Artikel finden Sie eine schrittweise Anleitung zur Problembehandlung des **Stopp Fehlers 7B: INACCESSIBLE_BOOT_DEVICE**. Dieser Fehler kann auftreten, nachdem einige Änderungen am Computer vorgenommen wurden, oder unmittelbar nach der Bereitstellung von Windows auf dem Computer.

Ursachen für den INACCESSIBLE_BOOT_DEVICE Abbruchfehler

Bei einem der folgenden Faktoren kann der Abbruchfehler auftreten:

- Fehlende, beschädigte oder fehlerhafte Filtertreiber, die mit dem Speicherstapel verknüpft sind
- Dateisystem Beschädigung
- Änderungen am Speichercontroller Modus oder an den Einstellungen im BIOS
- Verwenden eines anderen Speichercontrollers als derjenige, der bei der Installation von Windows verwendet wurde
- Verschieben der Festplatte auf einen anderen Computer mit einem anderen Controller
- Fehlerhafte Motherboards oder Speichercontroller oder fehlerhafte Hardware
- In ungewöhnlichen Fällen: der Fehler des TrustedInstaller-Diensts zum übernehmen neu installierter Updates aufgrund von komponentenbasierten Speicherbeschädigungen
- Beschädigte Dateien in der **Start** Partition (beispielsweise Beschädigungen des Volumes, das beim Ausführen des **** `diskpart` > `list vol` Befehls System beschriftet ist)

Problembehandlung für diesen Fehler

Starten Sie den Computer im Windows-Wiederherstellungsmodus (WinRE). Führen Sie dazu die folgenden Schritte aus.

1. Starten Sie das System mithilfe der Installationsmedien für die installierte Version von Windows.
2. Wählen Sie auf dem Bildschirm **Windows installieren** die Option **weiter** > **Reparatur Ihres Computers** aus.
3. Wählen Sie auf dem Bildschirm **System Wiederherstellungsoptionen** die Option **nächste** > **Eingabeaufforderung** aus.

Überprüfen, ob die Startdiskette verbunden und barrierefrei ist

Schritt 1

Führen `diskpart` Sie an der WinRE-Eingabeaufforderung aus, und `list disk` führen Sie dann aus.

Eine Liste der physikalischen Datenträger, die an den Computer angeschlossen sind, sollte angezeigt werden und der folgenden Anzeige ähneln:

```
Disk ###  Status         Size     Free     Dyn  Gpt

--------  -------------  -------  -------  ---  ---

Disk 0    Online         **size*  GB      0 B        *
```

Wenn der Computer eine Unified Extensible Firmware Interface (UEFI)-Start Schnittstelle verwendet, befindet sich in der Spalte**GPT* * ein Sternchen ().

Wenn der Computer eine BIOS-Schnittstelle (Basic Input/Output System) verwendet, wird in der Spalte **dyn** kein Sternchen angezeigt.

Schritt 2

Wenn der `list disk` Befehl die Betriebssystemdatenträger korrekt aufführt, `list vol` führen Sie `diskpart` den Befehl in aus.

`list vol` generiert eine Ausgabe, die der folgenden Anzeige ähnelt:

```
Volume ###  Ltr  Label        Fs     Type        Size     Status     Info

----------  ---  -----------  -----  ----------  -------  ---------  --------

Volume 0         Windows RE   NTFS   Partition    499 MB  Healthy

Volume 1     C   OSDisk       NTFS   Partition    222 GB  Healthy    Boot

Volume 2         SYSTEM       FAT32  Partition    499 MB  Healthy    System
```

> **NOTE**
> Wenn die Festplatte, die das Betriebssystem enthält, nicht in der Ausgabe aufgeführt ist, müssen Sie den OEM-oder Virtualization-Hersteller einbinden.

Überprüfen der Integrität der Startkonfigurationsdatenbank

Überprüfen Sie, ob die Startkonfigurationsdatenbank (Start Configuration Database, BCD) alle korrekten Einträge enthält. Führen `bcdedit` Sie dazu an der Eingabeaufforderung WinRE.

So überprüfen Sie die BCD-Einträge:

1. Überprüfen Sie den **Windows-Start-Manager-** Abschnitt mit dem **{** Start-ID-Bezeichner. Stellen Sie sicher, dass die **Geräte** -und **Pfad** Einträge auf die richtige Geräte-und bootloaderdatei verweisen.

   Eine Beispielausgabe, wenn der Computer UEFI-basiert ist:

   ```
   device                  partition=\Device\HarddiskVolume2
   path                    \EFI\Microsoft\Boot\bootmgfw.efi
   ```

   Eine Beispielausgabe, wenn der Computer BIOS-basiert ist:

   ```
   Device                partition=C:
   ```

   > **NOTE**
   > Diese Ausgabe enthält möglicherweise keinen Pfad.

