

Einstellung	Beschreibung	Default-Wert	Beispiel
backupWrite	<p>Diese Einstellung legt fest, ob der Agent das Schreiben von Berechtigungen im sogenannten Backup-Operator-Mode durchführt. Es werden in diesem Fall beim Zugriff keine Berechtigungsprüfungen durch Windows durchgeführt.</p> <p> Um diese Einstellung verwenden zu können, muss das Dienstkonto mit dem der tenfold Agent ausgeführt wird über die Berechtigung "Sicherungs-Operatoren" verfügen.</p>	false	true / false
scanSharepointFiles	Legt fest, ob für SharePoint einzelne Dokumente eingescannt werden sollen oder ob einzelne Dokumente beim Scan ausgelassen werden.	false	true / false
usePowershellScripts	<p>Diese Einstellung legt das Verhalten beim Scan von Exchange-Mailboxen fest.</p> <p> Aus Performancegründen wird in großen Exchange-Umgebungen empfohlen, diesen Wert auf "true" zu setzen.</p>	false	true / false
ewsPoolSize	Legt fest, wie viele EWS (Exchange® Web Services) Verbindungen für Scan-Vorgänge gleichzeitig zur Verfügung stehen	100	1-500
powershellMinPoolSize	Legt fest, wie viele parallele PowerShell Verbindungen mindestens durch diesen Agent zur Verfügung gestellt werden sollen	15	1-100
powershellMaxPoolSize	Legt fest, wie viele parallele PowerShell Verbindungen maximal durch diesen Agent zur Verfügung gestellt werden sollen	25	1-100
powershellOutOfProcesses	<p>Legt fest, ob der Powershellaufruf des PowershellServices in einem neuen Prozess gestartet werden soll</p> <p> Ist der Wert auf "false" gesetzt, werden die Einstellungen "powershellMajorVersion" und "powershellMinorVersion" ignoriert</p>	false	true / false
powershellMajorVersion	<p>Legt die Hauptversion der erstellten Powershellinstanz des PowershellServices fest. Die festgelegte Version muss auf dem lokalen Rechner installiert sein</p> <p> Dieser Wert wird nur beachtet wenn der Wert hinter "powershellOutOfProcess" auf "true" gesetzt ist</p>	3	3

Einstellung	Beschreibung	Default-Wert	Beispiel
powershellMinorVersion	Legt die Nebenversion der erstellen Powershellinstanz des PowerShellServices fest. Die festgelegte Version muss auf dem lokalen Rechner installiert sein  Dieser Wert wird nur beachtet wenn der Wert hinter "powershellOutOfProcess" auf "true" gesetzt ist	0	0
pathScanDurationDepth	Diese Einstellung legt fest bis zu welcher Ordertiefe, Logausgaben über die Scandauer eines Ordners geschrieben werden. Der Wert 0 deaktiviert diese Funktion	0	0-100
stompClientSize	Diese Einstellung legt die Anzahl der Verbindungen zu tenfold fest. Diese Einstellung wird bei Scans von NTFS, Exchange und Sharepoint verwendet.  Ist die zu scannende Umgebung sehr schnell, wie eine lokale SSD mit NTFS-Dateisystem, empfiehlt sich die Anzahl der Verbindungen zu erhöhen, damit mehrere Threads gleichzeitig Nachrichten an tenfold senden können	20	1-100

Kommunikationseinstellungen

Der tenfold Agent muss mit dem tenfold Applikationsserver kommunizieren. Dies geschieht über SOAP-Webservice für alle Anfragen vom Applikationsserver zum Agent und mit STOMP (für high performance queueing) für alle Antworten vom Agent für den Applikationsserver. Im tenfold Agent können Sie den Port festlegen, auf welchem der tenfold Agent auf Anfragen wartet. Die Defaulteinstellung ist TCP-Port 8000. Um diese Einstellung zu ändern, muss die Konfigurationsdatei an allen relevanten Punkten angepasst werden:

- in allen <add baseAdress> Anweisungen nach dem "*:"
- in der <add scheme> Anweisung über den Parameter "port"

STOMP

Der Port für die STOMP-Konfiguration für die Antworten für tenfold muss auf Seite des Applikationsservers angepasst werden.

Funktionen

In der Konfiguration kann hinterlegt werden, welche der folgenden Funktionen der Agent zur Verfügung stellt:

- NTFSSecure: Funktionalität für Fileserver (Lesen/Schreiben von Ordnern und Berechtigungen)
- Powershell: Bereitstellung der Ausführung von PowerShell Skripts über diesen Agent
- LocalSystem: Funktion zum Auslesen von lokalen Benutzern und Gruppen auf diesem System
- Exchange: Funktionalität für Exchange (Lesen von Mailboxen, Ordnern und Berechtigungen)

- Sharepoint: Funktionalität für SharePoint (Lesen von Sites, Listen und Items und deren Berechtigungen)

Um eine Funktion zu deaktivieren, muss der jeweilige <service> Eintrag deaktiviert werden. Es bietet sich an, den Eintrag nicht zu löschen, sondern lediglich per Kommentar zu deaktivieren. In XML wird alles, was sich zwischen den Zeichenketten <!-- und --> befindet als Kommentar gewertet. Die folgenden Beispiele zeigen den Unterschied zwischen einer aktivierten und einer deaktivierten Funktion:

Aktivierter Eintrag

```
<service name="NTFSSecure" behaviorConfiguration="MSIA_Secure_Behavior">
  <host>
    <baseAddresses>
      <add baseAddress="https://*:8000/MSIA/NTFSSecure"/> (see page 199)
    </baseAddresses>
  </host>
  <endpoint address="" binding="basicHttpBinding"
    bindingConfiguration="basicBindingConfig" contract="MSIA.ENTFSSecure"
    name="ntfsBindingConfig" bindingNamespace="http://NTFS"/> (see page 199)
    <endpoint address="mex" binding="mexHttpsBinding"
      contract="IMetadataExchange"/>
  </service>
```

Deaktivierter Eintrag

```
<!--
<service name="NTFSSecure" behaviorConfiguration="MSIA_Secure_Behavior">
  [... Inhalt wie oben ...]
</service>
-->
```

Was sollte man aktivieren und was nicht?

Es sollten alle Funktionen, die nicht unmittelbar benötigt werden aus Sicherheitsgründen deaktiviert werden. Für die Einrichtung der Fileserver werden in jedem Fall die Funktionen "NTFSSecure" und "LocalSystem" benötigt. In Multi-Domain-Umgebungen ist zusätzlich die Funktion "Powershell" zwingend erforderlich

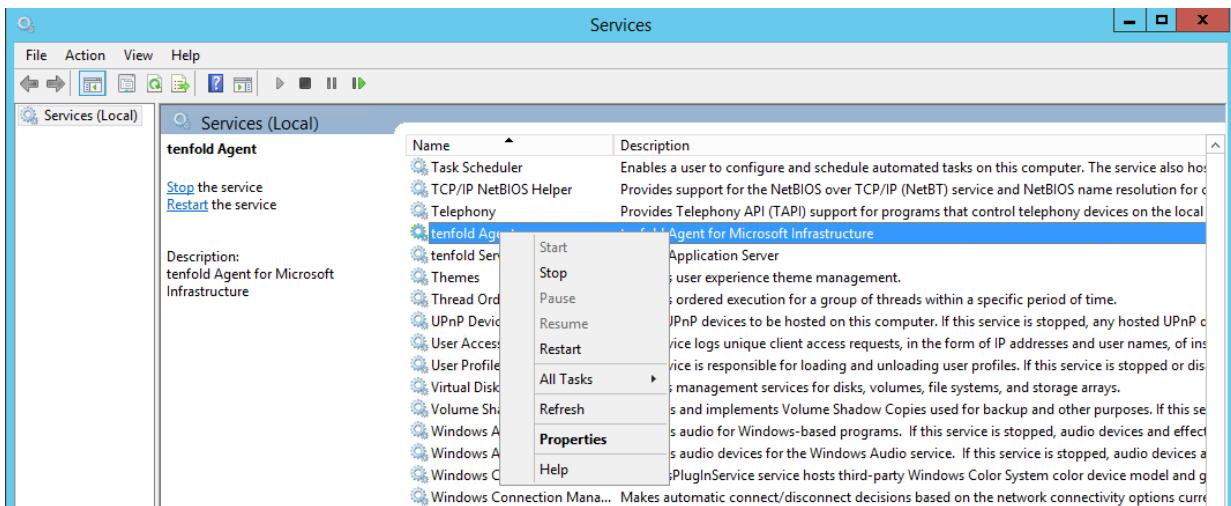
Wenn Sie in der Konfiguration Änderungen vorgenommen haben, müssen Sie den tenfold Agent neu starten.

Starten / Stoppen

Um den Agent zu starten, wechseln Sie in die Windows-Dienstverwaltung (Systemsteuerung > Verwaltung > Dienste) und suchen Sie den Eintrag "tenfold Agent".

- Klicken Sie mit der rechten Maustaste auf den Eintrag und wählen Sie "Start", um den Dienst zu starten.
- Um den Dienst wieder zu stoppen, klicken Sie erneut auf den Eintrag und wählen die Option "Stoppen"

- Alternativ wählen Sie Option "Neu starten" um den Agent in einem Durchgang zu stoppen und zu starten.



Agent in tenfold einbinden

Nachdem der Agent installiert wurde, muss dieser noch in tenfold registriert werden. Für dies und weitere Einstellungen des Agenten innerhalb von tenfold, siehe [tenfold Agenten](#)(see page 619).

7.1.3 WMI-Remotezugriff

Der WMI-Remotezugriff dient dazu, dass der tenfold Agent lokale Gruppen, Benutzer und Gruppenmitglieder von Remote PCs einlesen kann.

Voraussetzungen

Beschreibung	Wo?
Administrator-Berechtigung	PC auf dem der MSIA läuft
Administrator-Berechtigung	PC auf dem die Lokalen Berechtigungen ausgelesen werden sollen
Domainbenutzer mit Administrativen Berechtigungen	

PowerShell-Testscript zur Überprüfung ob die Berechtigungen richtig eingestellt sind:

PowershellScript

```
PS C:\Users\Administrator> Get-WmiObject -Class Win32_UserAccount -Namespace "root\cimv2" -Filter "LocalAccount='$True'" -ComputerName <PC-NAME> -ErrorAction Stop
```

Vorgehensweise

Konfigurieren der Firewall über die Befehlszeile

- Öffnen sie ein Befehlsfenster auf dem Computer auf den sie zugreifen wollen.

2. Geben Sie folgenden Befehl ein:
netsh firewall set service remoteadmin enable
3. Mit diesem Befehl wird die Remoteverwaltungsausnahme aktiviert. Testen Sie nun mit dem Oben angegeben Script von einem anderen PC ob die Aktivierung Funktioniert hat.

Konfigurieren der Firewall mithilfe von Gruppenrichtlinien

1. Start -> Ausführen -> gpmc.msc als Administrator ausführen auf dem Domänen-Controller
2. Auf gewünschte OU rechtsklicken -> neues Gruppenrichtlinienobjekt erstellen
3. Rechtsklick auf das eben erstellte Gruppenrichtlinienobjekt und Bearbeiten klicken
4. Richtlinien -> Administrative Vorlagen -> Netzwerk -> Netzwerkverbindungen -> Windows-Firewall -> Domänenprofil
5. Rechtsklick auf "Windows-Firewall: Eingehende RemoteVerwaltungsausnahmen zulassen -> Bearbeiten
6. Aktiviert anklicken und bei Optionen * (für alle Zugriffe) oder eine Subnetzmaske für Zugriffe aus diesem Subnetz

Alles speichern und auf dem Zielcomputer folgendes ausführen um die Gruppenrichtlinien zu erneuern.

GpUpdate

```
gpupdate /force
```

Danach kann wieder mittels dem oberen PowershellScript die Einstellung getestet werden.

[WMI-Remotezugriff\(see page 204\)](#)

7.1.4 Berechtigungsstufen

Allgemein

Berechtigungsstufen definieren, welche Art von Berechtigung ein Benutzer auf eine bestimmte Ressource - im Kontext der Microsoft-Systeme - zugeordnet hat (Lesen, Ändern, Vollzugriff und ähnliche). Diese Berechtigungsstufen existieren für folgende Systeme:

- Fileserver
- Exchange Server
- SharePoint Server

Aktuell ist es nur möglich, die Berechtigungsstufen für Fileserver anzuzeigen und zu bearbeiten. Die Verwaltung ist über das Menü erreichbar unter *Berechtigungen > Fileservergruppen > Berechtigungsstufen*.

Anzeige

Kurzname	Name	Suffix	Zuordnungen	Self-Service erlauben
LST	Ordnerinhalt anzeigen	lst	7	-
RX	Lesen & Ausführen	rx	7	✓
MD	Ändern	md	14	-
MX	Ändern Plus	mx	13	✓
FC	Vollzugriff	fc	18	-
S	Spezielle	spo	0	-

Die Listenansicht zeigt alle Berechtigungsstufen an, die in tenfold hinterlegt sind. Im Auslieferungszustand sind dies folgende:

- Ordnerinhalt anzeigen
- Lesen & Ausführen
- Ändern
- Ändern Plus (tenfold-spezifische Berechtigungsstufe)
- Vollzugriff
- Spezielle

Diese vordefinierten Stufen können lediglich angezeigt oder bearbeitet, aber nicht gelöscht werden.

Ändern Plus

Alle Berechtigungsstufen mit Ausnahme von "Ändern Plus" entsprechen den jeweiligen Berechtigungsstufen, die auch in Windows vordefiniert sind. "Ändern Plus" entspricht grundsätzlich "Ändern", mit der einzigen Abweichung, dass die Berechtigung "Modify" nicht gesetzt ist. Dies verhindert, dass Benutzer mit einer unbeabsichtigten Mausbewegung im Explorer aus Versehen einen Ordner an einen unbekannten Ort verschieben.

Bearbeitung

Bearbeitung nicht möglich

Seit der Version tenfold 2019 R4 ist die Bearbeitung und Erstellung von Berechtigungsstufen nicht mehr möglich.

7.1.5 Fileserver-Berechtigungsgruppen

Allgemeines

Benötigte Berechtigung

Um die Konfiguration der Berechtigungsgruppen vorzunehmen, ist die Systemberechtigung "Resource Group Configuration Administration" (8091) erforderlich.

Werden mit tenfold Berechtigungen auf Fileserver / Verzeichnisse gesetzt, so werden diese Berechtigungen ausschließlich nach den Best Practices von Microsoft gesetzt. Das bedeutet, dass je Verzeichnis und Berechtigungsstufe entsprechende Gruppenstrukturen angelegt werden (welche genau, hängt von der Konfiguration ab). Für eine allgemeine Beschreibung der Best Practices (AGDLP-Prinzip) siehe [AGDLP bei Wikipedia](#)⁵. Um die Konfiguration festzulegen, wechseln Sie im Menü zu Windows > Fileservergruppen. Es können eine oder mehrere Konfigurationen hinterlegt werden, welche dann in den konfigurierten Windows Domains verwendet werden können. Eine Konfiguration kann in mehreren Domains verwendet werden und jeder Domain ist genau eine Konfiguration zugeordnet.

Scope

Die Konfiguration steuert den strukturellen Aufbau der Gruppen sowie die Namenskonvention. Die Organisationseinheiten, in denen die Gruppen abgelegt werden, werden jedoch bei den Einstellungen zur Domain konfiguriert ([Einrichten einer Windows Domain](#)(see page 196)).

Anlegen einer neuen Konfiguration

Um eine neue Konfiguration anzulegen, klicken Sie auf die Schaltfläche "Hinzufügen" und nehmen Sie anschließend die nachstehende Einstellungen vor.

Namenskonvention

Die Namenskonvention innerhalb einer Konfiguration gibt an, wie Gruppen, die von tenfold zur Berechtigungsvergabe angelegt werden, benannt werden sollen. Es ist dabei möglich den Namen aus mehreren Bestandteilen zusammenzusetzen. Die Einstellung erfolgt im rechten Bereich in der Liste "Bestandteile". Die Reihenfolge kann dabei über die Schaltflächen "Aufwärts" und Abwärts" frei gewählt werden.

Folgende Bestandteile stehen zur Verfügung, welche zum Teil direkt auf der Maske zu konfigurieren sind:

- Präfix: Das Präfix wird je Konfiguration festgelegt. Das gewünschte Präfix wird in das Textfeld "Präfix" eingegeben.
- Server: Repräsentiert das, bei der betroffenen Freigabe, auf dem sich das Verzeichnis befindet, hinterlegte Feld "Servername"
- Freigabe: Repräsentiert das, bei der betroffenen Freigabe, auf dem sich das Verzeichnis befindet, hinterlegte Feld "Freigabename"

⁵ <https://en.wikipedia.org/wiki/AGDLP>

- Verzeichnis: Repräsentiert den gesamten Pfadnamen des betroffenen Verzeichnisses ab der Freigabe; Unterverzeichnisse werden dabei durch das gewählte Trennzeichen getrennt (z.B. Folder1\Folder2\Folder3 mit Trennzeichen "Unterstrich" wird zu Folder1_Folder2_Folder3)
- Gruppenbereich: Repräsentiert die Bezeichnung des jeweiligen Gruppentyps (global, lokal, universal). Die gewünschten Bezeichnungen (Abkürzungen) werden in den Textfeldern "Bez. lokale Gruppe", "Bez. globale Gruppe" und "Bez. universale Gruppe" festgelegt.
- Suffix: Es handelt sich hierbei um das Suffix der jeweiligen Berechtigungsstufe (Lesen & Ausführen, Ändern, etc.), für welche die Gruppe angelegt wird. Das Suffix für die jeweilige Berechtigungsstufe kann auf der Maske "[Berechtigungsstufen\(see page 205\)](#)" geändert werden.

Strukturkonfiguration

Die wesentliche Einstellung zur Struktur der Gruppen wird über den RBAC-Modus festgelegt. Der RBAC-Modus definiert, welcher Gruppentyp oder Gruppentypen bei der Berechtigungsvergabe angelegt werden. Es stehen hierbei folgende Optionen zur Verfügung, welche anschließend kurz erklärt werden.

Single- vs. Multi-Domain

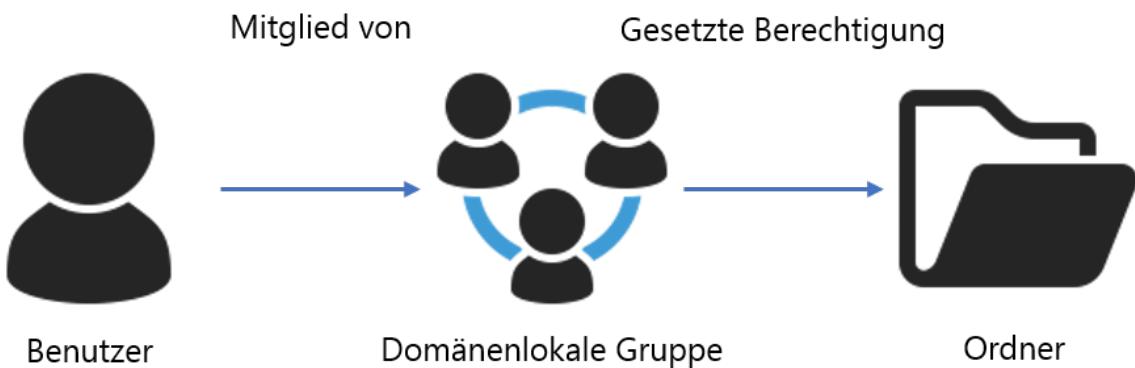
Nicht alle RBAC-Modi sind für jede Umgebung geeignet:

Der Modus "AGGP/AGP" kann nur in Single-Domain Umgebungen genutzt werden. Der Modus "AGDLP - Benutzer in globaler Gruppe" sollte nur in Multi-Domain-Umgebungen verwendet werden.

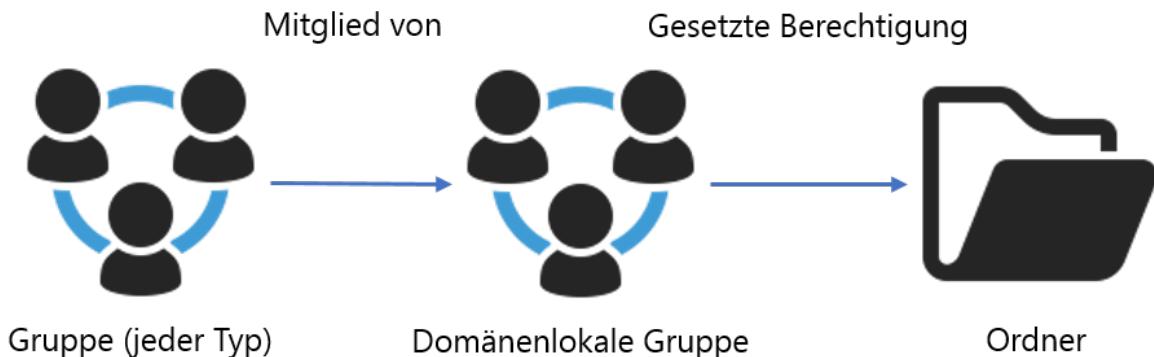
AGDLP - Benutzer in domänenlokaler Gruppe

- Es wird eine domänenlokale Gruppe als Berechtigungsgruppe in der Domain des Fileservers angelegt. Diese Gruppe wird in die ACL des Dateisystems eingetragen.
- Berechtigte Benutzer aus jeglichen Domains werden als direkte Mitglieder der Berechtigungsgruppe aufgenommen
- Berechtigte Gruppen jeglichen Typs aus jeglicher Domain werden als direkte Mitglieder der Berechtigungsgruppe aufgenommen

Für berechtigte Benutzer sieht der Aufbau folgendermaßen aus:



Für berechtigte Gruppen sieht der Aufbau folgendermaßen aus:



AGDLP - Benutzer in globaler Gruppe

- Es wird eine domänenlokale Gruppe als Berechtigungsgruppe in der Domain des Fileservers angelegt.
Diese Gruppe wird in die ACL des Dateisystems eingetragen.

Die restliche Verarbeitung hängt davon ab, ob das zu berechtigende Objekt ein Benutzer oder eine Gruppe ist.

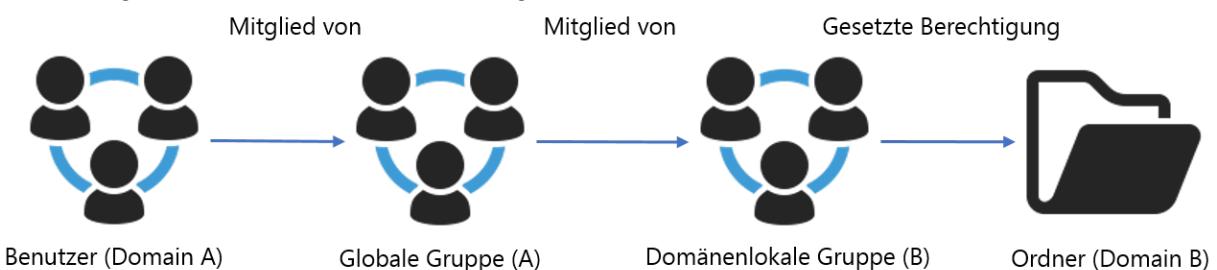
Für Benutzer:

- Es wird eine globale Gruppe in der Domain des berechtigten Benutzers angelegt
- Diese Gruppe wird als Mitglied der domänenlokalen Fileservergruppe aufgenommen.
- Berechtigte Benutzer werden als direkte Mitglieder der globalen Gruppe in ihrer eigenen Domain aufgenommen.

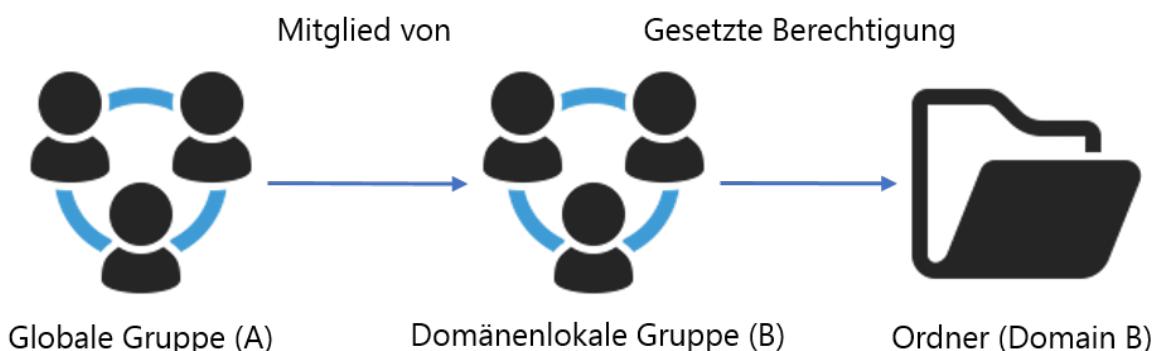
Für Gruppen:

- Die zu berechtigende Gruppe wird direkt als Mitglied der domänenlokalen Fileservergruppe aufgenommen
- Achtung: Es wird keine separate globale Gruppe in der Domain der zu berechtigenden Gruppe angelegt

Für berechtigte Benutzer sieht der Aufbau folgendermaßen aus:



Für berechtigte Gruppen sieht der Aufbau folgendermaßen aus:



AGUP/AUP

- Es wird eine universale Gruppe als Berechtigungsgruppe in der Domain des Fileservers angelegt. Diese Gruppe wird in die ACL des Dateisystems eingetragen.
- Berechtigte Benutzer aus jeglichen Domains werden als direkte Mitglieder der Berechtigungsgruppe aufgenommen
- Berechtigte Gruppen jeglichen Typs aus jeglicher Domain werden als direkte Mitglieder der Berechtigungsgruppe aufgenommen

Aufbau

Der Aufbau der Gruppen ist analog zum Modus "AGDLP - Benutzer in domänenlokaler Gruppe" - lediglich der Gruppentyp ändert sich auf "Universal".

AGGP/AGP

- Es wird eine globale Gruppe als Berechtigungsgruppe in der Domain des Fileservers angelegt. Diese Gruppe wird in die ACL des Dateisystems eingetragen.
- Berechtigte Benutzer werden als direkte Mitglieder der Berechtigungsgruppe aufgenommen (es können nur Benutzer aus der gleichen Domain berechtigt werden)
- Berechtigte Gruppen jeglichen Typs aus jeglicher Domain werden als direkte Mitglieder der Berechtigungsgruppe aufgenommen

Aufbau

Der Aufbau der Gruppen ist analog zum Modus "AGDLP - Benutzer in domänenlokaler Gruppe" - lediglich der Gruppentyp ändert sich auf "Global".

Multi-Domain

Dieser Modus ist nicht für Multi-Domain-Umgebungen geeignet, da Benutzer aus anderen Domains nicht Mitglied der globalen Berechtigungsgruppen werden können, welche auf dem Fileserver gesetzt wurden.

Konfiguration in einer Domäne verwenden

Einstellen der Konfiguration

Nachdem Sie die Konfiguration abgeschlossen haben, können Sie diese in den konfigurierten Domains verwenden:

- Öffnen Sie die Konfiguration für die jeweilige Domain und wechseln zum Karteireiter "Fileserver" ([Einrichten einer Windows Domain\(see page 196\)](#)).
- Wählen Sie unter dem Punkt "Fileservergruppen" die gewünschte Konfigurationseinstellung aus.

Änderungen

Achtung: Es ist absolut nicht empfohlen, diese Einstellung nachträglich zu ändern, sobald auf dem betroffenen Fileserver bereits Änderungen durch tenfold durchgeführt wurden, und somit entsprechende Gruppen angelegt wurden. Das System verhindert das Ändern der Einstellung nicht aktiv, eine Änderung darf allerdings nur nach entsprechender Prüfung und von Personen mit entsprechendem technischen Know-How erfolgen.

Konfiguration der Organisationseinheiten

Um die Konfiguration zu vervollständigen, muss noch festgelegt werden, in welchen Organisationseinheiten im Active Directory die von tenfold generierten Gruppen gespeichert werden sollen. Diese Konfiguration ist mehrstufig. Folgende Einstellungen können, abhängig vom gewählten RBAC-Modus, getroffen werden.