2. Vergewissern Sie sich, dass im **Windows-Bootloader** , der den **{default}** -Bezeichner hat, **Device** , **path** , **osdevice** und **systemroot** auf das richtige Gerät oder die richtige Partition, die winload-Datei, die Betriebssystempartition oder das Gerät und den Betriebssystemordner verweisen.

> **NOTE**
>
> Wenn der Computer UEFI-basiert ist, enthalten **die voll** ständigen Einstellungen für den **Winload** unter **{Standard}** eine **EFI** -Erweiterung.

```
X:\Sources>bcdedit

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=\Device\HarddiskVolume2
path                    \EFI\Microsoft\Boot\bootmgfw.efi
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
integrityservices       Enable
default                 {default}
resumeobject            {794a37b9-6ff0-11e6-8ad9-8d64679fc580}
displayorder            {default}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {default}
device                  partition=C:
path                    \Windows\system32\winload.efi
description             Windows 8.1
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {794a37bd-6ff0-11e6-8ad9-8d64679fc580}
integrityservices       Enable
recoveryenabled         Yes
isolatedcontext         Yes
allowedinmemorysettings 0x15000075
osdevice                partition=C:
systemroot              \Windows
resumeobject            {794a37b9-6ff0-11e6-8ad9-8d64679fc580}
nx                      OptOut
pae                     ForceDisable
bootmenupolicy          Standard
```

Wenn eine der Informationen falsch ist oder fehlt, empfehlen wir, eine Sicherungskopie des BCD-Speichers zu erstellen. Führen Sie hierzu `bcdedit /export C:\temp\bcdbackup` aus. Dieser Befehl erstellt eine Sicherung in **C:\temp** mit dem Namen **bcdbackup** . Wenn Sie die Sicherung wiederherstellen `bcdedit /import C:\temp\bcdbackup` möchten, führen Sie. Mit diesem Befehl werden alle BCD-Einstellungen mithilfe der Einstellungen in **bcdbackup** überschrieben.

Führen Sie nach Abschluss der Sicherung den folgenden Befehl aus, um die Änderungen vorzunehmen:

```
bcdedit /set *{identifier}* option value
```

Wenn beispielsweise das Gerät unter {Standard} falsch oder nicht vorhanden ist, führen Sie den folgenden Befehl aus, um es einzurichten: `bcdedit /set {default} device partition=C:`

Wenn Sie die BCD-Datei vollständig neu erstellen möchten, oder wenn Sie eine Meldung erhalten, die besagt, dass "**der Startkonfigurationsdatenspeicher nicht geöffnet werden konnte. Das System konnte die angegebene Datei nicht finden:** "Ausführen `bootrec /rebuildbcd`.

Wenn BCD über die **richtigen Einträge verfügt** , überprüfen Sie, ob die **Winload** -und-Eintrags Einträge am richtigen Speicherort für den im Befehl **Bcdedit** angegebenen Pfad vorhanden sind. Standardmäßig befindet sich der Startwert **in der BIOS-Partition** im Stammverzeichnis der **System** Partition. Um die Datei anzuzeigen, führen `Attrib -s -h -r` Sie.

Wenn die Dateien fehlen und Sie die Startdateien neu erstellen möchten, führen Sie die folgenden Schritte aus:

1. Kopieren Sie den gesamten Inhalt unter der **System** Partition an einen anderen Speicherort. Sie können auch die Eingabeaufforderung verwenden, um zum Betriebssystemlaufwerk zu navigieren, einen neuen Ordner zu erstellen und dann alle Dateien und Ordner aus dem **System** Datenträger wie folgt zu kopieren:

```
D:\> Mkdir  BootBackup
R:\> Copy *.* D:\BootBackup
```

1. Wenn Sie Windows 10 verwenden oder bei der Problembehandlung unter Windows 10 ISO an der Eingabeaufforderung für die Windows-Umgebung vor der Installation arbeiten, können Sie den Befehl **BCDboot** verwenden, um die Startdateien wie folgt neu zu erstellen:

   ```
   Bcdboot <**OSDrive* >:\windows /s <**SYSTEMdrive* >: /f ALL
   ```

   Beispiel: Wenn wir den Buchstaben R `<System Drive>` (WinRE Drive) und den `<OSdrive>` Buchstaben D zuweisen, lautet dieser Befehl wie folgt:

   ```
   Bcdboot D:\windows /s R: /f ALL
   ```

   > **NOTE**
   > Der **gesamte** Teil des **BCDboot** -Befehls schreibt alle Startdateien (sowohl UEFI als auch BIOS) an deren jeweilige Speicherorte.

Wenn Sie nicht über ein Windows 10 ISO verfügen, müssen Sie die Partition formatieren und einen anderen Arbeitscomputer mit einem ähnlichen Windows- **Build kopieren.** Gehen Sie hierzu folgendermaßen vor:

1. Starten Sie **Editor** .
2. Drücken Sie STRG + O.
3. Navigieren Sie zu der Systempartition (in diesem Beispiel ist es R).
4. Klicken Sie mit der rechten Maustaste auf die Partition, und formatieren Sie Sie dann.

Problembehandlung, wenn dieses Problem nach einer Windows Update-Installation auftritt

Führen Sie den folgenden Befehl aus, um die Windows Update-Installation und die Datumsangaben zu überprüfen:

```
Dism /Image:<Specify the OS drive>: /Get-packages
```

Nachdem Sie diesen Befehl ausgeführt haben, werden die Pakete " **Ausstehend** " und " **Deinstallation ausstehend** " angezeigt:

```
Package Identity : Package_for_KB4459941~31bf3856ad364e35~amd64~~6.3.1.2285
State : Install Pending
Release Type : Update
Install Time : 11/13/2018 7:41 PM

Package Identity : Package_for_KB4462930~31bf3856ad364e35~amd64~~6.3.1.0
State : Installed
Release Type : Update
Install Time : 11/7/2018 4:54 PM

Package Identity : Package_for_KB4467694~31bf3856ad364e35~amd64~~6.3.1.0
State : Installed
Release Type : Security Update
Install Time : 11/13/2018 7:40 PM

Package Identity : Package_for_RollupFix~31bf3856ad364e35~amd64~~9600.18874.1.4
State : Superseded
Release Type : Security Update
Install Time : 11/7/2018 3:12 PM

Package Identity : Package_for_RollupFix~31bf3856ad364e35~amd64~~9600.19155.1.5
State : Uninstall Pending
Release Type : Security Update
Install Time : 11/7/2018 4:54 PM

Package Identity : Package_for_RollupFix~31bf3856ad364e35~amd64~~9600.19182.1.6
State : Install Pending
Release Type : Security Update
Install Time : 11/13/2018 7:43 PM
```

1. Führen Sie `dism /Image:C:\ /Cleanup-Image /RevertPendingActions` den Befehl aus. Ersetzen Sie **C:** durch die Systempartition für Ihren Computer.

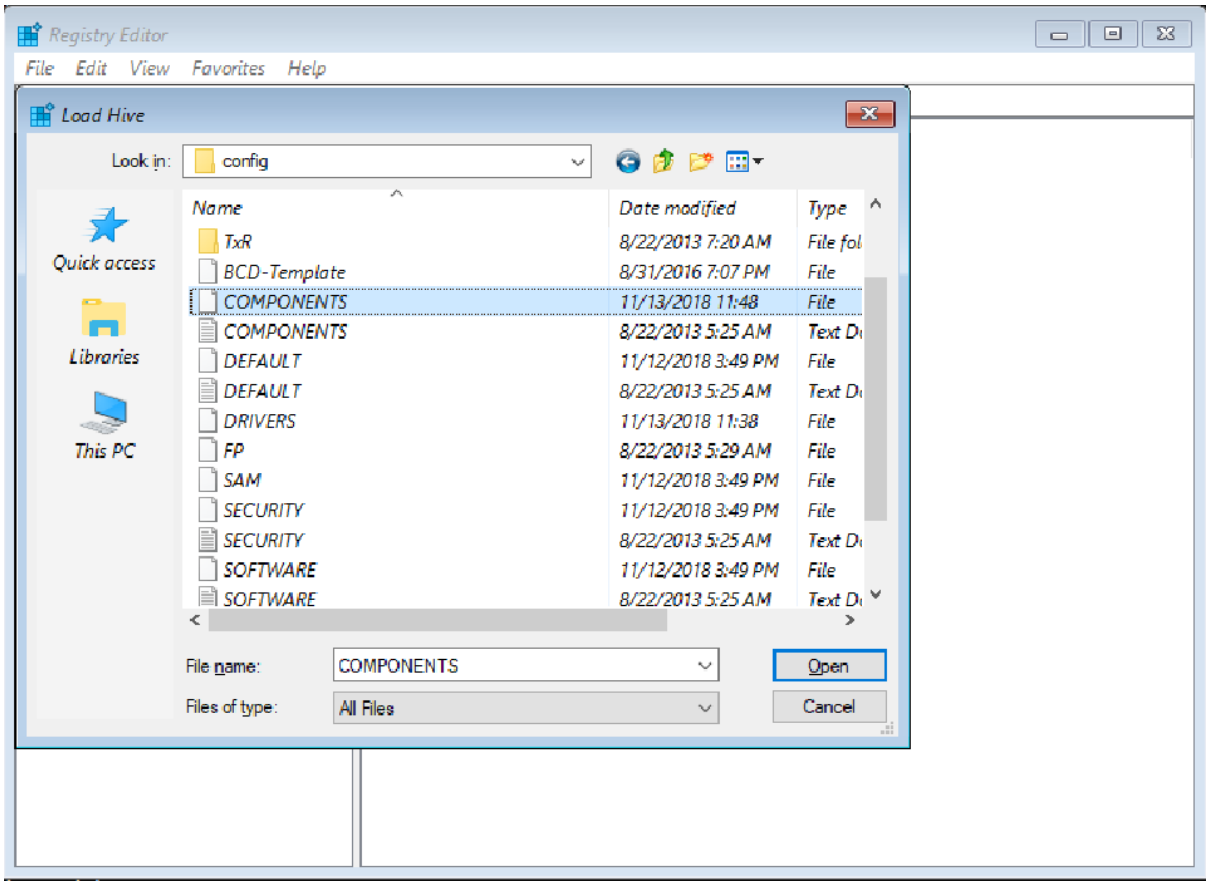
```
X:\Sources>dism /Image:C:\ /Cleanup-Image /RevertPendingActions

Deployment Image Servicing and Management tool
Version: 10.0.17134.1

Image Version: 6.3.9600.17709

The scratch directory size might be insufficient to perform this operation. This can cause unexpected behavior.
Use the /ScratchDir option to point to a folder with sufficient scratch space. The recommended size is at least 1024 MB.


Reverting pending actions from the image...
The operation completed. Revert of pending actions will be attempted after the reboot.
The operation completed successfully.
```