Domainweite Einstellung der OE für Berechtigungsgruppen von Fileservern aus der Domain

Im einfachsten Fall wird für eine gesamte Domain eine OE festgelegt, in welcher alle Berechtigungsgruppen abgelegt werden. Diese Einstellung wird am Karteireiter "Organisationseinheit-Konfiguration" im Feld "OU für Fileservergruppen" eingestellt. Diese Einstellung gilt grundsätzlich für die gesamte Domain.

Freigabespezifische Einstellung der OE für Berechtigungsgruppen der betreffenden Freigabe

Ist es nicht gewünscht, dass alle Gruppen in der gleichen OE abgelegt werden, so kann je Freigabe eine alternative OE definiert werden. Diese dient als Ablageort für alle Gruppen die für Verzeichnisse unter der betreffenden Freigabe angelegt werden. Um eine freigabespezifische Einstellung festzulegen, muss auf der Maske zur Konfiguration der Freigabe (siehe [Einrichtung der Fileserver](#)(see page 223)) die Einstellung "Organisationseinheit für Fileservergruppen" von "Übernehmen" auf "Überschreiben" umgestellt werden. Anschließend kann die gewünschte, freigabespezifische OE im Textfeld "DN" festgelegt werden.

Spezielle Einstellungen für den Modus "AGDLP - Benutzer in globaler Gruppe"

Diese folgenden Einstellungen sind nur verfügbar, wenn der RBAC-Modus der für die Domain hinterlegten Konfiguration "AGDLP - Benutzer in globaler Gruppe" ist.

Multi-Domain

Diese Einstellung ist nur für Multi-Domain-Umgebungen sinnvoll.

In diesem Fall ist es möglich, nicht zur festzulegen, in welcher OE die domänenlokal Berechtigungsgruppen für die Fileserver aus dieser Domain abgelegt werden sollen. Es ist darüber hinaus möglich festzulegen, in welcher OE der anderen Domains die entsprechenden globalen Gruppen angelegt werden sollen, in welche die Benutzer als Mitglieder aufgenommen werden. Es steht hierbei für jede Domain ein Karteireiter zur Verfügung, in der entweder die domainweite Einstellung der Domain übernommen werden kann (default), oder ob eine andere OE als Ablageort definiert werden soll.

Bearbeiten einer Konfiguration

Um eine bestehende Konfiguration zu bearbeiten, wechseln Sie im Menü zu Windows > Fileservergruppen. Anschließend wählen Sie in der Tabelle die entsprechende Konfiguration aus und wählen den Punkt "Bearbeiten" im Aktionsmenü.

Änderungen

Achtung: Es ist absolut nicht empfohlen, eine Konfiguration nachträglich zu ändern, sobald diese in einer Domain konfiguriert wurde, und auf einem der Fileserver der Domain Änderungen durch tenfold durchgeführt wurden, und somit entsprechende Gruppen angelegt wurden. Das System verhindert das Ändern der Einstellung nicht aktiv, eine Änderung darf allerdings nur nach entsprechender Prüfung und von Personen mit entsprechendem technischen Know-How erfolgen.

Löschen einer Konfiguration

Um eine bestehende Konfiguration zu löschen, wechseln Sie im Menü zu Windows > Fileservergruppen. Anschließend wählen Sie in der Tabelle die entsprechende Konfiguration aus und wählen den Punkt "Löschen" im Aktionsmenü.

Löschen von genutzten Konfigurationen

Eine Konfiguration kann nur gelöscht werden, wenn sie aktuell nicht in einer der konfigurierten Domains eingestellt ist. Versuchen Sie eine genutzte Konfiguration zu löschen, erhalten Sie eine entsprechende Warnmeldung. In diesem Fall müssen Sie die Einstellung bei allen Domains auf eine andere Konfiguration ändern. Anschließend können Sie die Konfiguration löschen. Beachten Sie jedoch unbedingt die Hinweise oberhalb betreffend Konfigurationsänderungen.

7.1.6 Exchange-Berechtigungsgruppen

Allgemeines

Benötigte Berechtigung

Um die Konfiguration der Berechtigungsgruppen vorzunehmen, ist die Systemberechtigung "Resource Group Configuration Administration" (8091) erforderlich.

Berechtigungen auf dem Exchange-Server werden genauso wie Berechtigungen auf dem Fileserver nach den Best-Practices von Microsoft gesetzt (siehe [Fileserver-Berechtigungsgruppen\(see page 207\)](#)). Analog zu den Fileserver-Berechtigungsgruppen müssen daher auch für Exchange-Berechtigungsgruppen Namensschemen definiert werden, welcher zur Anlage von Berechtigungsgruppen benutzt werden.

Die Einstellungen zu den Konfigurationen finden Sie im Menü unter Berechtigungen > Exchange-Gruppen > Einstellungen.

Scope

Die folgenden Einstellungen steuern lediglich wie die Namen der erstellten Gruppen erzeugt werden. Die Einstellung in welcher OU im Active Directory die erzeugten Gruppen abgelegt werden, treffen Sie in den Domäneninstellungen ([Einrichten einer Windows Domain\(see page 196\)](#)).

Anlegen einer neuen Konfiguration

Um eine neue Konfiguration anzulegen, klicken Sie auf die Schaltfläche "Neu" und nehmen Sie anschließend die nachstehende Einstellungen vor:

Die Einstellungen in den Bereichen "Mailbox" und "Verzeichnis" sind identisch. Die Einstellungen unter "Mailbox" werden verwendet um Gruppennamen für Postfachberechtigungen zu erzeugen, die Einstellungen unter "Verzeichnis" hingegen werden Benutzt um Gruppennamen für Berechtigungen auf Postfachverzeichnissen zu erzeugen.

Einstellung	Beschreibung
Bereich "Allgemein"	
Name	Der Name unter welchem diese Konfiguration in tenfold aufzufinden ist.
Bereich "Mailbox" und "Verzeichnis"	
Berechtigungsmodus	Stellt ein ob bei der Berechtigung eines Benutzers eine Gruppe erzeugt werden soll oder der Benutzer direkt auf dem Postfach berechtigt werden soll.
Präfix	Diese Einstellung ist nur ersichtlich wenn unter den Bestandteilen die Option "Prefix" ausgewählt wurde. Dies ist eine feste Zeichenkette, welche am Beginn jedes Gruppennamens vorangestellt werden kann.
Trennzeichen	Eine Auswahl aus verschiedenen Trennzeichen, mit welchem die einzelnen Namensbestandteile, der Gruppen für Postfächer, voneinander getrennt werden.
Aus Exchange Global Address List entfernen	Wenn ausgewählt, bewirkt diese Einstellung, dass nach der Anlage der Gruppe, diese aus dem globalen Adressbuch von Exchange entfernt wird.

Mailbox-Bestandteil	Mit dieser Einstellung wird ausgewählt, welches Attribut des Postfaches, zur Erzeugung des Gruppennamens, für den Bestandteil "Mailbox" herangezogen wird. Die
Bestandteile	Hier können Sie Konfigurieren welche Bestandteile der Name der erzeugten Gruppe enthalten soll und in welcher Reihenfolge diese erscheinen.

Bearbeiten einer Konfiguration

Um eine bestehende Konfiguration zu bearbeiten, wechseln Sie im Menü zu Berechtigungen > Exchange-Gruppen. Anschließend wählen Sie in der Tabelle die entsprechende Konfiguration aus und wählen den Punkt "Bearbeiten" im Aktionsmenü.

Änderung der Namen

Eine Änderung der Konfiguration für die Namensschemen bewirkt nur, wie **zukünftig** erzeugte Gruppen benannt werden. Bereits bestehende Gruppen werden **nicht** umbenannt.

Löschen einer Konfiguration

Um eine bestehende Konfiguration zu löschen, wechseln Sie im Menü zu Berechtigungen > Exchange-Gruppen. Anschließend wählen Sie in der Tabelle die entsprechende Konfiguration aus und wählen den Punkt "Löschen" im Aktionsmenü.

Löschen von genutzten Konfigurationen

Eine Konfiguration kann nur gelöscht werden, wenn sie aktuell nicht in einer der konfigurierten Domains eingestellt ist. Versuchen Sie eine genutzte Konfiguration zu löschen, erhalten Sie eine entsprechende Warnmeldung. In diesem Fall müssen Sie die Einstellung bei allen Domains auf eine andere Konfiguration ändern. Anschließend können Sie die Konfiguration löschen. Beachten Sie jedoch unbedingt die Hinweise oberhalb betreffend Konfigurationsänderungen.

Anzeige bestehender Berechtigungsgruppen

Benötigte Berechtigung

Für die Anzeige wird die Berechtigung "View Exchange Groups" (8332) benötigt.

Auf der Maske "Verwendete Exchange-Gruppen", welche Sie über das Menü unter *Berechtigungen > Berechtigungsgruppen > Exchange> Verwendung* erreichen, können Sie sich anzeigen lassen, welche Berechtigungsgruppen bereits unter tenfold registriert sind.

The screenshot shows a table with the following columns:

Name	Vollzugriff	Senden als	Senden im Auftrag von	Externer Zugang	Objekt löschen	Berechtigungen anzeigen	Berechtigungen ändern	Besitzer ändern	Empfangen als	Bearbeiter
Bayer, Otto	Charlie Exchange_rr uder_fa									
Decker, Eric	Charlie Exchange_e decker_fa									
Grunewald, Michael	Exchange Charlie_G runewald Michael_fa									
IPM_SUBTREE\Multi SubFolders\Public Folder 1										Charlie Exchange_P Fc22d8c7edd...Su bfolders_Public Fol der 1_ed
Peter, Max		Exchange_Peter Ma x_sob				Exchange_Peter Ma x_cp				
Ruder, Rudi			Charlie Exchange_rr uder_ea	Charlie Exchange_rr uder_di	Charlie Exchange_rr uder_rp	Charlie Exchange_rr uder_cp	Charlie Exchange_rr uder_co	Charlie Exchange_rr uder_ra		
Shared Info Mailbox	Exchange Charlie_S hared Info Mailbox_ fa	Exchange Charlie_S hared Info Mailbox_ sa	Exchange Charlie_S hared Info Mailbox_ sob		Exchange Charlie_S hared Info Mailbox_ di					

Im Bereich "Filter" haben Sie die Möglichkeit, nur Berechtigungsgruppen eines bestimmten Exchange-Servers anzuzeigen. Mit der Auswahl "*" werden alle Gruppen angezeigt. Die verwendeten Gruppen werden Ihnen hierbei in einer Matrix angezeigt, wobei die Zeilen die einzelnen Exchange-Items darstellen und die Spalten die Berechtigungen.

Leere Anzeige

Beim Betreten der Maske werden noch keine Gruppen angezeigt. Die Gruppen werden erst beim Betätigen der Schaltfläche "Aktualisieren" geladen.

Sollte es für eine Berechtigung keine Gruppen geben, wird keine Spalte für diese Berechtigung angezeigt.

Reihenfolge

Die Reihenfolge der Spalten entspricht der Reihenfolge der Berechtigungen in der Berechtigungsverwaltung, wobei zuerst Postfachberechtigungen und dann Ordnerberechtigungen angezeigt werden.

Berechtigungsgruppen importieren

Benötigte Berechtigung

Für den Import wird die Berechtigung "Manage Exchange Groups" (8333) benötigt.

Wenn Sie Exchange-Berechtigungen mittels tenfold vergeben, wird tenfold, je nach Einstellungen, Berechtigungsgruppen anlegen, wenn tenfold noch keine Berechtigungsgruppe für das entsprechende Objekt (Postfach, Ordner) bekannt ist. Wenn Sie bereits bestehende Berechtigungsgruppen auf Ihren Postfächern

und Ordnern haben, müssen Sie diese zuerst in tenfold importieren, damit tenfold diese Gruppen verwendet, statt neue Gruppen anzulegen.

Um Berechtigungsgruppen zu importieren, verwenden Sie die Maske "Exchange-Gruppen Import". Sie erreichen diese Maske auf folgenden Wegen:

- Im Menü unter Berechtigungen > Berechtigungsgruppen > Exchange > Import
- Über die Schaltfläche "Exchange-Gruppen importieren" auf der Maske "Verwendete Exchange-Gruppen".

	Name	Vollzugriff	Senden als	Senden im Auftrag von	Externer Zugang	Objekt löschen	Berechtigungen anzeigen	Berechtigungen ändern	Besitzer ändern	Empfangen als
<input type="checkbox"/>	Bayer, Otto		Charlie Exchange_rv							
<input type="checkbox"/>	Decker, Eric		Charlie Exchange_edeker_fa							
<input type="checkbox"/>	Grunewald, Michael		Exchange Charlie_Gru newald Michael_fa							
<input type="checkbox"/>	Peter, Max		Charlie Exchange_edeker_fa	Exchange_Peter Max_sob				Exchange_Peter Max_cp		
<input type="checkbox"/>	Ruder, Rudi		Charlie Exchange_r ruder_fa		Charlie Exchange_rru der_ea		Charlie Exchange_rru der_di		Charlie Exchange_rru der_rp	
<input type="checkbox"/>	Shared Info Mailbox	Exchange Charlie_Shared Info Mailbox_fa	Exchange Charlie_Shared Info Mailbox_sa	Exchange Charlie_Shared Info Mailbox_sob			Exchange Charlie_Shared Info Mailbox_di			

Zunächst können Sie mit den Filtereinstellungen festlegen ob Sie die Gruppen für alle oder spezifische Server anzeigen möchten und ob Sie Gruppen für Postfach- und/oder Ordner-Berechtigungen anzeigen wollen. Betätigen Sie die Schaltfläche "Aktualisieren" um die Berechtigungsmatrix für Ihre Berechtigungsgruppen angezeigt zu bekommen.

In jeder Zeile finden Sie hierbei ein Postfach oder einen Ordner Ihres Exchange-Servers. In den Spalten werden die einzelnen Gruppen angezeigt, welche die Berechtigung der jeweiligen Spalte auf diesem Objekt besitzen. Sollten auf einem Objekt mehrere Gruppen eine Berechtigung besitzen, so wird Ihnen an dieser Stelle ein Dropdown-Menü angezeigt, mit welchem Sie auswählen können, welche der Gruppen als Berechtigungsgruppe importiert werden soll. Ist genau eine Gruppe berechtigt, wird Ihnen einfach nur der Name dieser Gruppe angezeigt.

Aktuelle Berechtigungsgruppe

Die aktuell registrierte Berechtigungsgruppe ist an dieser Stelle bereits vorausgewählt. Sie brauchen sich daher nur um jene Berechtigungen kümmern, die Sie anpassen möchten.

In beiden Fällen, befindet sich ein Löschen-Icon neben den Gruppen. Betätigen Sie dieses Icon, wird keine Gruppe als Berechtigungsgruppe für die Berechtigung verwendet.

Bestehende Berechtigungsgruppen

Sollte bereits eine Gruppe für diese Berechtigung importiert worden sein, so wird diese durch die Aktion "Löschen" beim Import entfernt. Die tatsächliche Berechtigung der Gruppe bleibt erhalten, sie wird von tenfold jedoch nicht mehr verwendet um die betroffene Berechtigung zu vergeben.

Beim Import von Berechtigungsgruppen, müssen diese einzigartig sein. Dies bedeutet, dass jede Gruppe nur auf einer einzelnen Berechtigung vergeben werden darf. Im Fall einer Überschneidung, werden Ihnen in den betroffenen Zellen Info-Icons angezeigt. Im Tooltip dieser Icons erhalten Sie Informationen darüber, an welchen Stellen eine Doppelverwendung dieser Gruppe stattfindet.

Import

Solange sich noch Zellen mit Info-Icons in der Anzeige befinden, kann der Import nicht gestartet werden. Beheben Sie diese zuerst.

Sollte die Anzeige durch die Anzahl an Berechtigungen zu unübersichtlich werden, können Sie Zeilen aus der Anzeige entfernen, indem Sie diese mit der Checkbox markieren und dann mit den Schaltflächen im Kopf der Tabelle entweder die ausgewählten Zeilen zu entfernen oder alle anderen Zeilen. Möchten Sie die ausgeblendeten Zeilen wieder einblenden, betätigen Sie die Schaltfläche "Aktualisieren".

Wenn Sie mit den getroffenen Einstellungen zufrieden sind, betätigen Sie die Schaltfläche "Speichern" um die Gruppen zu importieren. Sie gelangen daraufhin zur Maske für die Anzeige der Berechtigungsgruppen. Dort können Sie sich vergewissern, dass die Gruppen so wie gewünscht importiert wurden.

7.1.7 SharePoint-Berechtigungsgruppen

Allgemeines

Bei der Vergabe von Berechtigungen auf SharePoint verwendet tenfold Berechtigungsgruppen, um Benutzern die jeweiligen Berechtigungen zuzuordnen. Hierbei handelt es sich jedoch nicht um Active Directory-Gruppen, sondern um Gruppen, welche nur in SharePoint existieren. Wird einem Benutzer eine Berechtigung für ein Item zugeordnet, so prüft tenfold zuerst, ob eine Berechtigungsgruppe in tenfold registriert ist und legt diese, falls notwendig, mittels eines konfigurierbaren Namensschemas an. Daraufhin wird die Berechtigung nur noch mittels Vergabe von Mitgliedschaften in dieser Gruppe durchgeführt.

Doppelte Gruppenverwendung

In SharePoint ist es, im Gegensatz zu Fileservern, durchaus üblich, eine Gruppe mehrfach zu vergeben. Im Speziellen dann, wenn zur Vergabe neuer Berechtigungen die Berechtigungsvererbung auf einem Item aufgebrochen wurde, die Benutzer der übergeordneten Items jedoch weiterhin auf den Items darunter berechtigt sein sollen. Eine zwingende 1:1 Zuordnung von Berechtigungen auf Items zu Gruppen ist daher in SharePoint notwendig.

Gruppeneinstellungen verwalten

Benötigte Berechtigungen

Für die Verwaltung ist die Berechtigung "SharePoint Resource Group Configuration Administration" (8340) erforderlich.

Um einzustellen, wie tenfold die Gruppen in SharePoint anlegt, navigieren Sie im Menü zur Maske **Berechtigungen > Berechtigungsgruppen > SharePoint > Einstellungen**.

The screenshot shows a web-based application interface for managing SharePoint groups. At the top, there's a navigation bar with links like 'Personen', 'Ressourcen', 'Berechtigungen', 'Requests', 'Organisation', 'Workflows', 'Provisioning', and 'Einstellungen'. Below the navigation is a search bar and some user icons. The main content area has a title 'SharePoint-Gruppen (1)' with a sub-instruction: 'Sie können hier festlegen, wie die Anwendung Gruppen für Exchange-Berechtigungen anlegen soll'. A table lists one group: 'tenfold Default' (Name), 'Englisch' (Sprache), and '<objectName> (<permission>)' (Gruppennamensschema). To the right of the table is a 'Über mich'-Beschreibung section with the text: 'Use this group to grant people '<permissions>' permissions to the '<objectType>: <link>'. At the bottom right of the table is a yellow '+ Neu' button.

Hier erhalten Sie zunächst eine Tabelle mit allen bereits angelegten Einstellungen.

Wenn Sie eine neue Gruppe anlegen möchten, klicken Sie auf die Schaltfläche "Neu" im Kopfbereich der Maske. Möchten Sie eine bestehende Einstellung bearbeiten, betätigen Sie die Aktion "Bearbeiten" im Aktionsmenü der jeweiligen Zeile.

An dieser Stelle können Sie nun die Einstellungen zur Anlage neuer Berechtigungsgruppen verwalten.

Konfiguration

Name *: tenfold Default
Sprache *: English

Eigenschaften der neuen Gruppe:

Name *: <objectName> (<permission>)

'Über mich'-Beschreibung: Use this group to grant people '<permission>' permissions to the '<objectType>': <link>

Erklärung

Dynamische Attribute

Zusätzlich zum Eingabetext können folgende dynamische Attribute verwendet werden, um den Gruppennamen und die Beschreibung zu generieren:

- <nearestSite> : Nächste Site
- <objectName> : Objektname
- <objectType> : Objekttyp
- <objectId> : SharePoint-ID
- <permissions> : Berechtigung

Zusätzlich für Beschreibung:

- <link> : Link

Beispiele Gruppennamen:

- <permission> Gruppe für <objectName> - Vollzugriff Gruppe für HR
- <objectName> (<permission>) - HR (Vollzugriff)

Beispiel 'Über mich'-Beschreibung

- Verwenden Sie diese Gruppe, um Benutzern <permission> auf <objectType>: <objectName> zu vergeben - Verwenden Sie diese Gruppe, um Benutzern Vollzugriff auf Website: HR zu vergeben

Allgemein

- Gruppennamen dürfen nicht länger als 64 Zeichen sein. Generierte Namen, die die maximale Länge überschreiten, werden abgekürzt.
- Der Gruppename sollte innerhalb der Websitesammlung eindeutig sein. Wenn der generierte Gruppename bereits existiert, wird eine laufende Nummer verwendet, um einen eindeutigen Namen zu generieren.

Folgende Einstellungen können getroffen werden:

Einstellung	Beschreibung
Name	Der Name der Konfiguration. Dieser wird zur Anzeige in tenfold verwendet.
Sprache	Wählen Sie hier die Sprache aus, welche für die Erzeugung der Gruppennamen verwendet werden soll. Dies bewirkt, dass die entsprechende Sprache für übersetzbare Variablen verwendet wird. Insbesondere die Berechtigungen sind hiervon betroffen. Beispiel: Befindet sich <permission> im Namensschema der Gruppe wird für Englisch "Full control" und für Deutsch "Vollzugriff" in den Gruppennamen geschrieben.
Eigenschaften der neuen Gruppe	
Name	Legt das Namensschema für neue Gruppen fest. Hierbei handelt es sich um ein Freitextfeld, in welchem beliebige Texte mit Platzhaltern in spitzen Klammern (<>) eingegeben werden können. Eine Auflistung der möglichen Platzhalter finden Sie im Nachgang. Sämtliche Texte, welche keine speziellen Platzhalter darstellen, werden so, wie sie sind, in den Gruppennamen übernommen.
'Über mich'-Beschreibung	Analog zum Namensschema kann auch für das Beschreibungsfeld "Über mich" der anzulegenden Gruppe ein Schema hinterlegt werden, welches den Text dafür erzeugt.

Folgende Platzhalter stehen in den Schemen für Namen und Beschreibung zur Verfügung:

Platzhalter	Beschreibung
<nearestSite>	Name der am nächsten gelegenen Webseite zum Item. Hinweis: Es werden nur Websites überhalb des Items gesucht, nicht darunter.
<objectName>	Der Name des Items.
<objectType>	Der Name des Item-Typs. Beispiel: "Dokument Bibliothek" (Deutsch) / "Document library" (Englisch).
<objectId>	Die ID des Items in SharePoint. Hierbei handelt es sich um eine alphanumerische Zeichenkette, entsprechend dem GUID-Schema (Näheres hierzu unter: https://de.wikipedia.org/wiki/Globally_Unique_Identifier).
<permission>	Der Name der zu vergebenden Berechtigung. Beispiel: "Lesen" (Deutsch) / "View" (Englisch)
<link>	Der URL, mit welchem das Item in SharePoint erreicht werden kann. Hinweis: Dieser Platzhalter steht Ihnen nur für das Beschreibungsfeld zur Verfügung.

Erklärung

Im Bereich "Erklärung" auf der rechten Seite der Maske erhalten Sie noch einmal eine detaillierte Beschreibung über die einzelnen Variablen, welche in den Namensschemen zur Verfügung stehen.

Gruppennamen dürfen in SharePoint, ebenso wie in Active Directory, nicht länger als 64 Zeichen sein. Sollte der erzeugte Gruppenname länger sein als jene 64 Zeichen, so kürzt tenfold den Gruppennamen ab. Die Kürzung findet nach folgendem Schema statt:

- <Erste 30 Zeichen des erzeugten Namens>...<Letzte 30 Zeichen des erzeugten Namens>

Sollte der Gruppenname bereits vergeben sein, so wird eine fortlaufende Zahl an den Gruppennamen angehängt.

Schreibweise der Platzhalter

Die Schreibweise der Platzhalter beachtet Groß- und Kleinschreibung. <objectname> (statt <objectName>) ist daher kein anerkannter Platzhalter. Sollte ein falscher oder nicht vorhandener Platzhalter verwendet werden, so wird einfach der Text inklusive < und > im Feld ausgegeben. Um fehlerhafte Schreibweisen zu vermeiden, gibt es daher eine Auto vervollständigung für Platzhalter in den Textfeldern.

Sobald Sie die notwendigen Einstellungen getroffen haben, können Sie die Konfiguration mittels eines Klicks auf die Schaltfläche "Speichern" im Kopfbereich der Maske abspeichern.

Sie können nicht verwendete Konfigurationen mittels der Aktion "Löschen" im Aktionsmenü der jeweiligen Zeile wieder entfernen.

Anzeige bestehender Berechtigungsgruppen

Benötigte Berechtigung

Zur Anzeige wird die Berechtigung "View SharePoint Groups" (8341) benötigt.

Auf der Maske "Verwendete SharePoint-Gruppen", welche Sie über das Menü unter *Berechtigungen > Berechtigungsgruppen > SharePoint > Verwendung* erreichen, können Sie sich anzeigen lassen, welche Berechtigungsgruppen bereits unter tenfold registriert sind.

Name	Vollzugriff	Mitwirken	Lesen	Moderator	Bearbeiten	Nur ansehen
Communitymitglieder Projekte - Moonshot (P111)	Besitzer von Projekte - Moonshot (P111)		Besucher von Projekte - Moonshot (P111)	Projekte - Moonshot (P111) Moderatoren		
Development Development	SVN (full control)		Besucher von Development		Mitglieder von Development	
Kategorien Projekte - Moonshot (P111)	Besitzer von Projekte - Moonshot (P111)		Besucher von Projekte - Moonshot (P111)	Projekte - Moonshot (P111) Moderatoren		
Produkthilfe Produkthilfewebsite			HelpGroup			
Projekte - Moonshot (P111) Projekte - Moonshot (P111)	Besitzer von Projekte - Moonshot (P111)	Mitglieder von Projekte - Moonshot (P111)	Besucher von Projekte - Moonshot (P111)	Projekte - Moonshot (P111) Moderatoren		Excel Services-Viewer
Projekte - Skydive (P112) Projekte - Skydive (P112)	Besitzer von Projekte - Skydive (P112)		Besucher von Projekte - Skydive (P112)		Mitglieder von Projekte - Skydive (P112)	
Projekte - Upgrade (P133) Projekte - Upgrade (P133)	Besitzer von Projekte - Upgrade (P133)	Mitglieder von Projekte - Upgrade (P133)	Besucher von Projekte - Upgrade (P133)			
SVN Development	SVN (full control)		SVN (read)		SVN (edit)	
Testing Development	tenfold Group		tenfold Group		tenfold Group	
Webseiten Projekte - Moonshot (P111)	Besitzer von Projekte - Moonshot (P111)		Mitglieder von Projekte - Moonshot (P111)	Projekte - Moonshot (P111) Moderatoren		
Zentraladministration Zentraladministration	Farm Administrators	Delegated Administrators				

Im Bereich "Filter" haben Sie die Möglichkeit nur Berechtigungsgruppen eines bestimmten SharePoint-Servers anzuzeigen. Mit der Auswahl "*" werden alle Gruppen angezeigt. Die verwendeten Gruppen werden Ihnen hierbei in einer Matrix angezeigt, wobei die Zeilen die einzelnen SharePoint-Items darstellen und die Spalten die Berechtigungen.

Keine Gruppen

Zu Beginn wird Ihnen eine Leere Seite angezeigt. Betätigen Sie die Schaltfläche "Aktualisieren", damit Ihnen die Gruppen angezeigt werden.

Berechtigungsgruppen

Hier werden nur die Berechtigungsgruppen angezeigt, welche tenfold aktiv für die Vergabe von Berechtigungen verwendet, wenn Berechtigungen mittels tenfold vergeben werden. Hierbei handelt es sich **nicht** um eine vollständige Auflistung aller Gruppen, die die entsprechenden Berechtigungen haben.