2. Navigieren Sie zu ** *OSdriveLetter* :\Windows\WinSxS** , und überprüfen Sie, ob die Datei **Pending. XML** vorhanden ist. Wenn dies der Fall ist, benennen Sie Sie in **Ausstehend. Xml. Old**um.

3. Wenn Sie die Registrierungsänderungen wiederherstellen möchten, geben Sie **Regedit** an der Eingabeaufforderung ein, um den **Registrierungs-Editor**zu öffnen.

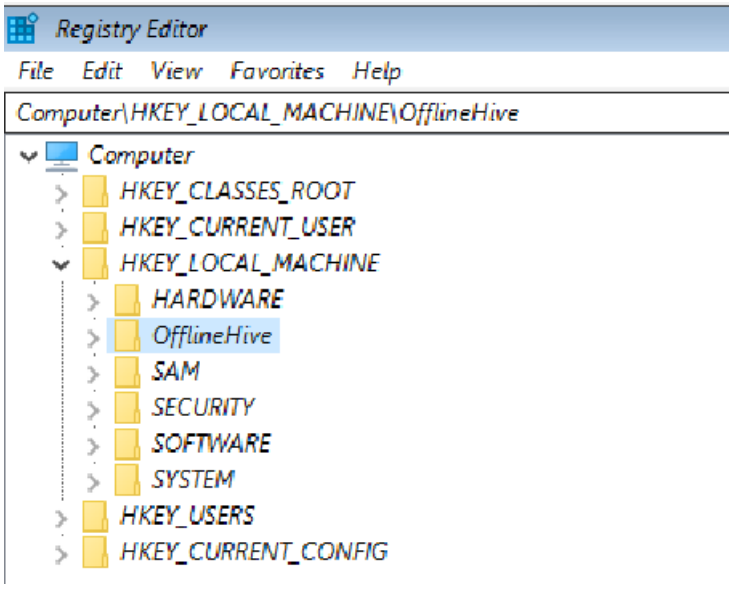
4. Wählen Sie **HKEY_LOCAL_MACHINE**aus, und wechseln Sie dann zu **Datei** > **Load Hive**.

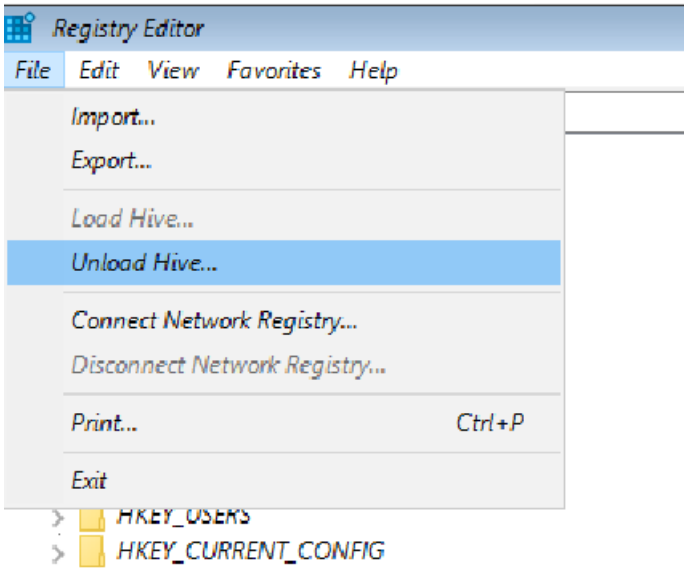
5. Navigieren Sie zu **OSdriveLetter: \ Windows\System32\config**, wählen Sie die Datei mit dem Namen **Komponente** (ohne Erweiterung) aus, und wählen Sie dann **Öffnen**aus. Wenn Sie dazu aufgefordert werden, geben Sie den Namen **OfflineComponentHive** für die neue Struktur ein.



6. Erweitern Sie **HKEY_LOCAL_MACHINE \offlinecomponenthive**, und überprüfen Sie, ob der **PendingXmlIdentifier** -Schlüssel vorhanden ist. Erstellen Sie eine Sicherungskopie des **OfflineComponentHive** -Schlüssels, und löschen Sie dann den **PendingXmlIdentifier** -Schlüssel.

7. Entladen Sie die Struktur. Markieren Sie dazu **OfflineComponentHive**, und wählen Sie dann **Datei** > aus, um die**Struktur zu entfernen**.





8. Wählen Sie **HKEY_LOCAL_MACHINE**aus, wechseln Sie zu **Datei** > **Load Hive**, navigieren Sie zu ** *OSdriveLetter* :\Windows\System32\config**, wählen Sie die Datei mit dem Namen **System** (ohne Erweiterung) aus, und wählen Sie dann **Öffnen** aus. Wenn Sie dazu aufgefordert werden, geben Sie den Namen **OfflineSystemHive** für die neue Struktur ein.

9. Erweitern Sie **HKEY_LOCAL_MACHINE \offlinesystemhive**, und wählen Sie dann die **Auswahl** Taste aus. Überprüfen Sie die Daten auf den **Standard** Wert.

10. Wenn die Daten in **HKEY_LOCAL_MACHINE \offlinesystemhive\select\default 1** sind, erweitern Sie **HKEY_LOCAL_MACHINE \offlinehive\controlset001**. Wenn es sich um **2**handelt, erweitern Sie **HKEY_LOCAL_MACHINE \offlinehive\controlset002**usw.

11. Erweitern Sie **Control\Session-Manager**. Überprüfen Sie, ob der **PendingFileRenameOperations** -Schlüssel vorhanden ist. Wenn dies der Fall ist, sichern Sie den **SessionManager** -Schlüssel, und löschen Sie dann den **PendingFileRenameOperations** -Schlüssel.

Überprüfen von wichtigen Starttreibern und-Diensten

Überprüfen von Diensten

1. Führen Sie die Schritte 1-10 im Abschnitt "Problembehandlung, wenn dieses Problem auftritt, nach einer Windows Update-Installation" aus. (Schritt 11 gilt nicht für dieses Verfahren.)

2. Erweitern Sie **Dienste**.

3. Stellen Sie sicher, dass die folgenden Registrierungsschlüssel unter **Dienste**vorhanden sind:

   - ACPI
   - Datenträger
   - VOLMGR
   - PARTMGR
   - VOLSNAP
   - Volumen

Wenn diese Schlüssel vorhanden sind, überprüfen Sie die einzelnen, um sicherzustellen, dass Sie einen Wert mit dem Namen " **Start** " und " **0**" festzulegen. Wenn dies nicht der Fall ist, setzen Sie den Wert auf **0**.

Wenn einer dieser Schlüssel nicht vorhanden ist, können Sie versuchen, die aktuelle Registrierungsstruktur zu ersetzen, indem Sie die Struktur von **RegBack**verwenden. Führen Sie dazu die folgenden Befehle aus:

```
cd OSdrive:\Windows\System32\config
ren SYSTEM SYSTEM.old
copy OSdrive:\Windows\System32\config\RegBack\SYSTEM OSdrive:\Windows\System32\config\
```

Überprüfen der oberen und unteren Filtertreiber

Überprüfen Sie, ob es sich um nicht-Microsoft-Filtertreiber auf dem Computer handelt, die auf einem anderen, ähnlichen Arbeitscomputer nicht vorhanden sind. Wenn Sie vorhanden sind, entfernen Sie die oberen und unteren Filtertreiber:

1. Erweitern Sie **HKEY_LOCAL_MACHINE \offlinehive\controlset001\control**.
2. Suchen Sie nach **UpperFilters** -oder **LowerFilters** -Einträgen.