Berechtigungsgruppen importieren

Benötigte Berechtigung

Für die Verwaltung ist die Berechtigung "Manage SharePoint Groups" (8342) erforderlich.

Sollten Sie bereits bestehende Berechtigungsgruppen auf Ihrem SharePoint haben, können Sie diese auf der Maske "Import von SharePoint-Gruppen" importieren. Sie erreichen diese im Menü unter *Berechtigungen > Berechtigungsgruppen > SharePoint > Import*. Alternativ dazu erreichen Sie die Maske auch über die Schaltfläche "SharePoint-Gruppen Importieren" auf der Maske "Verwendete SharePoint-Gruppen" aus dem vorhergehenden Kapitel. Wenn Sie die Maske über diese Schaltfläche betreten werden die Filtereinstellungen aus der vorhergehenden Maske übernommen und die Gruppen bereits geladen. Wenn Sie die Maske über das Menü betreten, wählen Sie zunächst einen SharePoint-Server in den Filtereinstellungen (oder "*" für alle Server) und betätigen die Schaltfläche "Aktualisieren", um die Daten zu laden.

Sie erhalten nun eine Matrix, welche Analog zur Matrix der Maske "Verwendete SharePoint-Gruppen" aufgebaut ist.

Name	Vollzugriff	Mitwirken	Lesen	Bearbeiten	Moderator	Nur ansehen
Communitymitglieder Projekte - Moonshot (P111)	Besitzer von Projekte - Moonshot (P111)		Besucher von Projekte - Moonshot (P111)		Projekte - Moonshot (P111) Moderatoren	
Development Development	SVN (full control)		Besucher von Development	Mitglieder von Development		
Kategorien Projekte - Moonshot (P111)	Besitzer von Projekte - Moonshot (P111)		Besucher von Projekte - Moonshot (P111)		Projekte - Moonshot (P111) Moderatoren	
Produkthilfe Produkthilfewebsite		HelpGroup				
Projekte - Moonshot (P111) Projekte - Moonshot (P111)	Besitzer von Projekte - Moonshot (P111)	Mitglieder von Projekte - Moonshot (P111)	Besucher von Projekte - Moonshot (P111)	Projekte - Moonshot (P111) (edit)	Projekte - Moonshot (P111) Moderatoren	Excel Services-Viewer
Projekte - Skydive (P112) Projekte - Skydive (P112)	Besitzer von Projekte - Skydive (P112)		Besucher von Projekte - Skydive (P112)	Mitglieder von Projekte - Skydive (P112)		Excel Services-Viewer
Projekte - Upgrade (P133) Projekte - Upgrade (P133)	Besitzer von Projekte - Upgrade (P133)	Mitglieder von Projekte - Upgrade (P133)	Besucher von Projekte - Upgrade (P133)	undefined Projekte - Upgrade (P133) (edit)		Excel Services-Viewer
SVN Development	SVN (full control)		SVN (read)	SVN (edit)		
Testing Development	tenfold Group		tenfold Group	tenfold Group		
Websiten Seiten Projekte - Moonshot (P111)	Besitzer von Projekte - Moonshot (P111)		Mitglieder von Projekte - Moonshot (P111)		Projekte - Moonshot (P111) Moderatoren	
Zentraladministration	Farm Administrators	Delegated Administrators				

Berechtigungsgruppen von Websites

Die von SharePoint automatisch erzeugten Berechtigungsgruppen für "Vollzugriff", "Bearbeiten" und "Lesen" werden bereits durch den SharePoint Sync (siehe [Jobs\(see page 443\)](#)) automatisch erkannt und als Berechtigungsgruppen registriert.

Überall dort, wo mehrere Gruppen über eine Berechtigung für ein SharePoint-Item verfügen, finden Sie eine Auswahlliste in der entsprechenden Zelle der Matrix. Sie können an dieser Stelle auswählen, welche der Gruppen für die Vergabe von Berechtigungen verwendet werden sollen.

Aktuelle Berechtigungsgruppe

Die aktuell registrierte Berechtigungsgruppe ist an dieser Stelle bereits vorausgewählt. Sie brauchen sich daher nur um jene Berechtigungen kümmern, die Sie anpassen möchten.

Sollte nur eine einzelne Gruppe berechtigt sein, wird einfach nur der Gruppenname in der jeweiligen Zelle angezeigt.

Egal, ob eine Auswahl getroffen werden kann oder nicht, in jeder Zelle mit zumindest einer bestehenden Gruppe befindet sich auch ein Löschen-Icon, mit welchem die Gruppe als Berechtigungsgruppe von dieser Berechtigung entfernt werden kann.

Berechtigung bleibt bestehen

Wenn Sie eine Berechtigungsgruppe entfernen bleibt die dahinterliegende Berechtigung dennoch bestehen. Die Gruppe wird jedoch nicht mehr von tenfold zur Vergabe der Berechtigung verwendet. Stattdessen wird bei der nächsten Berechtigungsvergabe eine neue Gruppe erzeugt.

Nach betätigen des Löschen-Icons wird die Gruppe durchgestrichen angezeigt, um anzudeuten, dass Sie im Begriff sind, die Berechtigungsgruppe zu entfernen. Außerdem wird Ihnen statt dem Löschen-Icon ein Rückgängig-Icon angezeigt, mit welchem Sie den Vorgang rückgängig machen können.

Wenn Sie nur bestimmte Zeilen bearbeiten möchten können Sie auch eine Menge an Zeilen mit der Checkbox in der linken Spalte der Matrix markieren und dann entweder die ausgewählten Zeilen oder alle anderen mit der entsprechenden Schaltfläche in der Kopfzeile der Tabelle entfernen.

Entfernte Zeilen

Entfernte Zeilen werden vom Import nicht berücksichtigt. Möchten Sie die Zeilen wieder anzeigen und importieren, betätigen Sie erneut die Schaltfläche "Aktualisieren".

Wenn Sie mit den getroffenen Einstellungen zufrieden sind, betätigen Sie die Schaltfläche "Speichern" im Kopfbereich der Maske, um die ausgewählten Berechtigungsgruppen zu übernehmen (bzw. die gelöschten Gruppen als Berechtigungsgruppen zu entfernen).

Sie gelangen daraufhin wieder auf die Maske "Verwendete SharePoint-Gruppen" und können sich davon überzeugen, ob Ihre Einstellungen korrekt waren.

7.1.8 Einrichtung der Fileserver

Auswahl der Domäne

Um einen Fileserver in tenfold einzubinden, müssen einige Einstellungen festgelegt werden. Um diese Einstellungen festzulegen, wählen Sie *Einstellungen > Domänen*. Klicken Sie "Bearbeiten" im Kontextmenü der Domäne, in der sich der Fileserver befindet. Wählen Sie anschließend den Karteireiter "Fileserver" aus.

Einstellungen für die Domäne

Bestimmte Einstellungen können für die gesamte Domäne festgelegt werden:

Einstellung	Beschreibung	Beispiel
Bereich "Berechtigungen"		
Besitzer	Diese Einstellung legt fest, wer als Besitzer für Verzeichnisse eingetragen werden soll, die über tenfold angelegt werden.	TENFOLD\Administrator
Benutzer mit Vollzugriff	Über diese Einstellung kann festgelegt werden, dass ein bestimmter Benutzer (oder eine bestimmte Gruppe) automatisch die Berechtigung "Vollzugriff" auf jedes über tenfold angelegte Verzeichnis erhält. Dies ist insbesondere wichtig, wenn ein Verzeichnis mit deaktivierter Vererbung angelegt wird. Wird hierbei durch tenfold kein Vollzugriffsbenutzer (oder Gruppe) festgelegt, so verliert tenfold jeglichen Zugriff auf dieses Verzeichnis. Es sollte für diese Einstellung eine Gruppe hinterlegt werden, in welcher das Dienstkonto des tenfold-Agenten Mitglied ist. Mehrere Gruppen und/oder Benutzerkonten können mittels Doppelpunkt(:) getrennt angegeben werden.	TENFOLD\fs-admins

Bereich "Fileservergruppen"	
Konfiguration	Wählen Sie hier einen Regelsatz zur Erzeugung von Fileservergruppen fest. Näheres siehe: Fileserver-Berechtigungsgruppen(see page 207)
Organisationseinheit	Legt eine Organisationseinheit im AD fest, in welcher Fileservergruppen für diese Domäne erzeugt wird. Diese Einstellung kann je Fileserver überschrieben werden.
Bearbeitung im Expertenmodus erlaubt	Ist diese Einstellung aktiviert, können im Expertenmodus der Maske "Personen bearbeiten" (siehe Personenverwaltung(see page 63)) Fileserverberechtigungen für Fileserver dieser Domäne bestellt werden. Hinweis: Sie können nur Fileserverberechtigungen bestellen, für die bereits Fileservergruppen angelegt wurden.

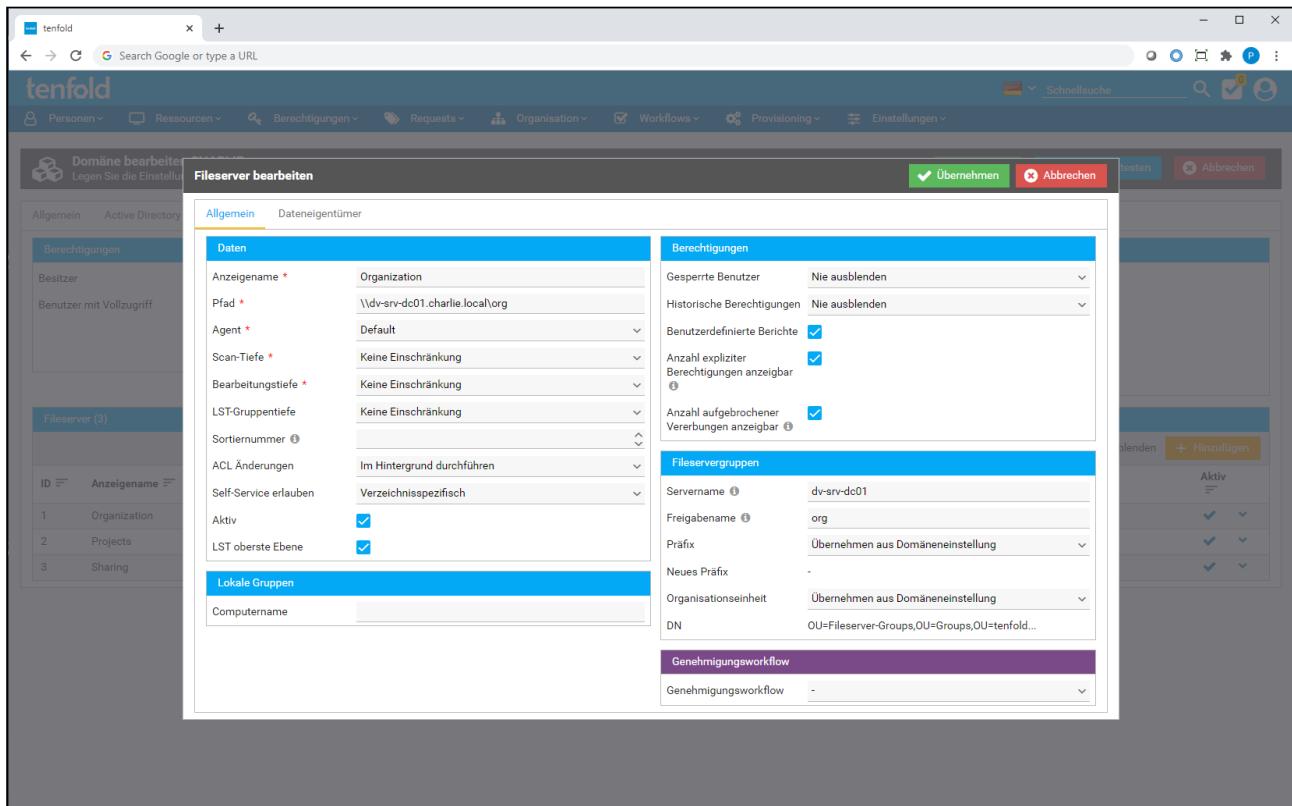
Einstellungen für einen Fileserver

Um einen neuen Fileserver hinzuzufügen, wählen Sie die Schaltfläche "Hinzufügen" an. Sie können pro Domäne beliebig viele Fileserver definieren.

Freigaben bearbeiten

Sie können die aktuellen Einstellungen zu einem Fileserver bearbeiten, indem Sie im Kontextmenü des jeweiligen Fileservers die Aktion "Bearbeiten" auswählen. Zusätzlich können Sie im Aktionsmenü direkt mit den entsprechenden Aktionen einen Fileserver aktivieren oder deaktivieren.

Einmal gespeichert können Fileserver nicht mehr gelöscht werden. Sie können sie aber deaktivieren, woraufhin sie nicht mehr gescannt oder auf Masken angezeigt werden. Um sie im Anschluss wieder zu reaktivieren, müssen Sie erst die Option "Deaktivierte Einträge ausblenden" neben der Schaltfläche "Hinzufügen" deaktivieren, um die Fileserver auf dieser Maske wieder sichtbar zu machen.



Es öffnet sich ein Dialog, auf welchem einige Einstellungen zu diesem Fileserver festgelegt werden müssen. Die Einstellungen befinden sich in zwei Karteireitern. Im ersten Karteireiter "Allgemein" befinden sich folgende Einstellungen.

Einstellung	Beschreibung	Beispiel
Bereich "Daten"		
Anzeigename	Diese Einstellung dient als Bezeichnung des Fileservers auf der tenfold Oberfläche.	Projektaufwerk
Pfad	Der Pfad legt den UNC-Pfad fest, unter welchem der Fileserver für den hinterlegten Agent erreichbar ist.	\\\srw-fs01\projects
Agent	Wählen Sie hier den Agent aus, der für die Verarbeitung (Scan/Administration) des Fileservers verantwortlich ist. Aus Performancegründen sollten Sie einen Agent wählen, der sich im gleichen LAN wie der Server befindet. Sie müssen darüber hinaus sicherstellen, dass das Dienstkonto, unter welchem der Agent läuft, über die Berechtigungsstufe "Vollzugriff" auf dem jeweiligen Fileserver verfügt.	

Scan-Tiefe	Legt fest, bis auf welche Hierarchiestufe der Agent den Fileserver scannen soll. Um den gesamten Fileserver zu scannen, geben Sie "Keine Einschränkung" an. Um die Performance zu steigern kann hier ein geringer Wert festgelegt werden. Dabei ist allerdings zu beachten, dass alle Verzeichnisse, die unter der gewählten Ebene liegen, nicht auf der Oberfläche und allen Berichten aufscheinen.	Keine Einschränkung
Bearbeitungstiefe	Legt fest, bis auf welcher Ebene durch tenfold Änderungen an dem Fileserver durchgeführt werden dürfen. Um die Bearbeitung auf allen Ebenen zu ermöglichen, geben Sie "Keine Einschränkung" an. Mit dieser Einstellung können Sie verhindern, dass Benutzer beispielsweise auf Verzeichnisse in der 5. Ebene neue Berechtigungen setzen können.	Keine Einschränkung
LST-Gruppentiefe	Bestimmt bis zu welcher Verzeichnisebene Listgruppen angelegt werden sollen. Ab der angegebenen Ebene werden keine eigenen Listgruppen mehr erzeugt, sondern die jeweilige (in tiefer liegender Verzeichnisebene) Berechtigungsgruppe wird mit Listrechten auf den Verzeichnissen, ab der angegebenen Ebene, verwendet. Der Vorteil dieser Einstellung ist, dass die Anzahl der Gruppen, die einem Benutzer zugeordnet werden, reduziert wird. Insbesondere bei sehr vielen Berechtigungen auf tiefen Verzeichnisebenen (z.B. ab Ebene 4 oder 5) kann diese Einstellung notwendig sein, um Platz im Anmeldetoken des Benutzers zu sparen. Der Nachteil dieser Einstellung ist, dass sie den Best Practices nicht entspricht, da die gleiche Berechtigungsgruppe auf mehr als einem Ordner verwendet wird.	
Sortiernummer	Diese Einstellung legt die Sortierreihenfolge der Fileserver auf den entsprechenden Masken fest. Sie können numerische Werte größer/gleich 1 vergeben.	1

ACL Änderungen	Dieses Kennzeichen legt fest, ob Requests, welche eine ACL-Änderung für diesen Fileserver mit sich bringen, sofort oder im Hintergrund durchgeführt werden sollen. Wenn diese Option aktiviert ist und Berechtigungen auf einem Ordner verändert werden, prüft das System, ob für die Änderung Operationen in den ACL des Fileservers notwendig sind. Wenn das der Fall ist, so wird der Request 1 Minute in die Zukunft geplant, um zu erreichen, dass die Verarbeitung im Hintergrund geschieht. NTFS-Operationen können, besonders auf oberen Ordnerebenen, viel Zeit in Anspruch nehmen (durch das Setzen der Vererbungen in den untergeordneten ACLs). Durch die Verarbeitung im Hintergrund erhält der Anwender sofort wieder die Kontrolle über tenfold und die Verarbeitung des Requests läuft im Hintergrund ab.	Sofort durchführen
Self Service erlauben	Legt die Default-Einstellung zur Verfügbarkeit der Verzeichnisse im Self-Service für den Fileserver fest. Mögliche Einstellungen sind: <ul style="list-style-type: none"> • Alle Verzeichnisse: Es gibt keine Einschränkung. Im Self-Service wird der gesamte Verzeichnisbaum des Fileservers angezeigt • Verzeichnisspezifisch: Grundsätzlich ist kein Verzeichnis im Self-Service verfügbar. Lediglich, wenn für das Verzeichnis die Einstellung "Self-Service erlauben" gesetzt wurde, ist das Verzeichnis verfügbar (siehe auch Verwaltung der Fileserver-Berechtigungen(see page 269)). Dies ist die empfohlene Einstellung, da sie am restriktivsten ist. • Bis Verzeichnisebene X: Alle Verzeichnisse bis zur angegebenen Ebene sind im Self-Service verfügbar. Zusätzlich kann zu dieser Einstellung bei einzelnen Verzeichnissen die Einstellung "Self-Service erlauben" gesetzt werden. Diese Verzeichnisse stehen dann im Self-Service zusätzlich - unabhängig von ihrer Verzeichnisebene - zur Verfügung. 	

Aktiv	Dieses Kennzeichen legt fest, ob dieser Fileserver angezeigt wird oder ob er verborgen wird. Darüber hinaus werden inaktive Fileserver bei der Synchronisation mit dem Fileserver nicht berücksichtigt.	ja / nein
LST oberste Ebene	Legt fest, ob durch tenfold auch auf der obersten Ebene eine Listgruppe angelegt werden soll.	ja / nein
Bereich "Lokale Gruppen"		
Computername	Wenn gewünscht ist, dass bei einem Windows File Server lokale Gruppen und Benutzerkonten berücksichtigt werden, so muss hier der NETBIOS-Computername des Servers eingetragen werden, von dem die lokalen Konten ausgelesen werden können (für diese Einstellung muss die Funktion "LocalSystem" beim jeweiligen Agent zwingend aktiviert sein). Wenn der Fileserver ein Domain-Controller (Primär oder Sekundär) ist, so darf diese Einstellung auf keinen Fall gesetzt werden, da Domain Controller keine lokalen Benutzer und Gruppen kennen und sich durch diese Einstellung Inkonsistenzen ergeben können.	SRV-FS01
Bereich "Berechtigungen"		
Gesperrte Benutzer	Hier kann eingestellt werden, ob gesperrte Active Directory-Benutzer immer ausgeblendet, nie ausgeblendet oder nur in der Dateneigentümersicht ausgeblendet werden sollen. Empfohlen wird, die gesperrten Benutzer für Dateneigentümer auszublenden.	
Historische Berechtigungen	Mit dieser Einstellung können die Möglichkeiten hinsichtlich der Anzeige von historischen Berechtigungen für diesen Fileserver festgelegt werden. Die Anzeige der historischen Berechtigungen erlaubt es, die Berechtigungen nicht nur zum aktuellen Zeitpunkt, sondern zu jedem beliebigen Zeitpunkt in der Vergangenheit anzuzeigen. Die Möglichkeit kann entweder immer zur Verfügung gestellt werden ("Nie ausblenden"), sie kann lediglich Dateneigentümern vorbehalten werden ("Für Dateneigentümer ausblenden") oder sie kann generell ausgeschaltet werden ("Immer ausblenden").	

Benutzerdefinierte Berichte	Diese Einstellung legt für den Administrator-Modus der Fileserver-Maske fest, ob Benutzer für diesen Fileserver Bericht erstellen können, für welche sie selbst die Einstellungen festlegen können, oder ob nur bereits definierte Vorlagen zur Verfügung stehen.	
Anzahl expliziter Berechtigungen anzeigbar	Diese Einstellung erlaubt es, auf der Maske der Fileserverberechtigungen die Anzahl expliziter Berechtigungen anzuzeigen. Diese Einstellung gilt nur für die Administratoransicht; für die Dateneigentümeransicht gibt es eine eigene Einstellung im Karteireiter "Dateneigentümer". Hinweis: Diese Einstellung blendet auf der Fileservermaske nur die Option ein, die expliziten Berechtigungen anzuzeigen. Standardmäßig ist diese Option nicht aktiviert.	ja/nein
Anzahl aufgebrochener Vererbungen anzeigbar	Diese Einstellung erlaubt es, auf der Maske der Fileserverberechtigungen die Anzahl aufgebrochener Vererbungen anzuzeigen. Hinweis: Diese Einstellung blendet auf der Fileservermaske nur die Option ein, die aufgebrochenen Vererbungen anzuzeigen. Standardmäßig ist diese Option nicht aktiviert.	ja/nein
Bereich "Fileservergruppen"		
Einstellungen	Mit dieser Einstellung kann festgelegt werden, ob für diesen Fileserver generell die automatische Gruppenverwaltung von tenfold zum Einsatz kommen soll, oder ob - entgegen der Best Practices - Berechtigungen auf dem Fileserver direkt auf Benutzerbasis vergeben werden sollen. In diesem Falle erfolgt jedoch keine automatische Herstellung von Listberechtigungen für übergeordnete Verzeichnisse. ACHTUNG: Diese Einstellung sollte nur dann gewählt werden, wenn sehr triftige Gründe dafür sprechen. Diese Einstellung entspricht nicht den Best Practices für Fileserver-Berechtigungen!	
Servername	Diese Einstellung legt den Wert fest, welcher für den Platzhalter "Servername" in der Fileservergruppenkonfiguration (Namenskonvention für von tenfold erstellten Berechtigungsgruppen) verwendet werden soll.	SRV-FS01
Freigabename	Diese Einstellung legt den Wert fest, welcher für den Platzhalter "Freigabe" in der Fileservergruppenkonfiguration verwendet werden soll.	projects

Präfix	Hiermit kann das in der Fileserververgruppenkonfiguration definierte Präfix für Gruppen, welche für diesen Fileserver angelegt werden, überschrieben werden.	srv_fs01
Organisationseinheit	Es kann hiermit die in der Domänenkonfiguration definierte Organisationseinheit für Gruppen, welche für diesen Fileserver angelegt werden, überschrieben werden.	OU=fs01,OU=groups,CN=tenfold,CN=local
Bereich "Genehmigungsworkflow"		
Genehmigungsworkflow	Mit dieser Einstellung kann ein Genehmigungsworkflow ausgewählt werden, welcher auf diesem Fileserver angewendet wird.	

Fileserver deaktivieren

Sollten Sie einen Fileserver deaktivieren, zu welchem es Ordner gibt, welche in Profilen (siehe [Profile \(see page 168\)](#)) hinterlegt wurden, so werden beim Speichern sämtliche Zuordnungen dieser Ordner aus allen Profilen entfernt. Wenn Sie den Fileserver später wieder reaktivieren, müssen Sie die Ordner erneut zu den Profilen hinzufügen.

Auf dem Karteireiter "Dateneigentümer" befinden sich weitere Einstellung zur Anpassung der Dateneigentümeransicht auf der Maske für Fileserverberechtigungen.

The screenshot shows the tenfold web interface with the URL 'tenfold'. The main window is titled 'Fileserver bearbeiten' (Edit Fileserver). The 'Dateneigentümer' (Data Owner) tab is active. In the 'Berechtigungen' (Permissions) section, there are two checkboxes: 'Anzahl expliziter Berechtigungen anzeigen' (Show number of explicit permissions) and 'Benutzerdefinierte Berechte' (User-defined permissions), with the latter checked. Below this is a section for 'Active Directory-Objekte ausschließen (0)' (Exclude Active Directory objects (0)). A dropdown menu for 'Active Directory-Objekt' is open, and a button '+ Hinzufügen' (Add) is visible. At the bottom of the dialog, there is a table with columns 'Name', 'Anzeigename', and 'Domäne'. The table shows two entries: '\\dv-srv-dc01.charlie.local\projects' and '\\dv-srv-dc01.charlie.local\sharing'. Both entries have 'Default' under 'Name' and 'Keine Einschränkung' (No restrictions) under 'Domäne'. The sidebar on the left lists 'Fileserver (3)': Organization (1), Projects (2), and Sharing (3).

Einstellung	Beschreibung	Beispiel
Bereich "Berechtigungen"		
Anzahl expliziter Berechtigungen anzeigen	Diese Einstellung gibt vor, ob Dateneigentümer die Anzahl explizit gesetzter Berechtigungen anzeigen können. Diese Einstellung ist analog zur selben Einstellung auf dem Karteireiter "Allgemein" im Bereich "Berechtigungen". Diese Einstellung gilt speziell nur für den Dateneigentümer Bereich und ist unabhängig von der Einstellung im Karteireiter "Allgemein".	ja/nein
Anzahl aufgebrochener Vererbungen anzeigen	Diese Einstellung gibt an, ob Dateneigentümer die Anzahl aufgebrochener Vererbungen anzeigen können. Diese Einstellung ist analog zur selben Einstellung auf dem Karteireiter "Allgemein" im Bereich "Berechtigungen". Diese Einstellung gilt speziell nur für den Dateneigentümer Bereich und ist unabhängig von der Einstellung im Karteireiter "Allgemein".	ja/nein
Benutzerdefinierte Berichte	Diese Einstellung legt für den Dateneigentümer-Modus der Fileserver-Maske fest, ob Benutzer für diesen Fileserver Berichte erstellen können, für welche sie selbst die Einstellungen festlegen können, oder ob nur bereits definierte Vorlagen zur Verfügung stehen.	
Bereich "Active Directory-Objekte ausschließen"		
Active Directory-Objekt	Wählen Sie hier Active Directory-Objekte (Gruppen, Benutzerkonten) aus und fügen Sie sie mit der Schaltfläche "Hinzufügen" zu einer Blacklist hinzu. Alle Objekte auf dieser Blacklist werden auf der Maske der Fileserverberechtigungen in der Dateneigentümeransicht ausgeblendet. In der Tabelle Unterhalb sehen Sie alle bereits hinzugefügten Objekte und können diese über die Aktion "Löschen" im Aktionsmenü wieder von der Liste entfernt werden.	Administrators

Speichern

Sämtliche Einstellungen, welche in den Dialogen der Fileserver vorgenommen wurde, werden erst mit dem Speichern der Domäne übernommen. Sollten Sie die Maske ohne Speichern verlassen, verfallen sämtliche Einstellungen, welche Sie in den einzelnen Dialogen vorgenommen haben.

Scan der Fileserver

Nachdem Sie den Fileserver konfiguriert haben, müssen Sie tenfold initial mit dem Fileserver synchronisieren. Dazu muss der Job "Share Sync" ausgeführt werden.

Für eine Beschreibung wie dazu vorzugehen ist siehe: [Jobs in tenfold\(see page 443\)](#)

7.1.9 Einrichtung der Exchange Server

Allgemeines

Um Berechtigungen in Exchange mittels tenfold bearbeiten und auswerten zu können, müssen diese erst in tenfold eingerichtet werden.

Remote-Kommunikation zwischen tenfold-Agent und Exchange-Server

Die Kommunikation zwischen tenfold und dem Exchange-Server erfolgt mittels des tenfold-Agents.

Für die Verwendung von Exchange mit tenfold wird der tenfold-Agent herangezogen, um die Kommunikation zwischen tenfold und dem Exchange-Server herzustellen. Die Installation und Konfiguration des Agents ist daher eine Grundvoraussetzung für die Einrichtung von Exchange ([Einrichten des tenfold-Agent\(see page 199\)](#)).

Der Zugriff auf Exchange kann hierbei entweder mit dem Account des Agent-Services erfolgen oder mit in tenfold konfigurierten Zugangsdaten ([Zugangsdaten\(see page 552\)](#)).

Der Agent verwendet, unabhängig von der Maschine, auf welcher er installiert ist, immer eine Remote-Powershell-Sitzung, um auf den Exchange-Server zuzugreifen. Um Probleme zu vermeiden wird daher empfohlen, den Agent **nicht** auf dem Exchange-Server zu installieren.

Einrichtung des Accounts

Der Account, welcher für Zugriff auf den Exchange-Server verwendet wird, muss sowohl Mitglied der Exchange Managementrolle "ApplicationImpersonation" sein als auch Mitglied der Rollengruppe "Organization Management".

Folgendes Powershell-Skript kann verwendet werden, um einen Account zum Mitglied der Managementrolle "ApplicationImpersonation" zu machen.

```
New-ManagementRoleAssignment -Role "ApplicationImpersonation" -User <username>
```

Mittels folgendem Powershell-Skript kann ein Account zum Mitglied der Rollengruppe "Organization Management" gemacht werden:

```
Add-RoleGroupMember "Organization Management" -Member <username>
```

Ein Account mit diesen Berechtigungen ist nun in der Lage, die tenfold-Funktionen für Exchange durchzuführen.

Um Zugriff auf öffentliche Ordner zu erhalten, muss der Benutzer ein Postfach besitzen.

Troubleshooting

Sollte die Kommunikation zwischen Agent und Exchange-Server, trotz erteilter Berechtigungen für den verwendeten Account, nicht funktionieren, so kann dies daran liegen, dass der Account nicht für die Verwendung von Remote Powershell auf dem Exchange-Server freigegeben ist.

Mit folgendem Powershell-Skript können Sie auf dem Exchange-Server prüfen, ob der Account die nötigen Powershell-Freigaben besitzt.

```
Get-User <username> | fl RemotePowerShellEnabled
```

Wenn *False* zurückgegeben wird, muss folgender Befehl durchgeführt werden:

```
Set-User <username> -RemotePowerShellEnabled $True
```

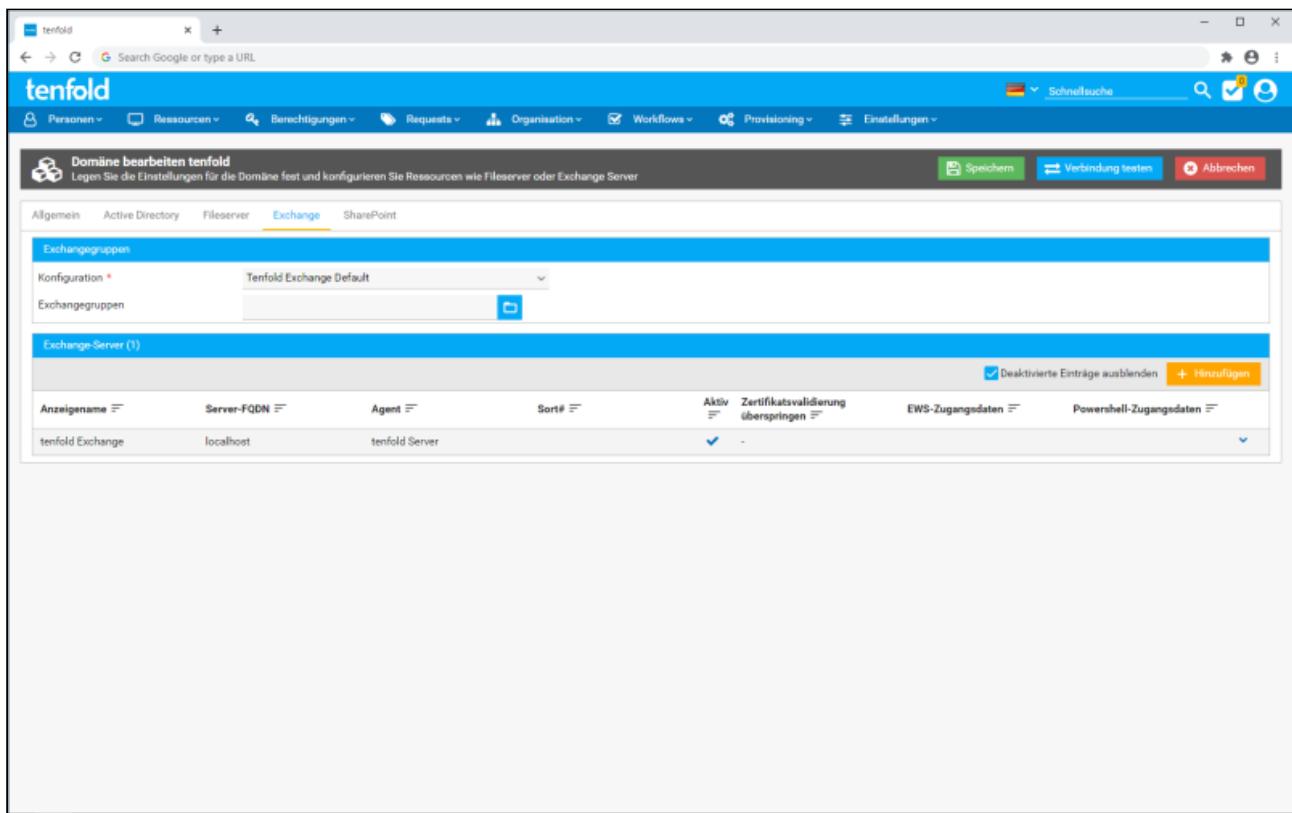
Domänenübergreifender Zugriff

Im Moment wird nur die Eingabe eines Benutzers unterstützt, welcher sich in der selben Domäne des Exchange-Servers befindet.

Falls ein Benutzer aus einer anderen Domäne verwendet werden soll, muss dieser direkt bei dem Service eingetragen werden, unter welchem der tenfold-Agent läuft.

Einrichtung des Exchange-Servers

Um einen Exchange-Server in tenfold einzubinden, müssen einige Einstellungen festgelegt werden. Um diese Einstellungen festzulegen, wählen Sie im Menü *Einstellungen > Domänen*. Klicken Sie "Bearbeiten" im Kontextmenü der Domäne, in der sich der Fileserver befindet. Wählen Sie anschließend den Karteireiter "Exchange" aus.



Einstellungen für die Domäne

Folgende Einstellungen gelten für alle Exchange-Server in der Domäne und können nicht individuell festgelegt werden.

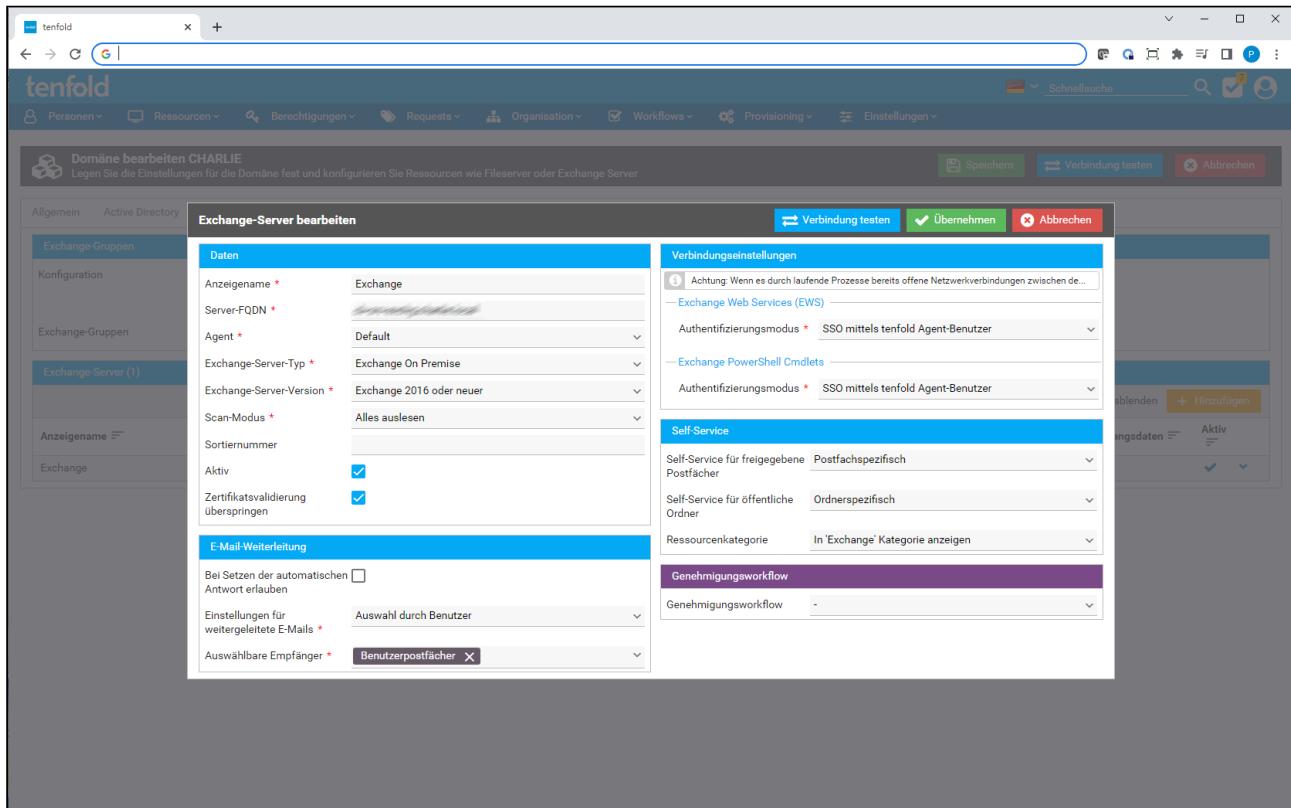
Einstellung	Beschreibung	Beispiel
Konfiguration	Mit dieser Einstellung legen Sie fest, welche der konfigurierten Namensschemen zur Anlage der Berechtigungsgruppen verwendet werden soll. Eine genaue Beschreibung über die möglichen Konfigurationen finden Sie unter Exchange-Berechtigungsgruppen(see page 212) .	Tenfold Exchange Default
Exchange-Gruppen	Diese Einstellung legt fest, in welcher OU im Active Directory die Exchange-Gruppen angelegt werden sollen (Exchange-Berechtigungsgruppen(see page 212)).	OU=Exchange,DC=ihredomain,DC=local

Einstellungen für einen Exchange-Server

Um einen neuen Exchange-Server hinzuzufügen, klicken Sie auf "Hinzufügen". Sie können pro Domäne beliebig viele Exchange-Server definieren.

Exchange Server bearbeiten

Sie können die aktuellen Einstellungen zu einem Exchange-Server bearbeiten, indem Sie im Kontextmenü des jeweiligen Servers die Aktion "Bearbeiten" auswählen.



Es öffnet sich ein Dialog, in dem die Einstellungen zum entsprechenden Server getroffen werden müssen:

Einstellung	Beschreibung
Bereich "Daten"	
Anzeigename	Diese Einstellung dient als Anzeigename auf der tenfold-Oberfläche.
Server-FQDN	Mit dieser Einstellung legen Sie fest, mit welchem Server tenfold Verbindung aufnehmen soll, um die Exchange-Operationen durchzuführen.
Agent	Diese Einstellung legt fest, welcher Agent die Operationen für diesen Exchange-Server durchführen soll.
EWS-Exchange-Server-Version	Die Version des Exchange-Web-Services. Sollten Sie eine neuere Version haben als angegeben, wählen Sie einfach die aktuellste Version im Dropdown.
Sortiernummer	Legt fest, in welcher Reihenfolge die Exchange-Server auf der Maske für Exchange-Berechtigungen angezeigt werden (siehe Verwaltung der Exchange-Berechtigungen (see page 294)). Die Darstellung erfolgt in aufsteigender Reihenfolge der Nummerierung.

Aktiv	Aktiviert oder deaktiviert den Exchange-Server. Deaktivierte Exchange-Server werden auf der Oberfläche ausgeblendet und vom Scan nicht mehr berücksichtigt. Sie können diese Einstellung auch durch die Aktion "Aktivieren" und "Deaktivieren" im Kontextmenü des Servereintrages ändern.
Zertifikatsvalidierung überspringen	Akzeptiert sämtliche Zertifikate, unabhängig davon, ob sie im Zertifikatsspeicher von tenfold liegen oder nicht.
Identitätswechsel für neue Postfächer verwenden	Beim Auslesen der Berechtigungen eines Postfaches wendet tenfold einen Identitätswechsel auf die Person an, welche dieses Postfach besitzt. Sollte noch nie eine Anmeldung an diesem Postfach stattgefunden haben, werden bei dieser Operation die Standardordner für Postfächer nach den Spracheinstellungen von Exchange vorgenommen. Mit dieser Einstellung können Sie bestimmen, ob dieser Identitätswechsel für Postfächer ohne Anmeldung durchgeführt werden soll. Ist diese Einstellung deaktiviert wird verhindert, dass für Personen, welche sich noch nie an ihrem Postfach angemeldet haben, Ordner in der falschen Sprache angelegt werden, Sie erhalten jedoch auch keine Informationen zu den Berechtigungen dieses Postfaches, bis sich eine Person einmal angemeldet hat.

Bereich "Genehmigungsworkflow"

Genehmigungsworkflow	Legt einen Genehmigungsworkflow fest, welcher für Requests, die diesen Exchange-Server betreffen, verwendet wird.
----------------------	---

Bereich "Sicherheit"

EWS-Zugangsdaten	Wählen Sie hier die Zugangsdaten aus, welche für den Zugriff auf den Exchange Webservice verwendet werden sollen. Sollten Sie keine Zugangsdaten hinterlegen wird der Benutzer gewählt, unter welchem der Dienst des ausgewählten Agents läuft.
Powershell-Zugangsdaten	Zugangsdaten für den Remote Powershell-Zugriff. Sollten Sie keine Zugangsdaten hinterlegen, wird der Benutzer gewählt, unter welchem der Dienst des ausgewählten Agents läuft.
Powershell-Authentifizierung	Diese Einstellung legt den Authentifizierungsmechanismus fest, mit welchem die Remote Powershell-Sessions für diesen Exchange-Server aufgebaut werden.

Bereich "Self-Service"

Self-Service für freigegebene Postfächer	Mit dieser Einstellung legen Sie fest, ob alle freigegebenen Postfächer dieses Servers im Self-Service verfügbar sind oder ob die Freigabe individuell je Postfache erfolgt.
--	--

Self-Service für öffentliche Ordner	Steuert die Verfügbarkeit der öffentlichen Ordner dieses Servers im Self-Service. Dies kann entweder für alle öffentlichen Ordner dieses Servers oder individuell je Ordner erfolgen.
Ressourcenkategorie	Legt fest, in welcher Ressourcenkategorie die Objekte dieses Servers im Self-Service angezeigt werden. Mit der Auswahl "In 'Exchange' Kategorie anzeigen" werden die Objekte in einer Standardkategorie für Exchange-Server angezeigt, welche nicht extra angelegt werden muss (siehe Ressourcenkategorien(see page 149)).

Deaktivierte Einträge ausblenden

Nachdem Sie einen Eintrag in der Liste deaktiviert haben, wird dieser standardmäßig ausgeblendet. Wenn Sie deaktivierte Einträge anzeigen möchten, entfernen Sie einfach den Haken "Deaktivierte Einträge ausblenden".

Verbindung testen

Mit der Schaltfläche "Verbindung testen" im Dialog eines Exchange-Servers kann geprüft werden, ob der tenfold-Agent mit den ausgewählten Einstellungen eine Verbindung zum Exchange-Server herstellen kann. **Achtung:** Die Schaltfläche "Verbindung testen" im Kopfbereich der Maske führt einen Verbindungstest zum Active Directory durch.

Scan der Exchange-Server

Nachdem Sie den Exchange-Server konfiguriert haben, müssen Sie tenfold initial mit dem Exchange-Server synchronisieren. Dazu muss der Job "Exchange Sync" ausgeführt werden.

Für eine Beschreibung, wie hierbei vorzugehen ist, siehe: [Jobs in tenfold](#)⁶

7.1.10 Einrichtung der SharePoint-Server

Bevor Sie mit der Verwaltung der SharePoint-Berechtigungen beginnen können, müssen zuerst ein oder mehrere SharePoint-Server in tenfold hinterlegt und eingescannt werden. Um einen **On Premises** SharePoint-Server in tenfold zu hinterlegen, verfahren Sie wie folgt:

SharePoint Online

Wie Sie die SharePoint-Online-Instanz Ihres Microsoft 365-Mandanten einbinden können, erfahren Sie unter [Einrichtung von Microsoft 365 Mandanten\(see page 243\)](#).

Navigieren Sie im Menü zum Punkt *Einstellungen > Active Directory-Domänen* und bearbeiten Sie dort die Domäne, in welcher sich Ihr SharePoint-Server befindet. Navigieren Sie daraufhin auf den Karteireiter "SharePoint"

Benötigte Berechtigung

Für die Verwaltung ist die Berechtigung "Manage Active Directory Domains" (8035) erforderlich.

⁶ <http://vi-srv-atlassian.prod.local:8090/display/ISMAD/Jobs>

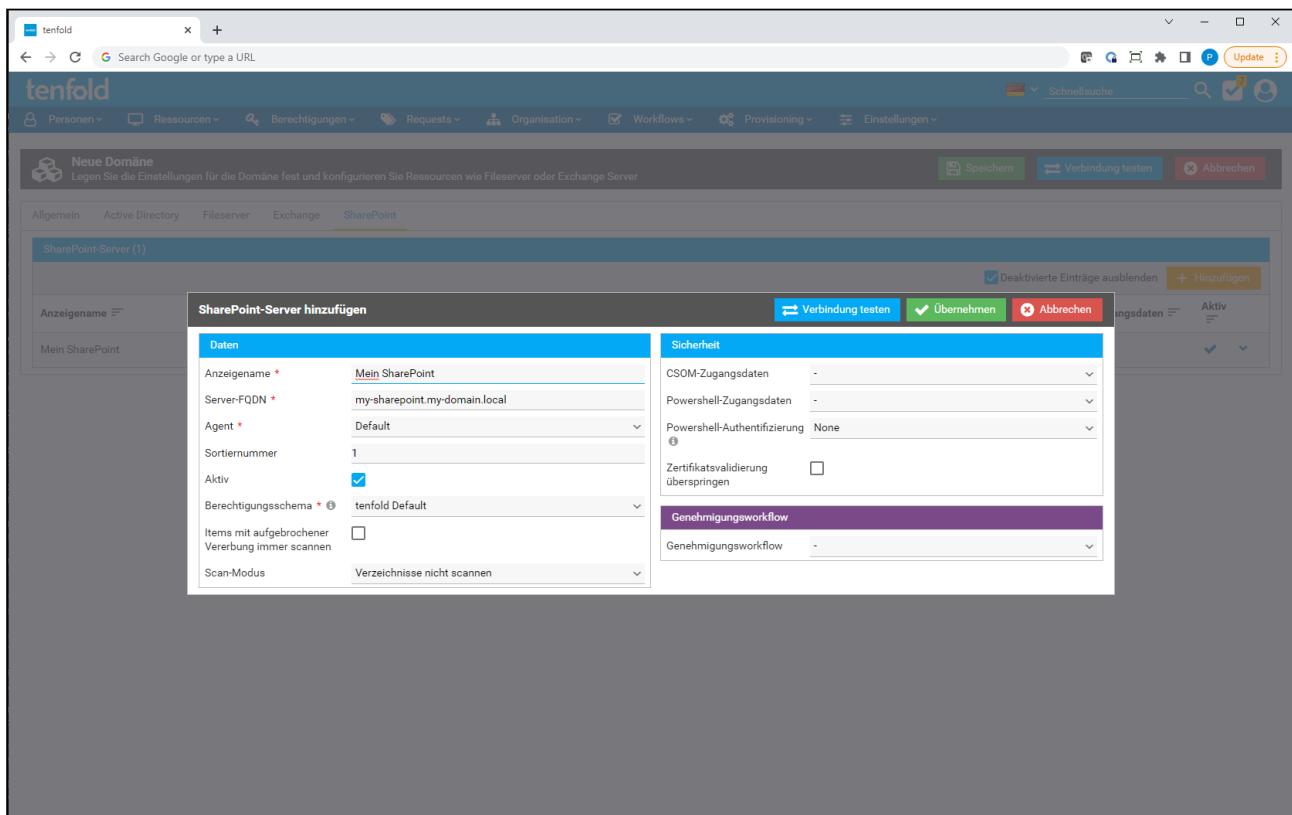
Anzeigename	Server-FQDN	Agent	Sort#	Zertifikatsvalidierung überspringen	CSOM-Zugangsdaten	Powershell-Zugangsdaten	Aktiv
Mein SharePoint	my-sharepoint.my-domain.local	Default	1	-	-	-	<input checked="" type="checkbox"/>

Sie erhalten eine Übersicht über alle bereits eingerichteten SharePoint-Server dieser Domäne.

Deaktivierte Server

Standardmäßig werden alle (in tenfold) deaktivierten Server ausgeblendet. Um diese einzublenden, entfernen Sie den Haken bei der Checkbox "Deaktivierte Einträge ausblenden".

Um einen neuen Server zu registrieren, betätigen Sie die Schaltfläche "Hinzufügen". Um einen bestehenden Eintrag zu bearbeiten, benutzen Sie die Aktion "Bearbeiten" im Aktionsmenü des jeweiligen Eintrages. Daraufhin öffnet sich ein Dialog, in welchem Sie die Daten des Servers bearbeiten können.



In diesem Dialog können Sie folgende Einstellungen vornehmen:

Einstellung	Beschreibung
Bereich "Daten"	
Anzeigename	Geben Sie hier einen Namen ein. Dieser Name wird nur zur Anzeige in tenfold verwendet.
Server FQDN	Der Vollständige Name des Servers, auf welchem Ihr SharePoint installiert ist.
Agent	Tragen Sie hier den tenfold-Agent ein, mit welchem Ihr SharePoint gescannt werden soll.
Sortiernummer	Geben Sie hier eine Nummer ein, nach welcher die SharePoint-Server auf der tenfold-Oberfläche sortiert werden sollen. Bei gleicher Sortiernummer werden die Server nach Anzeigename sortiert.
Aktiv	Haken Sie diese Checkbox an, damit der Server in tenfold angezeigt und beim Scan vom Agenten mit aufgenommen wird.
Berechtigungsschema	Gibt das Schema für die Berechtigungsgruppen an (siehe SharePoint-Berechtigungsgruppen (see page 217)).

Items mit aufgebrochener Vererbung immer scannen	Ist diese Einstellung aktiv, werden SharePoint-Items mit aufgebrochener Vererbung immer eingescannt, unabhängig von den Einstellungen "Scan-Modus" und "Scan-Tiefe". Hinweis: Da in SharePoint Berechtigungen nur auf Items mit aufgebrochener Vererbung vergeben werden können, können Sie die Datenmenge des Scans drastisch reduzieren, indem Sie nur die Items mit aufgebrochener Vererbung scannen.
Scan-Modus	Legt fest welche Items von Ihrem SharePoint gescannt werden sollen. Sie haben folgende Auswahlmöglichkeiten: <ul style="list-style-type: none"> • Verzeichnisse nicht scannen: Es werden weder Verzeichnisse (und Verzeichnisähnliche Items wie Websites, Dokumentbibliotheken, etc) noch Dateien gescannt. Achtung: Ist die Einstellung "Items mit aufgebrochener Vererbung immer scannen" nicht aktiviert, werden mit dieser Auswahl nur die Top-Level Websites eingescannt. • Verzeichnisse scannen: Es werden alle Items, außer Dateien, gescannt. • Verzeichnisse und Dateien scannen: Es werden alle Items, inklusive Dateien, gescannt.
Scan-Tiefe	Mit dieser Einstellung können Sie beschränken, wie viele Ebenen Ihres SharePoints eingescannt werden sollen. Mit der Auswahl "Keine Einschränkung" wird bis in die untersten Ebenen Ihres SharePoints gescannt (außer Dateien, wenn der "Scan-Modus" diese nicht enthält). Andernfalls wird bis in die angegebene Ebene hinunter gescannt.
Bereich "Sicherheit"	
CSOM-Zugangsdaten	Die Zugangsdaten, welche zur Verbindung mit dem SharePoint-Webservice verwendet werden. Hinweis: Die Zugangsdaten müssen vom Typ "Standard" sein (siehe Zugangsdaten(see page 552)).
Powershell-Zugangsdaten	Die Zugangsdaten, welche zur Verbindung mit dem SharePoint Powershell-Dienst verwendet werden. Hinweis: Die Zugangsdaten müssen vom Typ "Standard" sein (siehe Zugangsdaten(see page 552)).
Powershell-Authentifizierung	Legt den Authentifizierungsmodus fest, mit welchem der Agent eine Remote Powershell-Verbindung zum SharePoint-Server aufnehmen soll (Näheres finden Sie unter https://docs.microsoft.com/en-us/dotnet/api/system.management.automation.runspaces.authenticationmechanism).
Zertifikatesvalidierung überspringen	Mit dieser Einstellung können Sie die Prüfung des Zertifikates von Ihrem SharePoint-Server unterbinden. tenfold vertraut daraufhin allen Zertifikaten, welche der Server sendet. Achtung: Diese Einstellung ist dafür gedacht die Verbindung zu testen, sollte noch kein Zertifikat eingerichtet worden sein. Verwenden Sie diese Einstellung keinesfalls im laufenden Betrieb, sondern richten immer ein Zertifikat ein (siehe Zertifikatsverwaltung(see page 523)).
Bereich "Genehmigungsworkflow"	

Genehmigungsworkflow	Hier kann der Standard-Genehmigungsworkflow für diesen Server hinterlegt werden. Alle Anfragen für Berechtigungen auf diesem Server müssen dann zuerst mittels dieses Genehmigungsworkflows genehmigt werden. Ist kein Genehmigungsworkflow hinterlegt, werden nur die individuellen Genehmigungsworkflows auf Ihren Items herangezogen. Ist auch dort kein Workflow hinterlegt, findet keine Genehmigung statt.
----------------------	--

Sie können mit der Schaltfläche "Verbindung testen" im Dialog prüfen, ob der tenfold-Agent sich mit den ausgewählten Einstellungen zum SharePoint-Server verbinden kann. Mit der Schaltfläche "Übernehmen" werden die Daten übernommen.

Verbindung testen

Achten Sie darauf, die Schaltfläche "Verbindung testen" im Dialog der SharePoint-Server-Einstellungen zu verwenden. Die Schaltfläche "Verbindung testen" im Kopfbereich der Maske führt immer zu einem Verbindungstest des Active Directory.

Wenn Sie mit den Einstellungen fertig sind, betätigen Sie die Schaltfläche "Speichern" im Kopfbereich der Maske.

Speichern

Nur durch "Übernehmen" im Dialog der SharePoint-Server werden die Daten nicht gespeichert. Vergessen Sie nicht die Schaltfläche "Speichern" zu betätigen.