> **NOTE**
>
> Diese Filter beziehen sich hauptsächlich auf Speicher. Nachdem Sie den **Steuerelement** Schlüssel in der Registrierung erweitert haben, können Sie nach **UpperFilters** und **LowerFilters**suchen.

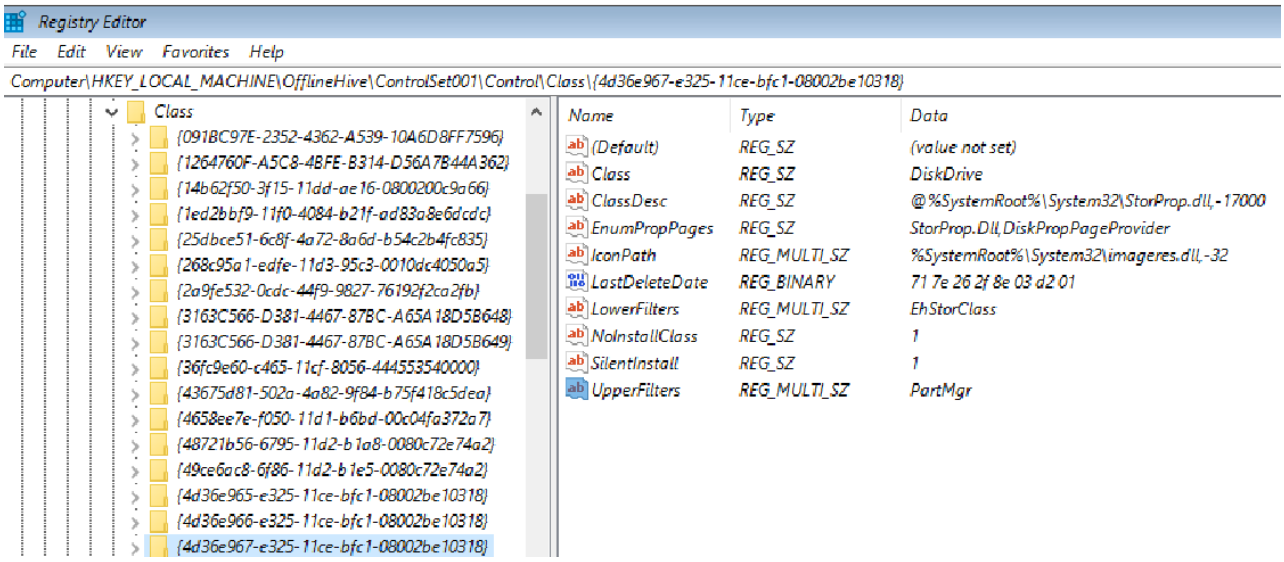
Im folgenden finden Sie einige der verschiedenen Registrierungseinträge, in denen Sie diese Filtertreiber finden können. Diese Einträge befinden sich unter **Controlset** und werden als **Standard** festgelegt:

\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}

\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}

\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}

\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}



Wenn ein **UpperFilters** -oder **LowerFilters** -Eintrag nicht standardmäßig ist (beispielsweise kein Windows-Standardfilter Treiber wie partmgr), entfernen Sie den Eintrag, indem Sie im rechten Bereich auf ihn doppelklicken und dann nur diesen Wert löschen.

> **NOTE**
>
> Es können mehrere Einträge vorhanden sein.

Der Grund dafür, dass diese Einträge uns beeinflussen können, liegt darin, dass ein Eintrag in der **Services** -Verzweigung vorhanden sein kann, bei dem ein Starttyp auf 0 oder 1 festgesetzt ist (der angibt, dass er beim Booten oder automatischen Teil des Startvorgangs geladen wird). Darüber hinaus ist entweder die Datei, auf die

verwiesen wird, nicht vorhanden oder beschädigt, oder Sie kann anders benannt werden als im Eintrag aufgeführt ist.

> **NOTE**
>
> Wenn tatsächlich ein Dienst vorhanden ist, der auf **0** oder **1** festgelegt ist, der einem **UpperFilters** -oder **LowerFilters** -Eintrag entspricht, wird durch das Festlegen des Diensts auf disabled in der **Dienste** -Registrierung (wie in den Schritten 2 und 3 des Abschnitts überprüfen von Diensten erläutert) ohne Entfernen des Eintrags des **Filter Treibers** der Computer abstürzen und ein 0x7B-Abbruchfehler generiert.