7.1.11 Active Directory Kategorien

Allgemein

Dieser Objekttyp dient dazu, Active Directory Benutzer und Gruppen nach bestimmten Merkmalen zu kategorisieren. Diese Kategorien können anschließend in verschiedenen Optionen beim Erstellen von Berichten verwendet werden, um diese übersichtlicher zu gestalten. An folgenden Punkten kommen Kategorien zum Einsatz:

- Auf dem Bericht "Verzeichnisberechtigungen", welcher die berechtigten Benutzer und Gruppen auf einem Verzeichnis am Fileserver zeigt, wird neben dem Benutzernamen auch die Kategorie angezeigt, sofern der Benutzer oder die Gruppe einer Kategorie zugewiesen ist.
- In den Optionen für den Bericht "Verzeichnisberechtigungen" haben Sie die Möglichkeit bestimmte Kategorien von der Anzeige auf dem Bericht auszuschließen (siehe dazu auch [Verwaltung der Fileserver-Berechtigungen](#)(see page 269))

Mitgliedschaft

Ein Benutzer und eine Gruppe können jeweils nur Mitglied einer Kategorie sein

Verwaltung

Die Verwaltung der Active Directory Kategorien erfolgt über den Menüpunkt Berechtigungen > Einstellungen > Kategorien. Die Maske zeigt eine Liste aller aktuell definierten Kategorien an.

Anlegen

Mit dem Plus-Button kann eine neue Kategorie hinzugefügt werden. Folgende Daten können hierbei hinterlegt werden:

- Name: Die Bezeichnung der Kategorie. Der Name wird in weiterer Folge im tenfold zur Anzeige verwendet.
- Externe ID: Die Externe ID dient lediglich dazu, Kategorien mit Fremdsystemen abzugleichen. Diese Funktion muss individuell per EXEC bereitgestellt werden und ist nicht out-of-the-box verfügbar.
- Beschreibung: Der Beschreibungstext dient zur Erklärung, was genau mit dieser Kategorie abgebildet werden soll.

Bearbeiten

Sie können eine bestehende Kategorie bearbeiten, indem Sie im Aktionsmenü der gewünschten Zeile die Option "Kategorie bearbeiten" auswählen.

Die Daten für Name, EID, Beschreibung können in weiterer Folge angepasst werden.

Mitglieder bearbeiten

Die Mitgliederliste einer Kategorie kann über die Option "Mitglieder bearbeiten" im Aktionsmenü bearbeitet werden. Der rechte Bereich der Maske zeigt die aktuellen Mitglieder der Kategorie an.

Benutzer und Gruppen, die Mitglied werden sollen, können über Eingabe des Namens, oder eines Teils des Namens im Suchfeld im linken Bereich der Maske gesucht werden. Um ein Objekt als Mitglied hinzuzufügen muss diese per Drag & Drop in den rechten Bereich der Maske (Mitgliederliste) gezogen werden.

Wenn Sie ein Mitglied aus der Kategorie entfernen wollen, so wählen Sie die Option "Löschen" aus dem Aktionsmenü der jeweiligen Zeile.

Löschen

Um eine gesamte Kategorie zu löschen, wählen Sie die Option "Löschen" aus dem Aktionsmenü der jeweiligen Zeile auf der Übersichtsliste aller Kategorien.

7.1.12 Einrichtung von Microsoft 365 Mandanten

Bevor Sie die Microsoft 365 Funktionen von tenfold verwenden können, muss zuerst der Mandant registriert werden. Dies erfolgt analog zur Einrichtung einer Windows-Domäne zur Anbindung des Active Directory (siehe [Einrichten einer Windows Domain\(see page 196\)](#))

Microsoft 365 Mandant vorbereiten

Netzwerk

Die notwendigen Netzwerkkonfigurationen finden Sie unter [Systemvoraussetzungen\(see page 32\)](#).

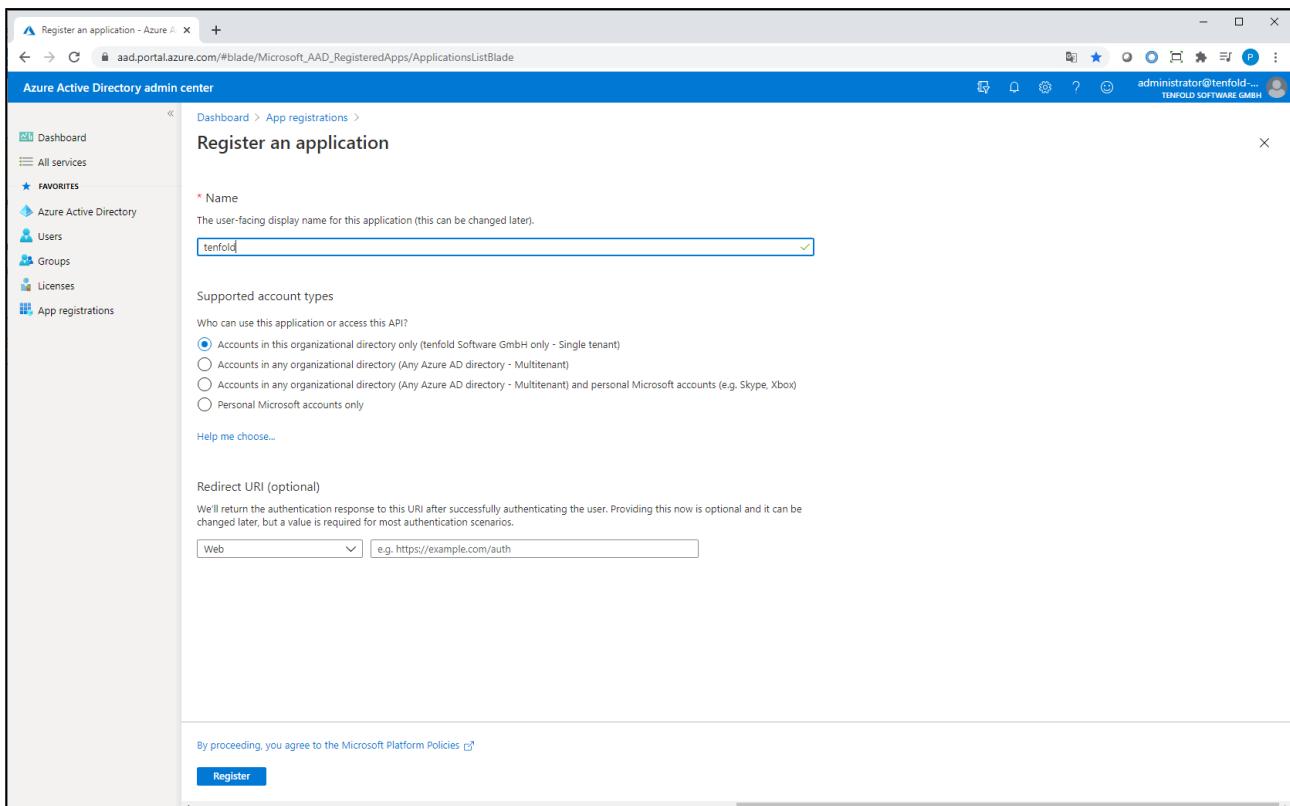
Bevor ein Microsoft 365 Mandant mit tenfold bearbeitet werden kann, muss tenfold als App für das Azure Active Directory (AAD) auf diesem Mandanten registriert werden.

Melden Sie sich hierfür im Azure Active Directory Portal unter <https://aad.portal.azure.com/> an und wählen dort All services in der Sidebar aus. Wählen Sie auf der darauffolgenden Seite App registrations.

Klicken Sie nun auf New registration, um eine neue App für den Zugriff auf Ihr AAD zu konfigurieren.

Azure Active Directory admin center

Bitte beachten Sie, dass Microsoft das Administrations-Tool für Azure Active Directory kontinuierlich ändert und anpasst. Es kann daher sein, dass die folgenden Schritte in dieser Anleitung, sowie die Abbildungen, nicht vollständig mit der aktuellen Darstellung übereinstimmen. Betrachten Sie die unten angeführten Schritte daher als Richtlinien.



Wählen Sie als Name *tenfold* und wählen Sie unter *Supported account types* die Option *Accounts in this organizational directory only*, sollte diese Option nicht bereits ausgewählt sein. Fahren Sie fort durch einen Klick auf *Register*. Sie gelangen daraufhin zu einer Übersicht der gerade erstellten App-Registrierung. Notieren Sie sich an dieser Stelle die *Application (Client) ID* sowie die *Directory (Tenant) ID*. Sie benötigen diese beiden Werte später bei der Einrichtung des Mandanten in tenfold.

The screenshot shows the Azure Active Directory admin center interface. The left sidebar has 'App registrations' selected. The main area shows the 'tenfold' application registration. The 'Overview' tab is active. Key details shown include:

- Display name:** tenfold
- Application (client) ID:** c435484c-dbbd-4b8b-aa59-948dbcb626db
- Directory (tenant) ID:** [redacted]
- Object ID:** [redacted]
- Supported account types:** My organization only
- Redirect URIs:** Add a Redirect URI
- Application ID URI:** Add an Application ID URI
- Managed application in L...**: tenfold test

Two informational cards are present:

- Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)
- Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

On the right, there's a 'Call APIs' section with icons for various Microsoft services like SharePoint, OneDrive, and Power BI, followed by a 'Documentation' section with links to Microsoft Identity platform, Authentication scenarios, etc.

Im nächsten Schritt müssen die Berechtigungen für die Anwendung festgelegt werden. Wählen Sie dafür im Menü den Abschnitt *API permissions* und klicken Sie auf die Schaltfläche *Add a permission*, woraufhin ein Popup zur Auswahl der Berechtigungen erscheint.

The screenshot shows the Azure Active Directory admin center with the URL aad.portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/CallAnAPI/appId/c435484c-dbbd-4b8b-aa59-940dbcb626db/objectId/1153b2ff-56b5-4e7f-8e4d-c2a4f4b79b.... The user is administrator@tenfold.de from TENFOLD SOFTWARE GMBH.

Request API permissions

Select an API

Commonly used Microsoft APIs

API / Permissions name	Type
Microsoft Graph (1)	User.Read Delegated

Wählen Sie hier **Microsoft Graph** und im Anschluss **Application Permissions**. Folgende Berechtigungen aus der daraufhin erscheinenden Liste sind anzuwählen:

- Directory.ReadWrite.All (Anwendung)
- Group.ReadWrite.All (Anwendung)
- GroupMember.ReadWrite.All (Anwendung)
- Team.ReadBasic.All (Anwendung)
- User.ReadWrite.All (Anwendung)

Sie können den Suchfilter verwenden, um die Suche nach den gewünschten Berechtigungen zu vereinfachen. Wenn Sie fertig sind, betätigen Sie die Schaltfläche **Add permissions**.

Darüber hinaus werden noch Berechtigungen aus dem Exchange-Bereich benötigt. Klicken Sie hierfür erneut auf **Add a permission**. Wechseln Sie dieses Mal jedoch auf den Karteireiter **APIs my organization uses** und wählen im Anschluss **Office 365 Exchange Online**.

The screenshot shows the Azure Active Directory admin center with the URL [https://aad.portal.azure.com/#blade/Microsoft_AAD_B2B/ManageAPIPermissionsBlade/resourceId%3D/tenantId%3D/permissionsId%3D/](#). The left sidebar shows 'Dashboard', 'All services', 'FAVORITES' (with 'Azure Active Directory' selected), 'Users', 'Groups', and 'App registrations'. The main area shows the 'tenfold Markus | API permissions' page. The 'API permissions' section is selected in the left navigation. The right pane is titled 'Request API permissions' and shows a table of configured permissions for the 'office' application. The table includes columns for Name, Application (client) ID, and Type.

Name	Application (client) ID
Office 365 Enterprise Insights	f9d02341-e7aa-456d-926d-4a0ca599fbee
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 Information Protection	2f502c9-5679-4a5c-a605-0de55bd7d135
Office 365 Management APIs	c5393580-f805-4401-9568-94b7aef2fc2
Office 365 Search Service	66a88757-258c-4c72-893c-3e0bed4d6899
Office 365 SharePoint Online	00000003-0000-0ff1-ce00-000000000000
Office Scripts Service	62fd1447-0ef3-4ab7-a956-7dd05232ecc1
Office Shredding Service	b97be6bd4-a49f-4a0c-af18-af507d1da76c
Office365 Zoom	0d38933a-0bbd-41ca-9ebd-28c4b5ba7cb7

Wählen Sie hier jeweils aus den Bereichen *Delegated permissions* folgende Berechtigungen:

- EWS.AccessAsUser.All (Delegiert)
- Group.ReadWrite.All (Delegiert)
- User.Read.All (Delegiert)

The screenshot shows the Azure Active Directory admin center with the 'Request API permissions' page for an app registration. The left sidebar has 'API permissions' selected. The main area shows 'Configured permissions' for Microsoft Graph, including 'User.Read' (Delegated) and 'User.ReadWrite.All' (Application). A separate 'Select permissions' section shows expanded categories like Calendars, Contacts, EAS, Exchange, Group, and MailboxSettings.

Im Anschluss wählen Sie noch aus dem anderen Bereich (*Application permissions*) folgende Berechtigungen:

- Exchange.ManageAsApp (Anwendung)
- full_access_as_app (Anwendung)
- User.Read.All(Anwendung)

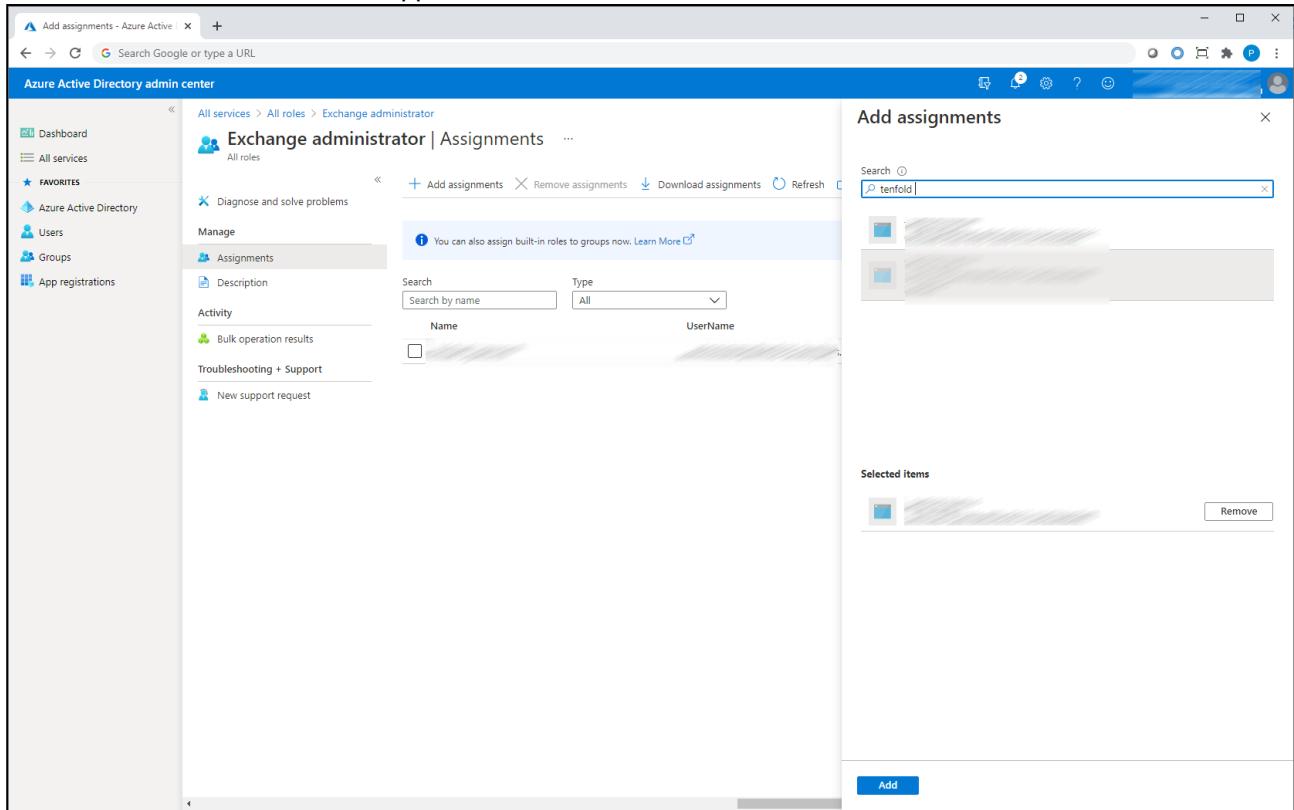
Betätigen Sie nun noch die Schaltfläche *Grant admin consent* im Hauptbereich über der Liste der Berechtigungen. Die Berechtigungen sollten nun wie folgt aussehen:

The screenshot shows the Azure Active Directory admin center with the URL aad.portal.azure.com. The left sidebar is titled "Azure Active Directory admin center" and includes sections for Dashboard, All services, Favorites (Azure Active Directory, Users, Groups, App registrations), and App registrations. Under "App registrations", the "API permissions" section is selected. The main content area is titled "API permissions" and shows a list of granted permissions for the application "tenfold Markus". A message at the top states "Successfully granted admin consent for the requested permissions." Below this, a table lists "Configured permissions" for Microsoft Graph and Office 365 Exchange Online. The table columns include API / Permissions name, Type, Description, Admin consent req..., and Status. Most permissions have a green checkmark in the status column, indicating they are granted.

Zuletzt muss die Anwendung noch zu den Exchange-Administratoren hinzugefügt werden. Öffnen Sie dafür wieder die Seite *All services* in der Sidebar und suchen Sie den Service *Azure AD roles and administrators*.

The screenshot shows the "All roles" page in the Azure Active Directory admin center. The URL is aad.portal.azure.com. The left sidebar is identical to the previous screenshot. The main content area is titled "All roles" and shows a list of administrative roles. A search bar at the top right contains the text "exch". The table has columns for Role, Description, Type, and more. One role is listed: "Exchange administrator" (Type: Built-in), which is described as "Can manage all aspects of the Exchange product." A note at the top of the page says "To create custom roles, your organization needs Azure AD Premium P1 or P2. Start a free trial.".

Suchen Sie hier in der Liste nach der *Exchange administrator* Rolle und klicken Sie auf *Add assignments*. Suchen Sie daraufhin nach ihrer App, wählen diese aus und klicken auf die Schaltfläche *Add*.



Für die Verwaltung der SharePoint-Berechtigungen werden des Weiteren noch folgende Berechtigungen benötigt:

- Sites.FullControl.All (Anwendung)
- Sites.ReadWrite.All (Anwendung)
- User.ReadWrite.All (Anwendung)

Sie finden diese Berechtigungen, wenn Sie auf "Add permission" klicken und dann im Reiter "Microsoft APIs" auf die Kachel "SharePoint" klicken. Wählen Sie dann noch "Application permissions". Die benötigten Berechtigungen befinden sich in dieser Liste.

Ebenso werden aus dem Microsoft Graph API folgende Berechtigungen benötigt:

- Group.ReadWrite.All (Anwendung)
- Sites.FullControl.All (Anwendung)
- User.ReadWrite.All (Anwendung)

Verfahren Sie wie oben beschrieben, wählen jedoch die Kachel "Microsoft Graph" statt "SharePoint". Für die Verwaltung der Teams benötigen Sie noch folgende Berechtigungen, welche ebenso unter "Microsoft Graph" zu finden sind.

- ChannelSettings.ReadWrite.All (Anwendung)
- ChannelMember.ReadWrite.All (Anwendung)
- Team.Create (Anwendung)

Damit ist die Vergabe der notwendigen Berechtigungen abgeschlossen. Für eine erfolgreiche Verbindung von tenfold zu Ihrem AAD muss nun zuletzt noch ein Zertifikat für tenfold installiert werden.

Navigieren Sie hierfür zu dem Bereich *Certificates & secrets*. Dort klicken Sie auf *Upload certificate*.

Sie werden daraufhin aufgefordert, eine Zertifikatsdatei hochzuladen. Laden Sie hier eine Zertifikatsdatei **ohne** privatem Schlüssel hoch. Es handelt sich hierbei normalerweise um eine Datei mit der Endung .cer. Im Anschluss verwenden Sie die Zertifikatsverwaltung von tenfold (siehe [Zertifikatsverwaltung \(see page 523\)](#)), um dort das dazugehörige Zertifikat **mit** privatem Schlüssel zu installieren. Es handelt sich hierbei zumeist um Dateien mit der Endung .pfx, .pem oder Ähnlichem.

Damit ist die Registrierung von tenfold seitens AAD abgeschlossen.

Welches Zertifikat?

Für die Verbindung ist lediglich erforderlich, dass das verwendete Zertifikat sowohl in AAD (ohne privatem Schlüssel) als auch in tenfold (mit Privatem Schlüssel) hinterlegt ist. Welches Zertifikat Sie verwenden spielt dabei keine Rolle. Sie können hierfür entweder ein neues Self-Signed Zertifikat erstellen (z.B. mit PowerShell) oder ein neues Zertifikat von Ihrer CA erstellen lassen. Am Ende müssen die installierten Zertifikate nur übereinstimmen.

Vorbereitung des Agents

tenfold nutzt den tenfold Agent zur Kommunikation mit der Microsoft 365-Plattform. Der Agent nutzt für gewisse Aktionen PowerShell-Befehle, um diese durchzusetzen. Dafür ist es notwendig, dass auf allen Maschinen, auf denen Agenten zur Verwendung mit Microsoft 365 betrieben werden, das PowerShell-Modul "Exchange Online PowerShell V3-Modul" installiert ist.

Administratorberechtigungen

Damit die folgenden PowerShell-Befehle erfolgreich durchgeführt werden können, muss die PowerShell mit Administratorberechtigungen gestartet werden.

Zur Installation führen Sie einfach folgende PowerShell-Befehle durch:

Notwendige PowerShell-Module installieren

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Install-Module -Name ExchangeOnlineManagement -RequiredVersion 3.1.0 -Force
```

Exchange Online Remote PowerShell

In tenfold Versionen < 2022 R3 Update 5 verwendet tenfold Remote PowerShell Session, um Ihre Exchange Online-Instanz zu verwalten. Mit 01.07.2023 stellt Microsoft die Verwendung von Remote PowerShell für Exchange Online ein. Damit Sie weiterhin Ihre Exchange Online-Instanz ab diesem Zeitpunkt verwalten können, updaten Sie Ihre tenfold-Installation und Ihre Agents auf die Version 2022 R3 Update 5 (22.3.5) sowie das ExchangeOnlineManagement PowerShell-Modul auf die Version 3.1.0.

Für die Verwaltung von SharePoint ist noch folgendes Modul zu installieren:

SharePoint Powershell Modul

```
Install-Module -Name PnP.PowerShell -RequiredVersion 1.9.0
```

Fehler bei Modulinstallation

Sollten Sie die Fehlermeldung "PackageManagement\Install-Package : Für die angegebenen Suchkriterien und den Paketnamen "PnP.PowerShell" wurde keine Übereinstimmung gefunden. Verwenden Sie Get-PSRepository, um alle verfügbaren, registrierten Paketquellen anzuzeigen." oder ähnliches erhalten, so liegt dies wahrscheinlich daran, dass Sie in Ihrer Powershell noch TLS < 1.2 aktiviert haben.

Mit folgendem Befehl sollte sich der Fehler beheben lassen:

```
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
```

Genauere Informationen finden Sie unter: <https://dev.to/darksmile92/powershell-disabled-support-for-tls-1-0-for-the-gallery-update-module-and-install-module-broken-1oii>

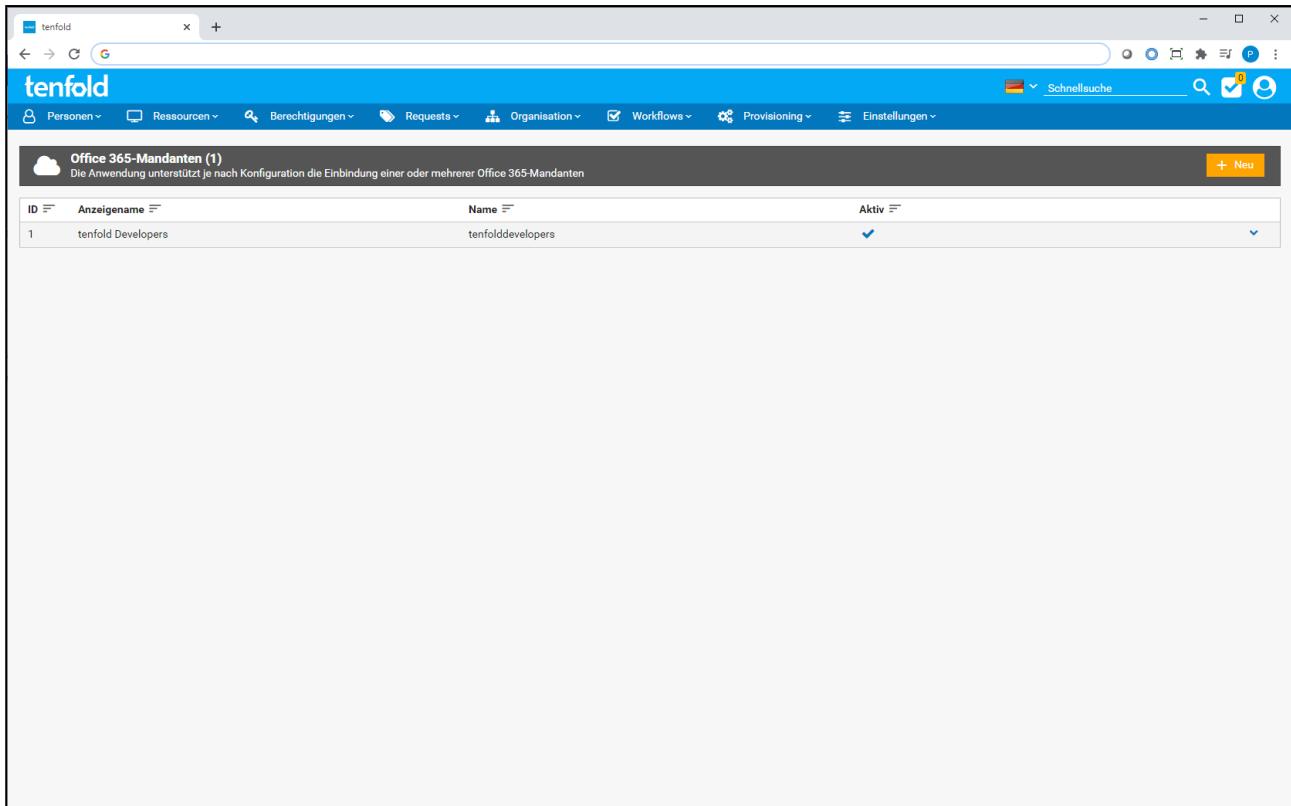
Sobald die Befehle erfolgreich durchgeführt wurden ist der Agent auf dieser Maschine für den Einsatz von Microsoft 365 vorbereitet.

Einrichtung des Mandanten in tenfold

Zur Verwaltung der Mandanten, navigieren Sie im Menü zur Seite *Einstellungen > Microsoft 365 Mandanten*.

Benötigte Berechtigungen

Für den Zugriff auf diese Seite wird die tenfold-Berechtigung "Manage Microsoft 365 Tenants" (8350) benötigt.



The screenshot shows a browser window with the tenfold logo at the top. The main content area displays a table titled 'Office 365-Mandanten (1)'. The table has columns for ID, Anzeigename, Name, and Aktiv. There is one entry: ID 1, Anzeigename 'tenfold Developers', Name 'tenfolddevelopers', and Aktiv status is checked. A yellow button labeled '+ Neu' is visible in the top right corner of the table header.

ID	Anzeigename	Name	Aktiv
1	tenfold Developers	tenfolddevelopers	✓

Betätigen Sie hier die Schaltfläche *Neu* im Kopfbereich, um einen neuen Mandanten in tenfold zu erstellen oder wählen Sie *Bearbeiten* im Aktionsmenü eines vorhandenen Mandanten, um diesen zu bearbeiten.

Allgemeine Einstellungen

The screenshot shows the 'Allgemein' tab selected in the Microsoft 365 tenant configuration interface. It displays the following fields:

- Allgemein:**
 - Anzeigename: tenfold Developers
 - Name: tenfolddevelopers
 - Aktiv: checked
 - Exchange-Modus: Exchange Online
- Genehmigungsworkflow:**
 - Gruppen: -
 - Lizenzen: -
- Verbindungseinstellungen:**
 - Verzeichnis-ID (Mandant): [REDACTED]
 - Anwendungs-ID (Client): [REDACTED]
 - Zertifikat: tenfold-o365
 - Agent: [REDACTED]
 - Zertifikatsvalidierung überspringen: unchecked

Activity Runner Plugin

Für das korrekte Funktionieren gewisser Microsoft-365-Prozesse, wird die Installation des *Activity Runner* Plugins vorausgesetzt. Installieren Sie daher dieses Plugin, bevor Sie Ihren ersten Mandanten in tenfold einrichten. Sollte das Plugin nicht installiert sein wird Ihnen eine Warnmeldung beim Erstellen/Bearbeiten der Mandanten angezeigt.

Im Karteireiter *Allgemein* befinden sich allgemeine Einstellungen zum Mandanten, wie etwa die Einstellungen, die zur Verbindung notwendig sind.

Folgende Einstellungen finden Sie hier vor:

Einstellung	Beschreibung
Bereich "Allgemein"	
Anzeigename	Legen Sie hier einen Namen fest, unter welchem dieser Mandant in tenfold angezeigt werden soll. Dieser Name wird nur zur Anzeige in tenfold verwendet.
Name	Tragen Sie hier den Namen Ihres Mandanten aus Microsoft 365 ein. Dieser ist die Adresse Ihres Mandanten, z.B. mycompany.onmicrosoft.com

Aktiv	Ist diese Einstellung angehakt wird dieser Mandant, beim Scan der Daten, durch tenfold berücksichtigt.
Exchange-Modus	<p>Gibt an, wie sich tenfold bei der Vergabe von Lizenzen, welche Exchange beinhalten, verhalten soll. Folgende Auswahlmöglichkeiten stehen zur Verfügung:</p> <ul style="list-style-type: none"> • Exchange Online: tenfold vergibt Exchange-Lizenzen sofort. Wählen Sie diese Option, sollten Sie Exchange nur in der Cloud betreiben. • Exchange Hybrid: tenfold wartet mit der Vergabe von Exchange-Lizenzen bis eine Mailbox in der Cloud existiert. Damit ist sichergestellt, dass die durch die Lizenzvergabe erzeugte Mailbox nicht der synchronisierten Mailbox in die Quere kommt. Wählen Sie diese Einstellung, sollten Sie Exchange in einem Hybridsystem betreiben.

Bereich "Verbindungseinstellungen"

Verzeichnis-ID (Mandant)	Tragen Sie hier die <i>Directory (tenant) ID</i> ein, welche Sie bei der Registrierung der App aus dem AAD Portal erhalten haben.
Anwendungs-ID (Client)	Tragen Sie hier die <i>Application (client) ID</i> ein, welche Sie bei der Registrierung der App aus dem AAD Portal erhalten haben.
Zertifikat	Wählen Sie hier das in tenfold installierte Zertifikat aus, welches für die Kommunikation mit dem Mandanten vorgesehen ist.
Agent	Mit dieser Einstellung wird festgelegt, welcher tenfold-Agent für Microsoft-365-Operationen herangezogen werden soll.
Zertifikatsvalidierung überspringen	<p>Ist diese Einstellung aktiv prüft tenfold, bei der Kommunikation mit dem Mandanten, das Server-Zertifikat nicht. Andernfalls muss tenfold dem Server-Zertifikat vertrauen, was bedeutet, dass es im Zertifikatsspeicher (Windows oder tenfold) vorhanden sein sollte.</p> <p>Warnung: Verwenden Sie diese Option aus Sicherheitsgründen nur vorübergehend und auch nur dann, wenn es zwingend notwendig ist.</p>

Bereich "Genehmigungsworkflow"

Gruppen	Diese Einstellung legt den Genehmigungs-Workflow fest, welcher bei der Verwaltung von Microsoft 365 Gruppen verwendet wird.
Lizenzen	Mit dieser Einstellung können Sie bestimmen welcher Genehmigungsworkflow bei der Verwaltung von Microsoft 365 Lizenzen herangezogen wird.

Mandanten in tenfold < 2022 R3 Update 5

In tenfold-Versionen < 2022 R3 Update 5 wurde im Feld "Name" die Adresse des Mandanten ohne "onmicrosoft.com" eingetragen. Um Mandanten zu unterstützen, welche nicht auf "onmicrosoft.com" enden, muss seit 2022 R3 Update 5 der vollständige Name eingetragen werden. Mit dem Update auf 2022 R3 Update 5 wird Ihre Konfiguration automatisch migriert, damit diese "onmicrosoft.com" enthält. Sie müssen die Einstellung daher nicht manuell anpassen. Löschen Sie daher das Suffix "onmicrosoft.com" nicht weg.

Lizenzen und Apps

Auf diesem Karteireiter können Sie konfigurieren, welche Lizenzen und Apps mittels tenfold zugewiesen werden können und welche nur angezeigt werden.

Hierfür gibt es 3 mögliche Einstellungen:

Einstellung	Beschreibung
Erlauben	Die Lizenz/App kann einer Person <i>und</i> Profilen zugeordnet werden.
Nur in Profilen erlauben	Die Lizenz/App kann <i>nur</i> Profilen zugeordnet werden, Personen jedoch nicht direkt. Damit kann man erreichen, dass gewisse Lizenzen z.B. nur als Standard für gewisse Abteilungen verfügbar sind, jedoch nicht individuell zuordenbar sind.

Einstellung	Beschreibung
Nicht erlauben	Die Lizenz/App kann über tenfold <i>gar nicht</i> zugeordnet werden. Die Zuordnung muss händisch über die Microsoft 365 Benutzerverwaltung erfolgen. Zugewiesene Lizenzen/Apps werden in tenfold jedoch trotzdem angezeigt.

Sie können diese Einstellung individuell für alle Lizenzen und die darin enthaltenen Apps vergeben. Zusätzlich dazu existieren zwei Einstellungen, um Standards für neu hinzugefügte Lizenzen und Apps festzulegen.

Standardeinstellung für	Beschreibung
Lizenz-Zuweisungen	Legt die Standardeinstellung für alle neuen Lizenzen fest, welche beim Datenabgleich erkannt werden.
App-Zuweisungen	Legt die Standardeinstellung für alle neuen Apps fest, welche beim Datenabgleich erkannt werden.

Bestehende Einstellungen

Diese Einstellungen wirken sich nur auf Lizenzen/Apps aus, welche beim Datenabgleich des Jobs *O365 Object Sync* neu gefunden werden. Sie sollten diese Einstellungen daher festlegen bevor Sie zum ersten Mal den Datenabgleich durchführen. Alle Lizenzen/Apps, welche bereits auf der Seite angezeigt werden, sind von diesen Einstellungen nicht mehr betroffen, sondern müssen bei Bedarf individuell angepasst werden.

Exchange

Wie bei Active Directory-Domänen können hier auch Einstellungen für das Auslesen und Anzeigen der Exchange-Berechtigungen getätigt werden.

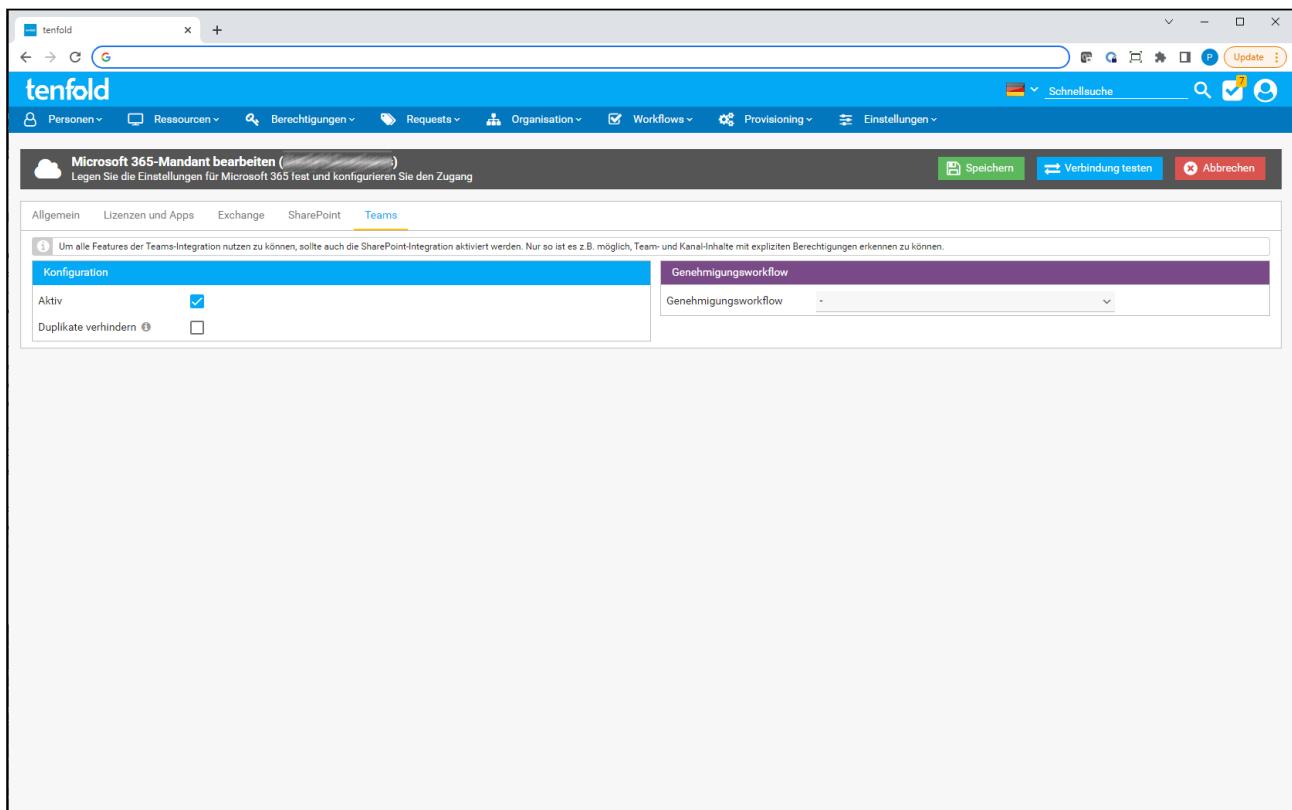
Folgende Einstellungen können hier getroffen werden:

Einstellung	Beschreibung
Bereich "Konfiguration"	
Aktiv	Diese Einstellung legt fest, ob der Exchange-Server dieses Mandanten von tenfold verwaltet werden soll. Ist diese Einstellung nicht angehakt, werden weder die Berechtigungen ausgelesen noch in tenfold angezeigt und lassen sich auch nicht bearbeiten. Sollte diese Einstellung nachträglich deaktiviert werden, so wird der Exchange-Server auf der Maske ausgeblendet und dessen Daten werden in tenfold nicht aktualisiert.
Berechtigungsschema	Hier kann eine zuvor erstellte Konfiguration zur Auswahl von Exchange-Gruppen getroffen werden. Nähere Details finden Sie unter Exchange-Berechtigungsgruppen (see page 212).

Scan-Modus	Hier können Sie einstellen, welche Objekte von tenfold gescannt werden sollen. Folgende Einstellungen sind möglich: <ul style="list-style-type: none"> Alles auslesen: Scannt alle Objekte des Servers ein. Dies sind Postfächer sowie darin enthaltenen Ordner und öffentliche Ordner. Nur Mailboxen auslesen: Scannt nur Postfächer ein. Postfachordner werden nicht ausgelesen. Mailboxen und Öffentliche Ordner auslesen: Scannt nur Postfächer und öffentliche Ordner ein. Postfachordner werden nicht ausgelesen.
Sortiernummer	Legt die Sortiernummer für den Exchange-Server auf der Seite für Exchange-Berechtigungen fest. Dies ist nur notwendig, sollten Sie mehrere Exchange-Server betreiben (zum Beispiel, wenn Sie mehrere Mandanten verwalten).
Bereich "Self-Service"	
Self-Service für freigegebene Postfächer	Gibt an, ob und welche Exchange-Postfächer im Self-Service verfügbar sein sollen. Sie können entweder alle Postfächer freigeben oder sich dafür entscheiden, diese Entscheidung für jedes Postfache individuell zu treffen. Im Falle der individuellen Auswahl ist zu Beginn kein Postfach freigegeben. Dies muss händisch beim Postfach aktiviert werden. Die Auswahl erfolgt unter Verwaltung der Exchange-Berechtigungen (see page 294).
Self-Service für öffentliche Ordner	Gibt an, ob und welche öffentlichen Exchange-Ordner im Self-Service verfügbar sein sollen. Es kann an dieser Stelle eingestellt werden, ob alle Ordner im Self-Service verfügbar sind oder, ob diese individuell ausgewählt werden sollen. Im Falle der individuellen Auswahl sind standardmäßig keine Ordner für den Self-Service freigegeben. Die Auswahl erfolgt unter Verwaltung der Exchange-Berechtigungen (see page 294).
Ressourcenkategorie	Legt fest, in welcher Ressourcenkategorie die Elemente dieses Servers im Self-Service angezeigt werden sollen.
Bereich "Genehmigungsworkflow"	
Genehmigungsworkflow	Legt den Standard-Genehmigungsworkflow für alle Elemente auf diesem Exchange-Server fest.

SharePoint

Um die Berechtigungen Ihrer SharePoint Online-Instanz zu verwalten, muss diese zunächst in tenfold konfiguriert werden. Öffnen Sie dazu den Karteireiter "SharePoint" auf der Maske Ihres Microsoft-365 Mandanten.



Die Einstellungen hierfür sind ähnlich denen, die Sie für On-Premises SharePoint-Installationen in Ihrer Active Directory-Domäne treffen können. Näheres hierzu finden Sie unter [Einrichtung der SharePoint-Server \(see page 238\)](#).

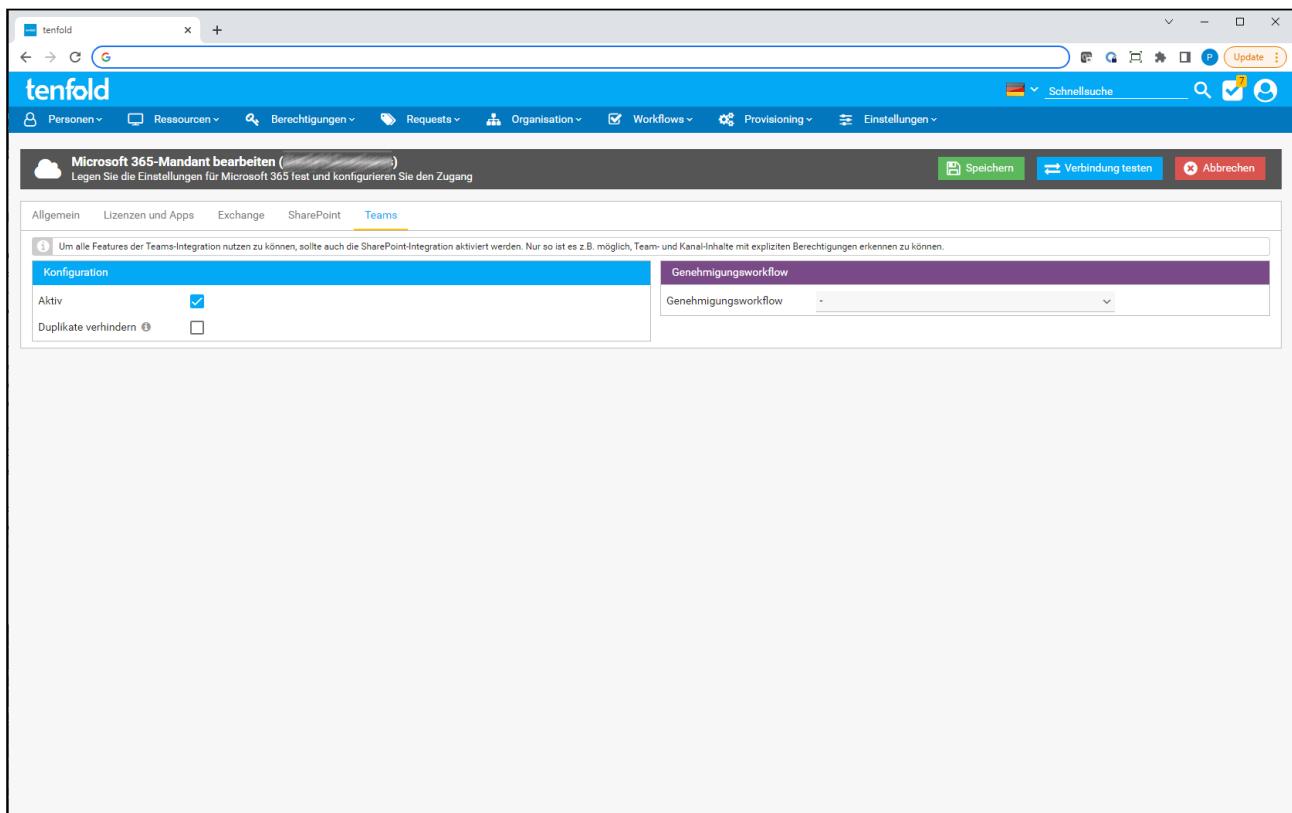
Da es jedoch nur eine SharePoint-Instanz auf jedem Mandanten geben kann und die Verbindung mit Ihrem Microsoft 365-Konto stattfindet, fallen hier einige Einstellungen weg, welche Sie für On-Premises SharePoint-Server treffen können. Die Einstellungen sind wie folgt:

Einstellung	Beschreibung
Bereich "Konfiguration"	
Aktiv	Mit dieser Einstellung legen Sie fest, ob Ihre SharePoint Online-Instanz von tenfold verwaltet werden soll oder nicht. Ist diese Einstellung deaktiviert, scheint Ihr SharePoint-Server nicht in der Berechtigungsverwaltung auf und die Daten werden nicht gescannt. Erst, wenn diese Einstellung aktiviert wurde, werden die anderen Einstellungen sichtbar.
Berechtigungsschema	Wählen Sie hier ein Schema aus, mit welchem die Berechtigungsgruppen für diese SharePoint-Instanz angelegt werden sollen. Siehe SharePoint-Berechtigungsgruppen (see page 217) für Details.
Items mit aufgebrochener Vererbung immer scannen	Ist diese Einstellung aktiv, so werden die Berechtigungen von Items (Websites, Dokumentbibliotheken, Ordner, etc.) immer eingescannt, wenn auf diesen die Vererbung der Berechtigungen aufgehoben wurde, unabhängig von den Einstellungen für "Scan-Modus" und "Scan-Tiefe".

Scan-Modus	Legt fest, welche Items Ihres SharePoints gescannt werden sollen. Sie haben folgende Auswahlmöglichkeiten: <ul style="list-style-type: none"> Verzeichnisse nicht scannen: Es werden weder Verzeichnisse (und Verzeichnisähnliche Items wie Websites, Dokumentbibliotheken, etc.) noch Dateien gescannt. Achtung: Ist die Einstellung "Items mit aufgebrochener Vererbung immer scannen" nicht aktiviert, so werden mit dieser Auswahl nur die Top-Level Websites eingescannt. Verzeichnisse scannen: Es werden alle Items außer Dateien gescannt. Verzeichnisse und Dateien scannen: Es werden alle Items, inklusive Dateien, gescannt.
Scan-Tiefe	Mit dieser Einstellung können Sie beschränken, wie viele Ebenen Ihres SharePoints eingescannt werden sollen. Mit der Auswahl "Keine Einschränkung" wird bis in die untersten Ebenen Ihres SharePoints gescannt (außer Dateien, wenn der "Scan-Modus" diese nicht enthält). Andernfalls wird bis in die angegebene Ebene hinunter gescannt.
Bereich "Genehmigungsworkflow"	
Genehmigungsworkflow	Hier kann der Standard-Genehmigungsworkflow für diesen Server hinterlegt werden. Alle Anfragen für Berechtigungen auf diesem Server müssen dann zuerst mittels dieses Genehmigungsworkflows genehmigt werden. Ist kein Genehmigungsworkflow hinterlegt, werden nur die individuellen Genehmigungsworkflows auf Ihren Items herangezogen. Ist auch dort kein Workflow hinterlegt, so findet keine Genehmigung statt.

Teams

Um die Features für Microsoft Teams in tenfold nutzen zu können, müssen diese zunächst für Ihre Microsoft 365-Mandanten aktiviert werden. Die notwendigen Einstellungen finden Sie im Karteireiter "Teams" auf der Maske zur Bearbeitung der Microsoft 365-Mandanten.



SharePoint

Da Microsoft Teams im Hintergrund SharePoint als Datenbackend verwendet, muss Ihre SharePoint Online-Instanz in tenfold eingescannt werden, um alle Features von Microsoft Teams in tenfold nutzen zu können.

Folgende Einstellungen können vorgenommen werden:

Einstellung	Beschreibung
Bereich "Konfiguration"	
Aktiv	Haken Sie diese Einstellung an, um die tenfold-Features für Microsoft Teams für diesen Mandanten zu aktivieren. Die anderen Einstellungen auf dieser Maske werden erst sichtbar, wenn diese Einstellung aktiviert wurde.
Duplikate verhindern	Für Microsoft Teams muss der Name eines Teams innerhalb Ihres Mandanten nicht eindeutig sein. Zur besseren Übersicht können Sie diese Einstellung aktivieren, damit tenfold bei der Anlage neuer Teams prüft, ob es bereits Teams mit dem angeforderten Namen gibt. Ist diese Einstellung nicht aktiv, dann prüft tenfold, ebenso wie Teams, nicht, ob die vergebenen Namen eindeutig sind.
Bereich "Genehmigungsworkflows"	

Genehmigungsworkflow	Hier können Sie einen Genehmigungsworkflow hinterlegen, welcher standardmäßig für Teams-Requests auf diesem Mandanten verwendet werden soll.
----------------------	--

OneDrive

Der Karteireiter OneDrive enthält nur eine einzige Einstellung "Aktiv". Mit dieser Einstellung können die OneDrive-Funktionen für diesen Mandanten aktiviert werden.

Datenabgleich

Zusätzlich zu dieser Einstellung muss auch der Job "OneDrive Sync" durchgeführt werden (siehe [Jobs\(see page 443\)](#)).

Datenabgleich

In regelmäßigen Abständen findet ein Datenabgleich zwischen tenfold und jenen Microsoft 365 Mandanten statt, die in tenfold als *aktiv* gekennzeichnet sind. Dieser Datenabgleich wird vom Job *O365 Object Sync* durchgeführt. Sie können die Intervalle der Durchführung auf der Jobverwaltungsseite unter *Einstellungen > Jobs > Verwaltung* anpassen (siehe [Jobs\(see page 443\)](#) für nähere Informationen).

Benötigte Berechtigung

Für den Zugriff auf diese Seite wird die tenfold-Berechtigung "Manage Jobs" (8013) benötigt.

Der Datenabgleich synchronisiert folgende Datenbestände nach tenfold:

- Vorhandene Lizenzen und Apps
- Vorhandene Objekte (Gruppen, Verteilerlisten, etc.) im Azure Active Directory
- Die Zuordnungen von AAD Objekten, Lizenzen und Apps zu Personen

Azure AD Connect

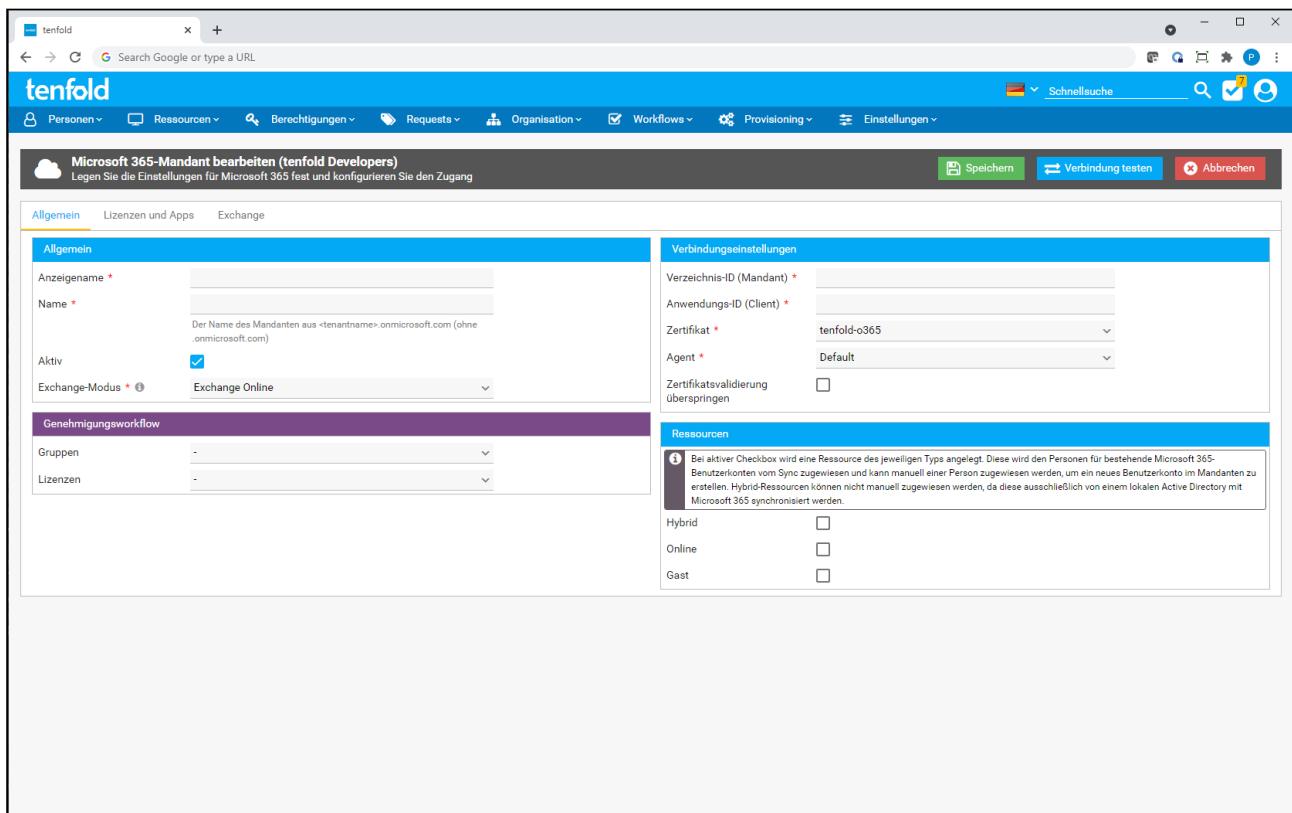
Bitte beachten Sie, dass dieser Datenabgleich nichts mit dem Azure AD Connect zu tun hat. Dieser Datenabgleich dient nur dazu, den tatsächlichen Zustand Ihres Microsoft-365-Mandanten mit den Daten in tenfold abzulegen. Den Azure AD Connect von Microsoft benötigen Sie weiterhin.

Exchange und SharePoint

Den Abgleich der Exchange Online-Berechtigungen sowie SharePoint Online-Berechtigungen übernehmen jeweils die Jobs "Exchange Sync" und "SharePoint Sync".

Microsoft 365 User Lifecycle Plugin

Das Microsoft 365 User Lifecycle Plugin ermöglicht es Ihnen, den Lifecycle von Benutzerkonten in Microsoft-365-Mandanten zu verwalten. Ohne dieses Plugin ist es Ihnen in tenfold nur möglich, die Gruppenmitgliedschaften und Lizenzen von bestehenden und eingescannten Benutzern zu verwalten. Sobald Sie das Plugin installiert haben, erscheint im Karteireiter *Allgemein* der Mandantenkonfiguration, ein neuer Bereich: *Ressourcen*.



In diesem Bereich können Sie einstellen, für welche Arten von Benutzerkonten Sie, beim Speichern des Mandanten, automatisch eine Ressource anlegen möchten.

Mithilfe dieser Ressourcen ist es Ihnen möglich, den Lifecycle Ihrer Microsoft 365-Benutzer zu verwalten. Es gibt folgende Typen von Benutzerkonten, welche tenfold verwaltet:

Typ	Beschreibung
Hybrid	Benutzerkonten vom Typ "Hybrid" werden ausschließlich durch den Microsoft Active Sync verwaltet. Es handelt sich hier um Konten, welche im On-Premises Active Directory existieren und mittels Active Sync mit Ihrem Mandanten synchronisiert werden. Ressourcenzuordnungen dieses Kontotyps dienen in tenfold lediglich zur Übersicht darüber, welche Personen tatsächlich über ein Hybridkonto in Microsoft 365 verfügen. Das Anlegen oder Aktualisieren dieser Konten mittels dieser Ressourcen ist nicht möglich.
Online	Hierbei handelt es sich um Benutzerkonten, welche ausschließlich in Ihrem Microsoft-365-Mandanten existieren. Sie haben kein synchronisiertes Active Directory Konto in Ihrer lokalen Umgebung. Konten dieser Art werden in tenfold mittels dieser Ressourcen angelegt, aktualisiert und gegebenenfalls entfernt.
Gast	Hierbei handelt es sich um Benutzer, welche, wie Online-Konten, nur in Microsoft 365 existieren. Hierbei handelt es sich jedoch um Benutzer aus fremden Mandanten, welche einen Gastzugriff auf Teilbereiche Ihres Mandanten erhalten haben. Diese werden über eine E-Mail eingeladen und können ebenso Rechte erhalten, wie Online-Konten. Die Lizenzierung seitens Microsoft unterscheidet sich jedoch von der der normalen Konten.

Sobald Sie die Einstellungen des Mandanten speichern wird für alle Kontotypen, welche Sie angewählt haben, eine Ressource erstellt. Diese wird auch gleichzeitig als Hauptressource für diesen Mandanten und den entsprechenden Typen markiert. Sollten Sie weitere Unterscheidungen für Konten auf demselben Mandanten benötigen (zum Beispiel Benutzer- und Administratorkonten), können Sie weitere Ressourcen in den Einstellungen des Microsoft 365 User Lifecycle Plugins anlegen. Für weitere Informationen zum Plugin, lesen Sie unter [Microsoft 365 User Lifecycle\(see page 803\)](#) nach.

7.2 Verwaltung der Active Directory Gruppen

7.2.1 Funktionalität

Benötigte Berechtigung

Um die Funktionen der Gruppenverwaltung nutzen zu können, muss der Benutzer entweder als Dateneigentümer einer Gruppe eingetragen sein oder über die Systemberechtigung "ADS Groups Administration" (8220) verfügen.

tenfold beinhaltet Funktionen zur Verwaltung der Gruppen in einer Active Directory Umgebung. Folgende Aktionen sind grundsätzlich über tenfold auslösbar:

- Erstellen von neuen Gruppen
- Ändern von Gruppen
- Löschen bestehender Gruppen
- Änderung der Mitgliedschaften einer Gruppe
- Festlegen der/des Eigentümer(s) einer Gruppe

Technischer Hinweis zu Fileservergruppen

Die Gruppenverwaltung in tenfold dient dazu, Organisationsgruppen zu verwalten. Diese Gruppen dienen dazu, Benutzer im Active Directory nach bestimmten organisatorischen Merkmalen zu gruppieren. Siehe hierzu auch: <https://en.wikipedia.org/wiki/AGDLP>.

Die Gruppenverwaltung in tenfold dient nicht dazu, interne Fileservergruppen zu bearbeiten. Diese Gruppen werden bei der Verwaltung von Fileserverberechtigungen automatisch erstellt und sollten auch nur über den Weg der Fileserverberechtigungen bearbeiten werden. Sie dazu auch: [Verwaltung der Fileserver-Berechtigungen\(see page 269\)](#). Die Fileservergruppen stehen aus Sicherheitsgründen bei der Gruppenverwaltung nicht zur Auswahl.

Wie bei allen Benutzer- oder Berechtigungsänderungen in tenfold werden diese durch die unterschiedlichen Aktionen nicht unmittelbar ausgeführt. Stattdessen wird ein entsprechender Request angelegt, welcher - konfigurationsabhängig - von den jeweiligen Verantwortlichen, die im Genehmigungsworkflow definiert werden, genehmigt werden muss, bis es zur tatsächlichen Ausführung kommt.

Workflow

Für alle Änderungen an Active Directory Gruppen wird der vordefinierte Workflow "ADS Request Approval" verwendet. Dieser Workflow kann entsprechend den Bedürfnissen angepasst werden. Es kann jedoch kein separater Workflow hinterlegt werden, sondern es muss dieser vordefinierte Workflow verwendet und angepasst werden.

7.2.2 Einstiegsmaske

Die Einstiegsmaske für die Gruppenverwaltung ist über das Menu unter Berechtigungen > Active Directory-Gruppen erreichbar. Die Maske gliedert sich in drei Bereiche:

- Links befindet sich der Suchbereich. Dieser wird genutzt, um Active Directory-Objekte zu suchen, um sie zu Gruppen hinzuzufügen. Der Bereich ist nur aktiv, wenn im mittleren Bereich der Abschnitt "Mitglieder", "Mitglied von" oder "Dateneigentümer" einer Gruppe selektiert ist.
- In der Mitte befindet sich der Zuordnungsbereich. Hier wird die Struktur der konfigurierten Domänen angezeigt. Darüber hinaus können die Mitglieder der jeweiligen Gruppen angezeigt werden. Sofern es neue oder offene Requests für Active Directory-Gruppen existieren, werden diese ganz oben im Zuordnungsbereich angezeigt.
- Rechts befindet sich der Informationsbereich, der detaillierte Informationen zum ausgewählten Objekt anzeigt.

Active Directory-Gruppe	
Bearbeiten	Löschen
Gruppenname	DS_Beauftragte
Gruppentyp	Sicherheitsgruppe
Gruppenbereich	Global
Beschreibung	TENFOLD
Domäne	TENFOLD
Verwaltet von	-
DN	CN=DS_Beauftragte,OU=Org-Groups,OU=Groups,OU=tenfold,DC=TENFOLD,DC=LOC
GUID	{3f109470-18ec-4f0c-8d05-9cd61b5539f9}
SID	S-1-5-21-3188900304-556115651-1426159621-1687

Neue Gruppe anlegen

Abhängig von der Konfiguration, die in der jeweiligen Domäne vorliegt, gibt es zwei unterschiedliche Wege, um eine neue Gruppe anzulegen:

- Wählt man im Bereich "Zuordnungen" eine Organisationseinheit aus, so kann anschließend im rechten Bereich "Organisationseinheit" der Button "Neue Gruppe" genutzt werden, um eine neue Gruppe in der ausgewählten Organisationseinheit anzulegen.
- Ist die Einstellung "Organisationsgruppen" (Einstellungen > Domänen > Tab "Organisationseinheiten") in der Domäne gesetzt, so ist der Button "Neue Gruppe" in der Titelzeile verfügbar. Die neue Gruppe wird in der Organisationseinheit angelegt, welche in der Einstellung "Organisationsgruppen" festgelegt ist. Die Organisationseinheit kann hierbei nicht angepasst werden.
- Ist diese Einstellung nicht gesetzt, so steht der Button in der Titelzeile nicht zur Verfügung.

Um eine neue Gruppe anzulegen, klicken Sie auf den Button "Neue Gruppe" in der Titelzeile oder im Detailbereich der ausgewählten Organisationseinheit. Es öffnet sich anschließend ein Dialog, in dem die Einstellungen für die neue Gruppe festgelegt werden können:

- Name: Name der neuen Gruppe (SAM-Account-Name)
- Anzeigename: Anzeigename der neuen Gruppe (displayName) .
- Gruppentyp: Sicherheitsgruppe oder Verteilergruppe
- Gruppenbereich: Global, Lokal oder Universell
- Beschreibung: Text, der den Zweck der Gruppe beschreibt
- Domäne: Domäne, in welcher die Gruppe angelegt werden soll (nur Anzeige)
- Verwaltet von: Welches AD-Objekt ist für die Gruppe verantwortlich
- Organisationseinheit: OE, in welcher die Gruppe angelegt werden soll (nur Anzeige)
- Bemerkung: Bemerkungstext für den Request in tenfold
- Ticketnummer: Ticketnummer für den Request in tenfold

Durch Klick auf den Speichern-Button scheint der Request in der Mitte der Maske (Zuordnungsbereich) unter "Neue Requests" auf. Er ist zu diesem Zeitpunkt noch nicht in der Datenbank gespeichert. Sie haben nun die Möglichkeit, weitere Requests anzulegen. Durch Klick auf den Speichern-Button auf der Hauptmaske werden alle neue Requests in der Datenbank gespeichert. Der weitere Verlauf hängt von der Konfiguration der Genehmigungsworflows ab.

7.2.3 Gruppeneinstellungen bearbeiten

Um die Einstellungen einer Gruppe zu bearbeiten, wählen Sie die gewünschte Gruppe in der Baumstruktur aus. Anschließend klicken sie im Detailbereich (rechts) auf "Bearbeiten".

Anschließend können Sie die Einstellungen der Gruppe bearbeiten. Um die Änderungen zu speichern, klicken Sie auf "Übernehmen". Sie können die Änderungen auch verwerfen, indem Sie auf "Abbrechen" klicken. Durch Klick auf den Übernehmen-Button scheint der Request für die Änderung in der Mitte der Maske (Zuordnungsbereich) unter "Neue Requests" auf. Er ist zu diesem Zeitpunkt noch nicht in der Datenbank gespeichert. Sie haben nun die Möglichkeit, weitere Requests anzulegen. Durch Klick auf den Speichern-Button auf der Hauptmaske werden alle neue Requests in der Datenbank gespeichert. Der weitere Verlauf hängt von der Konfiguration der Genehmigungsworflows ab.

Eine Gruppe vom Typ "Global" lässt sich nicht unmittelbar in eine Gruppe vom Typ "Lokal" umwandeln. Wenn Sie eine Gruppe vom Typ "Global" auf den Typ "Lokal" umstellen, so wandelt tenfold die Gruppe zuerst in den Typ "Universell" um und anschließend in den Typ "Lokal"

7.2.4 Mitgliedschaften bearbeiten / Dateneigentümer festlegen

The screenshot shows the tenfold Active Directory Groups interface. On the left, there's a search bar and a list of groups under 'Name', including 'Org.Einkauf'. The main area is titled 'Zuordnungen' (Assignments) and shows a tree view of organizational units (TENFOLD, Built-in, tenfold, Groups, Org-Groups). Under 'Org-Groups', 'DS_Beauftragte' is expanded, showing 'Mitglieder (2)' and 'Mitglied von (1)'. A yellow box highlights the 'Mitglied von (1)' entry. On the right, a 'Mitglied von' table lists 'Org.Einkauf' as a member of 'TENFOLD'. At the top, there are tabs for 'Neue Gruppe', 'Speichern', and 'Abbrechen'.

Um die Einstellungen einer Gruppe zu bearbeiten, wählen Sie die gewünschte Gruppe in der Baumstruktur aus.

1. Anschließend klicken Sie auf die Gruppe und wählen entweder den Eintrag "Mitglieder", "Mitglied von" oder "Dateneigentümer" aus.
2. Anschließend wird der Suchbereich auf der linken Seite der Maske aktiviert.
3. Suchen Sie über das Textfeld nach dem gewünschten AD-Objekt, welches Sie als Mitglied hinzufügen möchten.
4. Ziehen Sie das Objekt anschließend per Drag & Drop in den rechten Maskenbereich (während Sie das Objekt ziehen, verfärbt sich der Bereich, in dem Sie das Objekt auslassen können grün).

Je nachdem, welchen Abschnitt Sie zuvor aktiviert haben (Mitglieder, Mitglied von, Dateneigentümer), werden unterschiedliche Aktionen ausgelöst:

- Mitglieder: das Objekt wird Mitglied der ausgewählten Gruppe
- Mitglied von: die ausgewählte Gruppe wird Mitglied des Objekts
- Dateneigentümer: die ausgewählte Person wird zum Dateneigentümer der ausgewählten Gruppe

Die Veränderung einer Gruppenmitgliedschaft erzeugt einen neuen Request in der Mitte der Maske (Zuordnungsbereich). Das Festlegen des Dateneigentümers erzeugt keinen Request und wird sofort nach Klicken des Speichern-Buttons durchgeführt.

7.2.5 Gruppe löschen

Um die Einstellungen einer Gruppe zu bearbeiten, wählen Sie die gewünschte Gruppe in der Baumstruktur aus. Anschließend klicken Sie im Detailbereich (rechts) auf "Löschen".

Die Löschung muss anschließend bestätigt werden. Durch Klick auf den Löschen-Button scheint der Request in der Mitte der Maske (Zuordnungsbereich) unter "Neue Requests" auf. Er ist zu diesem Zeitpunkt noch nicht in der Datenbank gespeichert. Sie haben nun die Möglichkeit, weitere Requests anzulegen. Durch Klick auf den Speichern-Button auf der Hauptmaske werden alle neuen Requests in der Datenbank gespeichert. Der weitere Verlauf hängt von der Konfiguration der Genehmigungsworflows ab.

7.2.6 Gruppe umbenennen

Um eine Gruppe umzubenennen, wählen Sie die gewünschte Gruppe in der Baumstruktur aus. Anschließend klicken Sie im Detailbereich (rechts) auf "Bearbeiten".

Tragen Sie anschließend im Feld "Gruppenname" den neuen Namen der Gruppe ein und klicken auf "Übernehmen". Im Baumbereich wird die Gruppe daraufhin mit einem Stift-Icon markiert um anzuzeigen, dass die Gruppe bearbeitet wurde. Sie sehen auch oberhalb der Baumsicht einen neuen Bereich "Neue Requests" welcher den zu erstellenden Request für die Umbenennung der Gruppe enthält.

Klicken Sie auf "Speichern" um den Request zur Umbenennung zu erstellen. Sobald dieser genehmigt und durchgeführt wurde, ist die Gruppe im Active Directory umbenannt.

E-Mail-aktivierte Sicherheitsgruppen

E-Mail-aktivierte Sicherheitsgruppen von Exchange lassen sich mit den Standardeinstellungen von tenfold nicht umbenennen. Sie können dies über den Systemparameter (siehe [Systemparameter\(see page 484\)](#)) "Active Directory-Gruppen > E-Mail-aktivierte Gruppen umbenennen" aktivieren. **Achtung:** Beachten Sie, dass die Umbenennung von E-Mail-aktivierten Sicherheitsgruppen eine benutzerdefinierte Provisionierung benötigt. Seitens tenfold existiert keine standard Provisionierungslogik für die Umbenennung von E-Mail-aktivierten Sicherheitsgruppen.

7.2.7 Pathfinder

Sie können von einer Gruppe direkt in den Active Directory Pathfinder wechseln. Dazu wählen Sie die gewünschte Gruppe in der Baumstruktur aus und klicken im Detailbereich anschließend auf "Pathfinder". Es öffnet sich der Pathfinder mit der ausgewählten Gruppe im Mittelpunkt. Sie hierzu auch [Active Directory Pathfinder\(see page 348\)](#).

7.3 Verwaltung der Fileserver-Berechtigungen

7.3.1 Allgemeines

Benötigte Berechtigung

Um die Maske zur Verwaltung der Fileserver-Berechtigungen nutzen zu können, ist entweder eine administrative Berechtigung auf zumindest einem Fileserver erforderlich, oder der angemeldete Benutzer muss für zumindest einen Ordner auf einem der Fileserver als Dateneigentümer hinterlegt sein.

Sichten

Hat der angemeldete Benutzer die Systemberechtigung "Manage Fileservers" zugeordnet, so befindet er sich zu Beginn in der "Administratorsicht". Diese ermöglicht es, durch alle Verzeichnisse auf allen konfigurierten Fileservern zu navigieren. Ist der Benutzer lediglich als Dateneigentümer von einem oder mehreren Ordnern hinterlegt, so befindet er sich in der Dateneigentümersicht (erkennbar an dem Zusatz "Dateneigentümer" in der Überschrift). In dieser Sicht kann der Benutzer lediglich durch alle Verzeichnisse (und deren Unterverzeichnisse) navigieren, in denen er als Dateneigentümer hinterlegt ist. Verfügt ein Benutzer sowohl über die Systemberechtigung als auch über die Zuordnung als Dateneigentümer, so kann er über den Button "Dateneigentümermodus" beziehungsweise "Administratormodus" in der Titelzeile zwischen den Ansichten wechseln.

Folgende Funktionen stehen in der Dateneigentümersicht nicht zur Verfügung:

- Verzeichnis umbenennen (auf dem eigenen Verzeichnis, Unterverzeichnisse können umbenannt werden)
- Ablaufdatum setzen
- Verzeichnis löschen (das eigene Verzeichnis, Unterverzeichnisse können gelöscht werden)
- Vererbung ändern
- Dateneigentümer festlegen
- Einstellungen bearbeiten
- Verfügbarkeit festlegen
- Verzeichnis aktualisieren

Dateneigentümerberechtigungen

Die Aktionen, welche in der Dateneigentümer zur Verfügung stehen, hängen außerdem von den gesetzten Dateneigentümerberechtigungen ab. Näheres siehe [Dateneigentümer festlegen\(see page 289\)](#)

Aufbau

Die Maske zur Verwaltung der Fileserver-Berechtigungen ist wie alle tenfold-Masken aufgebaut, die Funktionen für das Berechtigungsmanagement in Microsoft® Systemen bereitstellen:

- auf der linken Seite befindet sich ein Baum der Ressourcen. Im Falle der Fileserver ist das der Verzeichnisbaum der hinterlegten Freigaben. Der Wurzelknoten ist die Freigabe selbst (es wird die Zeichenkette angezeigt, die als Anzeigename bei der Freigabenkonfiguration hinterlegt wurde).
- auf der rechten Seite befindet sich der Berechtigungsbaum, der über eine übersichtliche Baumstruktur die Berechtigungen auf dem auf der linken Seite ausgewählten Verzeichnis darstellt

7.3.2 Berechtigungen anzeigen

Fileserver	Vererbung aktiv	Anzahl	Größe
> \\WMI62247\projects			
\\WMI62247\org			
> Einkauf	5	0 Byte	
> Finanzen	6	0 Byte	
> IT	4	0 Byte	
> Personal	3	0 Byte	
> Produktion	4	0 Byte	
> Verkauf	5	0 Byte	
> \\WMI62247\home			

Details für Alle Berechtigungen (57)

Name	Anz. Zugriffspfade
Administrator	2
Arnhof, Ulrich	1
Bauer, Peter	1
Binder, Thomas	1
Brenner, Karl	1
Bruchmüller, Anita	1
Demel, Max	1
Ellmayer, Erich	1
Faber, Franz	1
Fuchs, Peter	1
Gans, Erich	1
Gans, Gustav	1
Glatz, Stefan	1
Gottlieb, Marie	1
Hofer, Georg	1
Huber, Ilse	1
Karner, Karl	1

Verzeichnisbaum

Um die Berechtigungen für ein bestimmtes Verzeichnis anzuzeigen, navigieren Sie auf der linken Seite zum gewünschten Verzeichnis und klicken Sie es an. Sobald Sie das Verzeichnis angeklickt haben, erscheint auf der rechten Seite ein Ladehinweis. Das System lädt nun die Berechtigungen, welche auf diesem Ordner gesetzt sind.

Wie greift tenfold zu?

Diese Daten werden aus der tenfold Datenbank geladen, es erfolgt kein ad-hoc Zugriff auf den Fileserver. Die Daten in der tenfold Datenbank wurden zuvor über den Agenten mit dem Fileserver synchronisiert. Dieser Abgleich findet üblicherweise einmal pro Tag statt. Dieses Intervall kann aber je nach Systemkonfiguration abweichen.

Anzeigebereich - Berechtigungsbaum

The screenshot shows the tenfold interface with the following structure:

- Fileserver** (selected tab)
 - Aktion ▾
 - Fileserver \\VMI62247\org
 - Domäne TENFOLD
 - Scan-Tiefe Keine Einschränkung
 - Bearbeitungstiefe Keine Einschränkung
 - Letzte Aktualisierung 25.10.2017 15:07:54
- Verzeichnis** (selected tab)
 - Berechtigungen Aktion ▾
 - \\VMI62247\org
 - Aus
 - Scan-Tiefe Fileserververeinstellung übernehmen (Keine Einschränkung)

Sobald die Berechtigungen im rechten Bereich geladen sind, werden folgende Informationen angezeigt:

- Der volle Name des Verzeichnisses, inklusive dem UNC-Pfad zum Server
- Der Status der Vererbung (An/Aus)
- Einstellung der Scan-Tiefe (bis zu welcher Verzeichnisebene liest tenfold die Struktur und Berechtigungen aus)

Wenn ein Top-Level-Eintrag (der Fileserver selbst) ausgewählt wird, werden zusätzlich folgende Informationen angezeigt:

- Domäne in dem sich der Fileserver befindet
- Einstellung der Scan-Tiefe (bis zu welcher Verzeichnisebene liest tenfold die Struktur und Berechtigungen aus)
- Einstellung der Bearbeitungstiefe (bis zu welcher Verzeichnisebene können über tenfold Berechtigungsänderungen durchgeführt werden)
- Zeitpunkt der letzten Aktualisierung des gesamten Fileservers (die Aktualisierung einzelner Verzeichnisse hat auf diese Information keinen Einfluss)

Berechtigungen							
	V	FC	MD	RX	LST	R	W
>Allgemeine Berechtigungen							
Ordnerinhalt anzeigen							
Vollzugriff							
FS.Admin							
Details für Alle Berechtigungen (367)							
Name	Anz. Zugriffspfade						
Abel, Susanne	2 ⚠						
Adam, Richard	1						
Administrator	2 ⚠						
Albrecht, Daniel	2 ⚠						
Almer, Ulf	1						
Amhof, Ulrich	2 ⚠						
Anwalt, Rudi	1						
Anzengruber, Alex	1						

Unterhalb der Verzeichnisinformationen wird der Berechtigungsbaum angezeigt. Der Berechtigungsbaum erlaubt es, ausgehend vom Wurzelknoten "Alle Berechtigungen" zu visualisieren, welche Berechtigungen auf

dem Ordner gesetzt sind. Je Berechtigung existiert ein weiterer Unterknoten. Folgende Möglichkeiten sind hierbei gegeben:

- Ordnerinhalt anzeigen
- Lesen & Ausführen
- Ändern
- Vollzugriff
- Spezielle Berechtigungen

Verweigern

Für jede Berechtigung kann es zusätzlich noch einen entsprechenden "Verweigern" Eintrag im Baum geben.

Wenn Sie im Berechtigungsbaum auf den Wurzelknoten klicken, öffnen sich die entsprechenden Unterknoten. Es werden jeweils nur die Berechtigungen angezeigt, für welche auch tatsächlich Objekte (Benutzer oder Gruppen) auf dem Ordner berechtigt sind.

Folgende Informationen sind in dieser Ansicht ersichtlich:

- Das jeweils berechtigte Objekt (das kann eine Gruppe oder ein Benutzer sein. Im Falle einer Gruppe kann diese aufgeklappt werden)
- Ein zugemachtes Schloss zeigt an, dass diese Berechtigung von oben vererbt wurde. Ein offenes Schloss zeigt an, dass diese Berechtigung auf dem Ordner initial gesetzt wurde.
- Die Häkchen in den Spalten FC (Full Control), MD (Modify), RX (Read & Execute), LST (List), R (Read) und W (Write) zeigen die einzelnen Berechtigungen an, die für den jeweiligen Benutzer/Gruppe gesetzt sind
- Die folgenden drei Symbole zeigen an, in welchem Modus dieses Berechtigung nach unten vererbt wird (Ordner, Unterordner, Dateien - von links nach rechts)

Anzeigebereich - Berechtigungspfade

Die untere Hälfte des Berechtigungsbereichs zeigt die Liste aller effektiv berechtigten Benutzer für die jeweilige Berechtigung an.

Dazu müssen Sie zuerst die Berechtigungsstufe auswählen, in dem Sie auf die jeweilige Berechtigungsstufe klicken (in diesem Beispiel auf "Lesen & Ausführen").

Die untenstehende Liste löst alle berechtigten (gegebenenfalls verschachtelten) Gruppen auf und zeigt deren Mitglieder gemeinsam mit etwaigen direkt gesetzten Benutzern an. Sie sehen daher eine Liste aller - über welchen Weg auch immer - berechtigten Benutzer, die das jeweils ausgewählte Recht auf dem aktuell selektierten Ordner haben. In Klammer wird die Anzahl der berechtigten Benutzer angezeigt.

Mehrfache Berechtigungen

Verfügt ein Benutzer über mehrere Zugriffsmöglichkeiten (zum Beispiel über verschiedene Gruppen), so wird der Benutzer lediglich ein Mal angezeigt. Die Zahl neben dem Benutzer zeigt dann die Anzahl der Zugriffspfade an. Sofern die Anzahl den Wert 1 überschreitet, so wird dies mit einem Warnhinweis verdeutlicht. Dies zeigt an, dass ein potentielles Problem beim Entzug der Berechtigung vorliegen könnte, das das Entfernen des Benutzers aus einer Gruppe nicht ausreicht, um die effektiven Berechtigungen zu entziehen.

Um die konkreten Berechtigungspfade für einen Benutzer anzuzeigen, klappen Sie den Eintrag für den jeweiligen Benutzer auf. Das System zeigt Ihnen an, welche Gruppen der Benutzer zur Ausübung der jeweiligen Berechtigung auf diesem Ordner nutzen kann.

Details für Alle Berechtigungen (367)	
Name	Anz. Zugriffspfade
▼ ⚡ Abel, Susanne	2 ⚠
📦 Org.Produktion	
📦 VMI62247_org_Finanzen_rx	
▼ ⚡ Adam, Richard	1
📦 Org.Verkauf	
> ⚡ Administrator	2 ⚠
> ⚡ Albrecht, Daniel	2 ⚠
> ⚡ Almer, Ulf	1

7.3.3 Historische Ansicht

Es ist möglich, die Verzeichnisstruktur und die Berechtigungen nicht nur für den aktuellen Zeitpunkt anzuzeigen, sondern zu einem beliebigen Zeitpunkt in der Vergangenheit zu wechseln.

Name	Anz. Zugriffspfade
Abel, Susanne	2 ⚠
Adam, Richard	1
Administrator	2 ⚠
Albrecht, Daniel	2 ⚠
Almer, Ulf	1

Um die Ansicht umzuschalten, verwenden Sie den Button "Datum auswählen" auf der Anzeigemaske. Es öffnet sich daraufhin ein Dialog, in dem der gewünschte Zeitpunkt ausgewählt werden kann. Anschließend werden die zum ausgewählten Zeitpunkt gültigen Daten geladen:

- Active Directory Benutzer, Gruppen und Gruppenmitgliedschaften
- Verzeichnisstruktur