Ausführen von SFC und chkdsk

Wenn der Computer immer noch nicht gestartet wird, können Sie versuchen, einen **chkdisk** -Prozess auf dem Systemlaufwerk auszuführen und auch die Systemdateiprüfung auszuführen. Führen Sie dazu an einer WinRE-Eingabeaufforderung die folgenden Befehle aus:

- `chkdsk /f /r OsDrive:`

```
X:\Sources>chkdsk /f /r C:
The type of the file system is NTFS.

Stage 1: Examining basic file system structure ...
Progress: 20780 of 255744 done; Stage:  8%; Total:  0%; ETA:   5:07:15 ...
```

- `sfc /scannow /offbootdir=OsDrive:\ /offwindir=OsDrive:\Windows`

```
X:\Sources>sfc /scannow /offbootdir=F:\ /offwindir=C:\Windows

Beginning system scan.  This process will take some time.
```

Mobile Geräteverwaltung

31.12.2019 • 2 minutes to read

Windows10 bietet eine Enterprise-Management-Lösung, um IT-Experten dabei zu unterstützen, Unternehmenssicherheitsrichtlinien und Geschäftsanwendungen zu verwalten, wobei die Privatsphäre der Benutzer auf Ihren persönlichen Geräten nicht beeinträchtigt wird. Eine integrierte Verwaltungskomponente kann mit dem Verwaltungsserver kommunizieren.

Die Windows10-Verwaltungskomponente besteht aus zwei Teilen:

- Der Registrierungsclient, der das Gerät für die Kommunikation mit dem Enterprise Management-Server registriert und konfiguriert.
- Der Verwaltungsclient, der in regelmäßigen Abständen mit dem Verwaltungsserver synchronisiert, um nach Updates zu suchen und die neuesten von ihm gesetzten Richtlinien anzuwenden.

MDM-Server von Drittanbietern können Windows10 mithilfe des MDM-Protokolls verwalten. Der integrierte Verwaltungsclient kann mit einem Drittanbieter-Server Proxy kommunizieren, der die in diesem Dokument beschriebenen Protokolle zur Durchführung von Unternehmens Verwaltungsaufgaben unterstützt. Der Drittanbieterserver verfügt über die gleiche konsistente Benutzeroberfläche für die Registrierung, die für Windows10-Benutzer ebenfalls vereinfacht wird. MDM-Server müssen keinen Client zum Verwalten von Windows10 erstellen oder herunterladen. Details zu den MDM-Protokollen finden Sie unter \ [MS-MDM]: Mobile Device Management Protocol und \ [MS-MDE2]: Registrierungsprotokoll für mobile Geräte, Version 2.

MDM-Sicherheits Basisplan

Mit Windows 10, Version 1809, gibt Microsoft auch eine Microsoft MDM-Sicherheitsbasislinie frei, die wie die Microsoft GP-basierte Sicherheitsbasislinie funktioniert. Sie können diesen Basisplan problemlos in alle MDM-Komponenten integrieren, um die betrieblichen Anforderungen der IT-Experten zu unterstützen, wobei Sicherheitsbedenken für moderne, von der Cloud verwaltete Geräte berücksichtigt werden.

> **NOTE**
>
> Die Intune-Unterstützung für die MDM-Sicherheitsbasislinie wird in Kürze verfügbar sein.

Der MDM-Sicherheits Basisplan umfasst Richtlinien für die folgenden Bereiche:

- Microsoft Posteingangs-Sicherheitstechnologie (nicht als veraltet markiert) wie BitLocker, Windows Defender SmartScreen und DeviceGuard (Virtual-Based Security), ExploitGuard, Defender und Firewall
- Einschränken des Remotezugriffs auf Geräte
- Festlegen von Anmeldeinformationen für Kennwörter und Pins
- Einschränken der Verwendung von Legacy Technologien
- Legacy-Technologierichtlinien, die alternative Lösungen mit modernen Technologien anbieten
- Und vieles mehr

Weitere Informationen zu den in der MDM-Sicherheitsbasislinie definierten MDM-Richtlinien und den empfohlenen Baseline-Richtlinienwerten von Microsoft finden Sie unter:

- MDM-Sicherheits Basisplan für Windows 10, Version 1909
- MDM-Sicherheits Basisplan für Windows 10, Version 1903

- MDM-Sicherheits Basisplan für Windows 10, Version 1809

Informationen zu den MDM-Richtlinien, die in der Public Preview-Baseline für InTune-Sicherheit definiert sind, finden Sie unter Windows-Sicherheits Basisplan-Einstellungen für InTune

Informationen zum Migrieren zu MDM

Wenn eine Organisation zu MDM wechseln möchte, um Geräte zu verwalten, sollten Sie Ihre aktuellen Gruppenrichtlinieneinstellungen analysieren, um zu sehen, was Sie für den Übergang zur MDM-Verwaltung benötigen. Microsoft hat das MDM-Migrationsanalyse Tool (FMAT) erstellt, um zu helfen. FMAT legt fest, welche Gruppenrichtlinien für einen Zielbenutzer oder Computer festgelegt wurden, und generiert dann einen Bericht, in dem die Unterstützung für die einzelnen Richtlinieneinstellungen in den MDM-Entsprechungen aufgeführt ist. Weitere Informationen finden Sie unter FMAT-Anweisungen.

Informationen zur Geräteregistrierung

- Registrierung mobiler Geräte
- Registrierung von Geräten mit Verbundauthentifizierung
- Registrierung von Geräten mit Zertifikatauthentifizierung
- Registrierung von Geräten mit lokaler Authentifizierung

Informationen zur Geräteverwaltung

- Integration von Azure Active Directory in MDM
- Verwaltung von Unternehmens-Apps
- Verwaltung mobiler Geräte (MDM) für Geräteupdates
- Aktivieren Sie offline Upgrades auf Windows 10 für Windows Embedded 8.1 Handheld-Geräte
- OMA-DM-Protokollunterstützung
- Struktur der OMA-DM-Bereitstellungsdateien
- Serveranforderungen für OMA-DM
- Enterprise-Einstellungen, -Richtlinien und -App-Verwaltung

Informationen zu Konfigurationsdienst Anbietern

- Referenz zum Konfigurationsdienstanbieter
- In Windows10 unterstützte WMI-Anbieter
- Verwenden der PowerShell-Skripterstellung mit dem WMI-Bridge-Anbieter
- MDM-Bridge-WMI-Anbieter

Änderungsverlauf für die Clientverwaltung

11.02.2020 • 2 minutes to read

In diesem Thema sind neue und aktualisierte Themen in der Clientverwaltungs-Dokumentation für Windows 10 und Windows 10 Mobile aufgeführt.

2020. Februar

NEUES ODER GEÄNDERTES THEMA	BESCHREIBUNG
Der blaue Bildschirm tritt auf, wenn Sie den in-Box-Broadcom-NIC-Treiber aktualisieren.	Neu
Erweiterte Problembehandlung für Windows-Start	Aktualisiert

Dezember 2019

NEUES ODER GEÄNDERTES THEMA	BESCHREIBUNG
Ändern der standardmäßigen Entfernungsrichtlinie für externe Speichermedien in Windows 10, Version 1809	Neu
Erweiterte Problembehandlung für Windows-Start	Aktualisiert
Erweiterte Problembehandlung für die Ereignis-ID 41 "das System wurde neu gestartet, ohne dass es zuerst sauber heruntergefahren wurde"	Neu

Dezember 2018

NEUES ODER GEÄNDERTES THEMA	BESCHREIBUNG
Erweiterte Problembehandlung für TCP/IP	Neu
Sammeln von Daten mithilfe des Netzwerkmonitors	Neu
Problembehandlung für TCP/IP-Verbindung	Neu
Problembehandlung für Portmangel	Neu
Problembehandlung für Remote Procedure Call (RPC)-Fehler	Neu

November 2018

NEUES ODER GEÄNDERTES THEMA	BESCHREIBUNG
Erweiterte Problembehandlung für Windows-basierte Computer, die einfrieren	Neu

NEUES ODER GEÄNDERTES THEMA	BESCHREIBUNG
Erweiterte Problembehandlung für Stoppfehler und Bluescreens	Neu

VERSION: Windows10, Version 1709

Die Themen in dieser Bibliothek wurden für Windows10, Version 1709 (auch Fall Creators Update genannt), aktualisiert.

Juli 2017

NEUES ODER GEÄNDERTES THEMA	BESCHREIBUNG
Gruppenrichtlinieneinstellungen, die nur für Windows10 Enterprise und Windows10 Education gelten	Die Startlayout-Richtlinieneinstellung kann jetzt auf Windows10 Pro, Version 1703, angewendet werden.

Juni 2017

NEUES ODER GEÄNDERTES THEMA	BESCHREIBUNG
Erstellen erforderlicher Benutzerprofile	Windows10, Version 1703, wurde zur Profilerweiterungstabelle hinzugefügt.

April2017

NEUES ODER GEÄNDERTES THEMA	BESCHREIBUNG
Neue Richtlinien für Windows 10	Eine Liste der neuen Gruppenrichtlinieneinstellungen für Windows10, Version 1703 wurde hinzugefügt

VERSION: Windows10, Version 1703

Die Themen in dieser Bibliothek wurden für Windows10, Version 1703 (auch Creators Update genannt), aktualisiert. Das folgende neue Thema wurde hinzugefügt:

- Verwalten der Einstellungs-App mit Gruppenrichtlinien