- Berechtigungen auf den Verzeichnissen

Achtung

Historische Berechtigungen werden unter Umständen nicht immer angezeigt. Ist die Option "Historische Berechtigungen" in der Fileserver-Konfiguration auf den Wert "Immer ausblenden" gestellt, oder befinden Sie sich in der Dateneigentümeransicht und die Option ist auf den Wert "Für Dateneigentümer ausblenden" gestellt, so werden die entsprechenden Fileserver im Verzeichnisbaum nicht angezeigt und ein entsprechender Warnhinweis wird eingeblendet. Würde aufgrund der Einstellungen kein einziger Fileserver angezeigt, so ist der Button "Datum wählen" nicht verfügbar. Für die Einstellungen zur Anzeige historischer Berechtigungen siehe auch [Verwaltung der Fileserver-Berechtigungen](#)(see page 269).

7.3.4 Erweiterte Eigenschaften anzeigen

Wenn die entsprechenden Einstellungen für einen Fileserver aktiviert sind (siehe [Einrichtung der Fileserver](#)(see page 223)), können Sie sich die Anzahl der direkt vergebenen Berechtigungen auf den Verzeichnissen anzeigen lassen. Auch die Anzahl der Unterverzeichnisse, mit aufgebrochener Vererbung, lässt sich anzeigen.

The screenshot shows the tenfold web interface with the following details:

- Header:** tenfold, Personensuche, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, Einstellungen.
- Left Sidebar:** Fileserver (3) - Analyse und Änderung von Fileserverberechtigungen.
- Main Content:** A table titled "Fileserver" showing the following data:

Fileserver	Eigenschaften	Anzahl	Größe
> Organization	11	2	
Projects	5		
P110_Plans	2 (18,2%)	0 Byte (0,0%)	
P111_Moonshot	2 (18,2%)	0 Byte (0,0%)	
Documents	0 (0,0%)	0 Byte (0,0%)	
Planning	0 (0,0%)	0 Byte (0,0%)	
P112_Skydive	2	2 (27,3%)	0 Byte (0,0%)
P133_Upgrade	2	2 (18,2%)	0 Byte (0,0%)
P144_Rollouts	2 (18,2%)	0 Byte (0,0%)	
Sharing	1		
- Right Sidebar:**
 - Eigenschaften:** Anzahl expliziter Berechtigungen ausblenden, Anzahl unterbrochener Vererbungen ausblenden.
 - Berechtigungen:** V FC MD RX LST R W, Details für Alle Berechtigungen (1)
 - Details für Alle Berechtigungen (1):** Name: Administrator, Anz. Zugriffspfade: 3.

Klicken Sie hierfür im Kopfbereich der Maske auf die Schaltfläche "Eigenschaften", um ein Dropdown-Menü zu erhalten, in welchem Sie auswählen können, welche erweiterten Eigenschaften Sie anzeigen möchten. Diese Informationen können Ihnen dabei behilflich sein, die Berechtigungen auf Ihrem Fileserver aufzuräumen.

Mit der Anzahl expliziter Berechtigungen, sehen Sie wie viele Berechtigungen auf diesem Verzeichnis vergeben wurden. Gezählt werden dabei folgende Objekte:

- Gruppen und Konten, welche direkt auf dem Verzeichnis, über das Dateisystem, berechtigt sind.
Ausgenommen sind die von tenfold verwalteten Berechtigungsgruppen.

- Direkte Mitglieder (Gruppen und Konten) der von tenfold verwalteten Berechtigungsgruppen, welche auf dem Verzeichnis berechtigt sind. LST-Gruppen werden nicht berücksichtigt.

Vererbte Berechtigungen werden bei dieser Anzeige nicht berücksichtigt. Zweck dieser Ansicht ist es herauszufinden, wo im Verzeichnis Berechtigungen vergeben wurden, um diese nach Möglichkeit in höhere Ebenen zu ziehen, da es von Microsoft nicht empfohlen ist, Berechtigungen in zu tiefen Ebenen zu vergeben. Mit der Anzeige der aufgebrochenen Vererbungen finden Sie sehr schnell alle Ordner, in welchen die Vererbung aufgebrochen wurde. Da Microsoft generell nicht empfiehlt, die Vererbungen aufzubrechen (außer auf der Dateifreigabe selbst), können Sie diese Funktion benutzen, um leicht alle Verzeichnisse zu finden, wo ein Aufräumbedarf besteht.

Update von tenfold

Die notwendigen Informationen zur Anzeige dieser Daten, werden vom Job "Share Sync" gesammelt. Direkt nach einem Update von tenfold werden diese Daten also nicht angezeigt, bevor dieser Job nicht einmal gelaufen ist. **Hinweis: Es kann vorkommen, dass dieser Job ein zweites mal durchgeführt werden muss, bevor die Daten korrekt angezeigt werden.**

Aktualisierung der Daten

Da die Daten vom tenfold Agenten gesammelt werden anstatt live ausgewertet zu werden, kann es, nach einer Änderung der Verzeichnisse, zu einer temporär falschen Anzeige der Daten kommen. Die Anzeige wird bei den folgenden Ereignissen aktualisiert:

- Der Durchführung des Jobs "Share Sync"
- Bei der Änderung von Berechtigungen

Andere Änderungen, wie zum Beispiel das Ändern der Vererbung, lösen keine Aktualisierung der Daten aus. Auch die Aktion "Aktualisieren" einzelner Verzeichnisse führt nicht zu einer Aktualisierung dieser Anzeige.

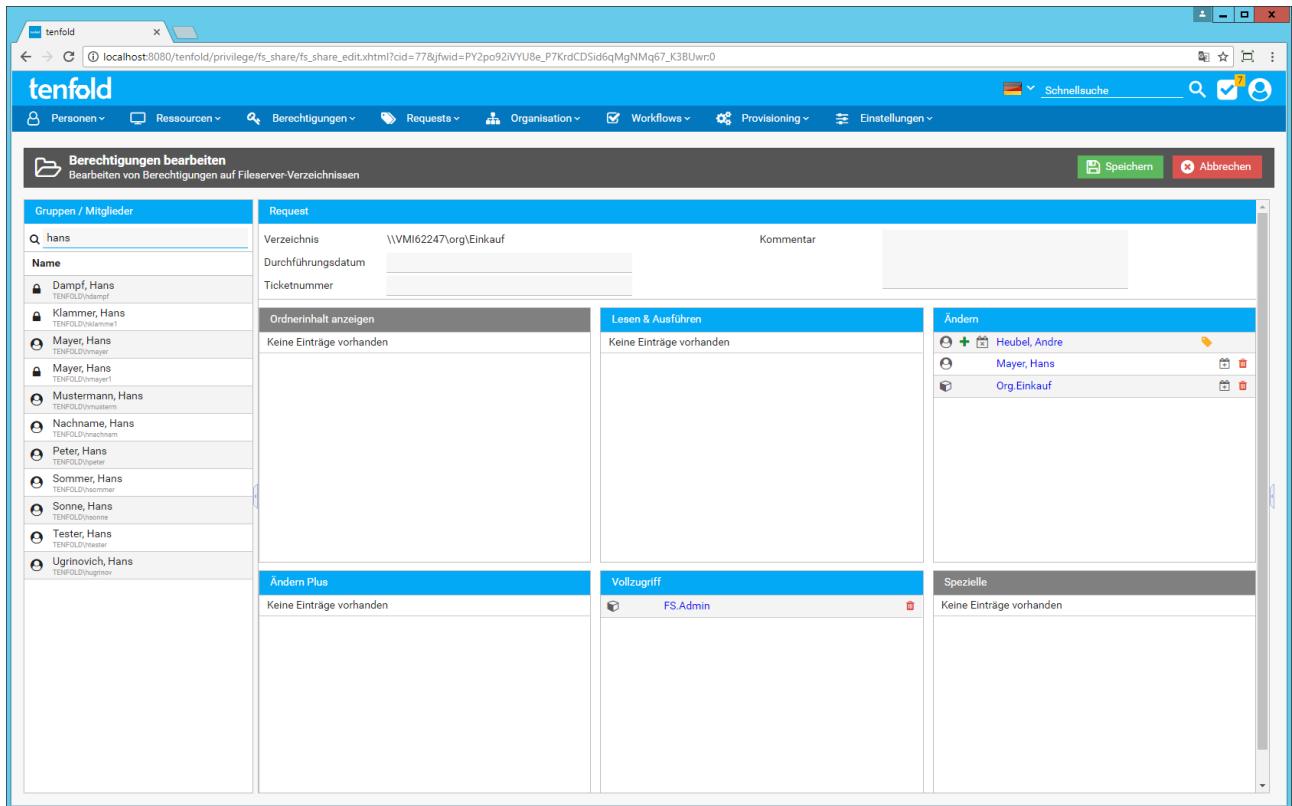
7.3.5 Verlauf anzeigen

Die Funktion "Verlauf" dient dazu, Änderungen, die auf einem Ordner durchgeführt wurden, zu visualisieren. Es gibt zwei Möglichkeiten, diese Änderungen anzuzeigen:

- Requests: Es wird eine Liste aller Änderungen dargestellt, die über einen Request, also ordnungsgemäß über tenfold, gemacht wurden. In der Auswahlliste "Request" kann die konkrete Änderung ausgewählt werden. Nach der Auswahl wird die Request-Ansicht unterhalb aktualisiert.
- Auditor: Das Verzeichnis wird in der Ansicht des Auditors gezeigt. Es werden - zusammenfassend - alle Änderungen in einem bestimmten Zeitraum gezeigt, wobei je Tag eine Anzahl dargestellt wird. Durch Klick auf die gewünschte Anzahl gelangen Sie auf eine detaillierte Aufstellung aller Änderungen. Im Falle des tenfold Auditors ist es unerheblich, ob die Änderung über tenfold selbst erfolgt ist, oder über andere Wege (z.B. den Microsoft-Tools). Dementsprechend sind in der Auditoransicht nicht alle Informationen wie in der Request-Ansicht verfügbar.

7.3.6 Berechtigungen bearbeiten

Um die Berechtigungen für einen Ordner zu bearbeiten, selektieren Sie zuerst den gewünschten Ordner und klicken Sie auf den Button "Berechtigungen" im Berechtigungsbereich (rechte Bildschirmseite).



Die Maske "Berechtigungen bearbeiten" besteht aus drei Teilen:

- Suche nach Benutzern und Gruppen (links)
- Berechtigungsfelder (Mitte)
- Detailinformationen (Rechts)

Alle Änderungen, die auf dieser Maske vorgenommen werden, werden erst als Request gesichert, wenn der Speichern-Button in der Toolbar betätigt wird. Alle Änderungen, die bis dahin ausgeführt werden, sind lediglich vorgemerkt. Um die Änderungen zu verwerfen, nutzen Sie den Abbrechen-Button in der Toolbar.

Berechtigungen anzeigen

In den Berechtigungsfeldern werden die aktuell gesetzten Berechtigungen angezeigt. Je Berechtigungsstufe existiert ein Feld. Die auf der jeweiligen Berechtigungsstufe zugeordneten Benutzer und Gruppen werden innerhalb des jeweiligen Berechtigungsfelds angezeigt. Das Icon kennzeichnet Benutzer mit einem Personensymbol und Gruppen mit dem Gruppensymbol. Das Symbol neben dem Personen- oder Gruppensymbol kennzeichnet den aktuellen Status der Berechtigung:

- Häkchen: Die Berechtigung ist aktuell zugeordnet.
- Stift: Die Berechtigung wird aktuell bearbeitet (zum Beispiel das Ablaufdatum wird angepasst)
- Plus: Die Berechtigung ist für eine neue Zuordnung vorgesehen
- Kreuz: Die Berechtigung ist zur Löschung vorgesehen

Neben der Bezeichnung des Objekts (Benutzer- oder Gruppenname) befinden sich zwei Buttons:

- Papierkorb: Diese Berechtigung löschen
- Kalender: Diese Berechtigung zeitlich befristen
- Rückgängig (kreisförmiger Pfeil): Die aktuelle Bearbeitung (zum Beispiel die Anpassung des Ablaufdatums) rückgängig machen

Vererbte Berechtigungen

Berechtigungen, die von einem übergeordneten Ordner vererbt werden, können nicht gelöscht oder zeitlich befristet werden. Sollen diese Berechtigungen entfernt werden, so muss dies am übergeordneten Ordner selbst gemacht werden.

Detailinformationen anzeigen

Details	
Mayer, Hans	
TENFOLD\hmayer	
S-1-5-21-3188900304-556115651-1426159621-1228	
CN=hmayer,OU=Wien,OU=tenfold,DC=TENFOLD,DC=LOCAL	
TENFOLD	
Mitglied von	
Name	
Domain Users	
NL.Wien	
Org.Verkauf	
Users	

Klickt man in einem Berechtigungsfeld auf ein Objekt (Benutzer- oder Gruppenname) so öffnet sich auf der rechten Seite die Anzeige der Detailinformationen. Auf dieser Ansicht werden folgende Informationen zum Benutzer oder der Gruppe angezeigt:

- Anzeigename
- Windows-2000-Anmeldename
- Security Identifier (SID)
- CN (Canonical Name)
- Domäne
- Mitglieder (für Gruppen) / Mitgliedschaften (für Benutzer)

Auflösung

Wird eine Gruppe ausgewählt, so befindet sich darunter eine Liste aller Mitglieder der Gruppe. Wird ein Benutzer ausgewählt, so befindet sich unterhalb eine Liste aller Gruppen des Benutzers. Die Anzeige der Mitglieder der Gruppe beziehungsweise der Mitgliedschaften des Benutzers umfasst nur die direkt zugeordneten Benutzer / Gruppen. Es erfolgt in dieser Ansicht keine automatische Auflösung dieser Objekte.

Neue Berechtigung setzen

Um eine neue Berechtigung für einen Benutzer oder eine Gruppe zu setzen, geben Sie zuerst einen Suchbegriff in der linken Seite der Maske in das Suchfeld ein.

Suchbegriff

Sie müssen mindestens 4 Zeichen eingeben, damit die Suche aktiviert wird.

Dieser Begriff kann sein:

- Anzeigename einer Gruppe
- Benutzername eines Benutzers
- Anzeigename eines Benutzers

Hinweis

Wenn Sie den genauen Benutzer- oder Gruppennamen nicht kennen, geben Sie einfach den Teil ein, der Ihnen bekannt ist. Sie müssen hierbei keine Wildcards (Platzhalter) wie "*" oder "%" nutzen.

Die Suche listet alle passenden Benutzer und Gruppen (erkennbar an den üblichen Symbolen) auf. Sie können diese nun per Drag & Drop in eines der Berechtigungsfelder ziehen. Der Eintrag erscheint daraufhin im gewählten Berechtigungsfeld mit einem Plussymbol. Dies kennzeichnet, dass die Berechtigung nun zur Zuordnung vorgesehen ist. Es bedeutet nicht, dass die Berechtigung schon zugeordnet ist. Der Request für die Änderung der Berechtigungen wird erst im System gespeichert, wenn sie den Speichern-Button in der Toolbar anwählen.

Berechtigungen befristen

Neues Ablaufdatum setzen	
<input type="text" value="Ablaufdatum"/>	<input checked="" type="button" value="Übernehmen"/> <input type="button" value="Abbrechen"/>
<input type="text" value="Kommentar *"/>	

Sie haben sowohl für bestehende als auch für gerade neu zuzuordnende Berechtigungen die Möglichkeit, diese zu befristen. Um eine Befristung einzustellen (oder eine bestehende Befristung zu ändern), klicken Sie auf das Kalendersymbol innerhalb der gewünschten Zeile im Berechtigungsfeld.

Bestehende Berechtigungen

Eine Befristung ist nur für Berechtigungen möglich, die über tenfold vergeben, oder im Vorfeld korrekt importiert wurden. Befristungen für bestehende, direkt gesetzte Berechtigungen sind nicht möglich.

Im Dialog, der sich durch Klick auf das Kalendersymbol öffnet, können Sie das gewünschte Enddatum sowie eine Begründung für die Befristung hinterlegen. Je nach eingestellter Konfiguration wird tenfold den Dateneigentümer des Verzeichnisses rechtzeitig vor Ablauf an die Befristung erinnern und dann die entsprechende Berechtigung automatisch zur Löschung beantragen. Abhängig von den Einstellungen ist die Eingabe eines Kommentars verpflichtend oder optional.

Berechtigung löschen

Bestehende Berechtigungen können gelöscht werden, indem Sie in der gewünschten Zeile, im jeweiligen Berechtigungsfeld, auf das Kreuzsymbol klicken. Für den Eintrag erscheint daraufhin ein Kreuzsymbol. Dies kennzeichnet, dass die Berechtigung nun zur Löschung vorgesehen ist. Es bedeutet nicht, dass die Berechtigung schon gelöscht wurde. Der Request für die Änderung der Berechtigungen wird erst im System gespeichert, wenn sie den Speichern-Button in der Toolbar angewählt haben.

Änderungen speichern

Um die Änderungen als Request zu speichern, klicken Sie abschließend auf den Speichern-Button in der Toolbar. Sie können, abhängig von der Konfiguration, zusätzliche folgende Informationen festlegen:

- Durchführungsdatum: Legt fest, dass die Durchführung frühestens zum angegebenen Datum gestartet werden soll. Sollte der Request zu diesem Zeitpunkt noch nicht genehmigt sein, verzögert dies die Durchführung zusätzlich.
- Ticketnummer: Ticketnummer, die im Request abgelegt werden soll. Hier kann beispielsweise eine Referenz zu einem Helpdesk-Ticket hinterlegt werden, welches die Änderung veranlasst hat.
- Kommentar: Es kann hier ein erklärender Kommentar, zum Beispiel eine Begründung für die Änderung, hinterlegt werden, welche zur Genehmigung durch den Dateneigentümer erforderlich ist.

Durch das Speichern werden die gewünschten Änderungen als Request in der Datenbank abgelegt. Die tatsächliche Durchführung der Änderung hängt vom hinterlegten Genehmigungsworkflow sowie anderen Einstellungen ab.

Undurchführbare Änderungen

Wenn tenfold während der Request-Durchführung feststellt, dass Berechtigungen auf einem DFS-Link oder der obersten Ebene einer Dateifreigabe gesetzt würden und auf diesen Verzeichnissen die Berechtigungsvererbung aktiv ist, lässt tenfold den Request mit einer entsprechenden Fehlermeldung fehlschlagen. Es ist dabei unerheblich, ob die Berechtigung durch die Erzeugung von LST-Gruppen in Überverzeichnissen oder durch die Vergabe einer Berechtigung direkt auf den Verzeichnissen erfolgen würde. Eine Vergabe von Berechtigungen in diesen Konstellationen kann zum Verlust von Berechtigungen führen.

Hinweis: Sollte tenfold feststellen, dass so eine Konstellation vorliegt, wird der Request sofort fehlschlagen und es werden **keine** Berechtigungen angelegt. Es werden also auch in den Unterverzeichnissen keine Berechtigungen angelegt, wenn festgestellt wird, dass auf oberster Ebene eine LST-Gruppe erzeugt werden würde.

7.3.7 Berechtigungsbericht

Es gibt nicht nur die Möglichkeit, die Berechtigungen für ein Verzeichnis und dessen Unterverzeichnisse online anzuzeigen, sondern auch diese in eine PDF- oder Excel-Datei zu exportieren. Dazu wählen Sie das gewünschte Verzeichnis aus und wählen im rechten Bildschirmbereich das Menü "Aktion", Unterpunkt "Bericht". Es gibt zwei Wege, um einen Bericht zu erstellen: als benutzerdefinierten Bericht, in dem alle Optionen individuell festgelegt werden können, oder als Berichtsvorlage, bei welcher die Optionen zuvor

festgelegt wurden und nicht individuell verändert werden können. Welche Möglichkeiten dabei zur Verfügung stehen hängt von den Einstellungen ab (siehe [Einrichtung der Fileserver\(see page 223\)](#)):

Benutzerdefinierte Berichte können nur erstellt werden, wenn die Option bei den Fileserver-Einstellungen berücksichtigt wurde. Wenn die Fileserver-Maske im Administrator-Modus geöffnet ist, ist dabei die Einstellung "Benutzerdefinierte Berichte" auf dem Karteireiter "Allgemein" der Fileserver-Einstellungen entscheidend. Ist die Maske im Dateneigentümer-Modus geöffnet, muss die gleiche Option auf dem Karteireiter "Dateneigentümer" ausgewählt sein. Darüber hinaus kann je Vorlage gesteuert werden, ob diese im Dateneigentümer-Modus oder nur im Administrator-Modus zur Verfügung steht.

Um die Optionen individuell festzulegen, wählen Sie die Kachel "Benutzerdefinierter Bericht". Um Berichte mit Voreinstellungen zu wählen, klicken Sie die gewünschte Kachel an, um den Bericht mit dieser Vorlage zu erstellen. Es können dann keine individuellen Einstellungen getroffen werden.

Für benutzerdefinierte Berichte stehen folgende Optionen zur Verfügung:

Option	Bedeutung
Format	Wählen Sie das gewünschte Dateiformat. PDF ist für die Archivierung und den E-Mail-Versand besser geeignet. Excel ist die bessere Wahl, wenn Sie den Bericht nachbearbeiten wollen.

Option	Bedeutung
Gruppen aufbrechen	Ist diese Option angewählt, so werden im Bericht keine Gruppen verwendet. Stattdessen werden die Gruppen, gegebenenfalls auch über mehrere Ebenen, bis auf einzelne Benutzer aufgelöst. Das erhöht die Verständlichkeit des Berichtes für nicht-IT-Administratoren erheblich. Hinweis: Gruppen, deren Mitgliedschaften dynamisch festgelegt werden (z.B. "Authenticated Users") werden auf dem Bericht nicht aufgebrochen, selbst, wenn diese Option angewählt wurde, da die aktuelle Liste der Mitglieder systemseitig nicht festgestellt werden kann.
Vererbung	Diese Option steuert, ob vererbte Berechtigungen Teil des Berichtes sein sollen, oder ob diese ausgeblendet werden sollen. Es wird empfohlen, die Option "Aus" zu wählen.
Gesperrte Benutzer ausschließen	Mit dieser Option wird gesteuert, ob im Active Directory gesperrte Benutzer aus dem Bericht ausgeschlossen werden sollen. Im Normalfall haben gesperrte Benutzer keine Möglichkeit, sich interaktiv anzumelden, womit auch die Möglichkeit auf Ordner zuzugreifen verschlossen ist. Es wird daher empfohlen gesperrte Benutzer auszuschließen. Werden gesperrte Benutzer nicht ausgeschlossen, so sind sie im Bericht in grauer Schrift und kursiv ausgewiesen.
BUILTIN ausschließen	Wenn diese Option gewählt ist, werden BUILTIN-Gruppen gänzlich aus dem Bericht ausgeschlossen. Dies macht insbesondere dann Sinn, wenn ein Bericht für einen Endanwender erstellt wird, dem diese internen IT-Systemgruppen unbekannt sind.
BUILTIN aufbrechen	Zusätzlich kann definiert werden, ob auch sogenannte BUILTIN-Gruppen aufgelöst werden sollen. BUILTIN Gruppen sind zum Beispiel "Administratoren" und "Sicherungs-Operatoren".
Unterverzeichnisse	Steuert, ob Unterverzeichnisse des aktuell gewählten Verzeichnisses ebenfalls exportiert werden sollen. Zusätzlich kann die Eingabe der maximalen Anzahl an Ebenen erfolgen.
Delta generieren	Gibt an, ob auf dem Bericht für jedes Verzeichnis jeweils nur die Änderungen zum übergeordneten Verzeichnis angezeigt werden sollen. Dies verkürzt die Reportlänge deutlich und ist zu empfehlen. Diese Option blendet nicht einfach alle vererbten Berechtigungen aus, sondern wirkt auf effektive Veränderungen. Ist für einen Ordner beispielsweise die Vererbung deaktiviert, wird aber ein Objekt auf dem Ordner initial exakt so berechtigt, wie es durch Vererbung auch berechtigt würde (gleiches Objekt ist am übergeordneten Ordner gleich berechtigt), so scheint diese Berechtigung anschließend nicht auf, da es sich um kein effektives Delta handelt.
Unveränderte Berechtigungen anzeigen	Diese Option steuert, wie mit Berechtigungen umgegangen wird, die sich nicht verändert haben (kein Delta), wenn die Option "Delta generieren" gesetzt wurde. "Immer" bedeutet, dass alle nicht veränderten Berechtigungen immer gekennzeichnet werden (dies erfolgt im Bericht mit einem speziellen Symbol).

Option	Bedeutung
Berichtigungsstufen auswählen	Sie können mit diesen beiden Listen steuern, welche Berechtigungen Teil des Berichts sein sollen. Alle Berechtigungen auf der rechten Seite werden ausgeschlossen und sind am Bericht nicht sichtbar.
Active Directory Kategorien ausschließen	Mit dieser Option ist es möglich, Active Directory Kategorien auszuschließen. Alle in den auszuschließenden Kategorien definierten Objekte werden am Bericht nicht angezeigt. Befindet sich in der Kategorie eine Gruppe, so wird diese ausgeblendet, sofern die Option "Gruppen aufbrechen" nicht aktiviert ist. Ist die Option aktiviert, so werden alle Mitglieder der betroffenen Gruppe ausgeblendet (allerdings nur, wenn sie über diese Gruppe berechtigt sind. Sind sie - eventuell zusätzlich - über eine andere Gruppe berechtigt, werden sie nicht ausgeblendet). Siehe dazu auch Verwaltung der Fileserver-Berechtigungen (see page 269).
Active Directory Objekte ausschließen	Hier können Benutzer und Gruppen definiert werden, für die Berechtigungen am Bericht ausgeschlossen werden sollen.
Nur bestimmte Active Directory Objekte berücksichtigen	Sind hier Benutzer oder Gruppen definiert, so werden nur diese Teile des Berichtes. Berechtigungen aller anderen Objekte werden nicht angezeigt.

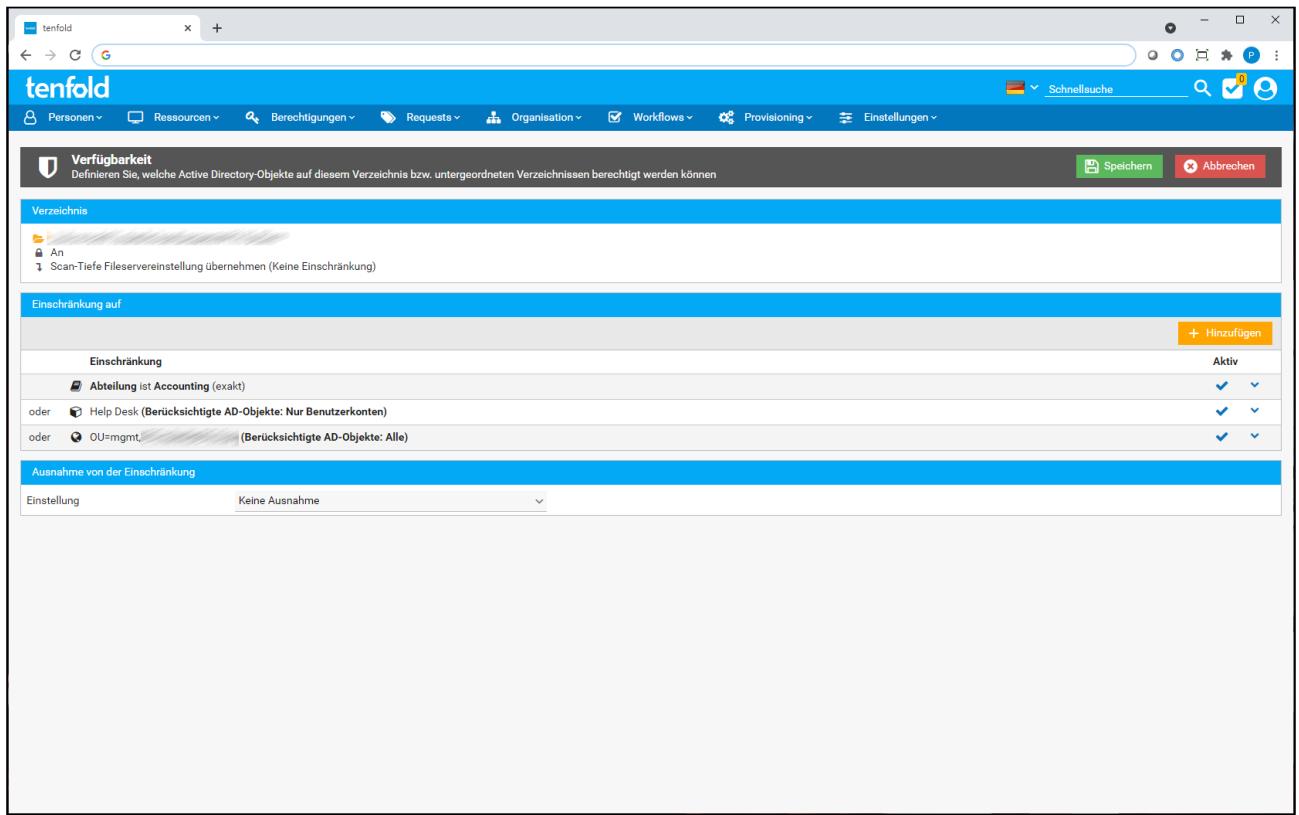
Die gewählten Einstellungen können direkt als neue Vorlage gespeichert werden (Button "Speichern als Vorlage"). Dazu ist die Systemberechtigung "Manage Report Templates" (3200) erforderlich.

Existierende Berichte

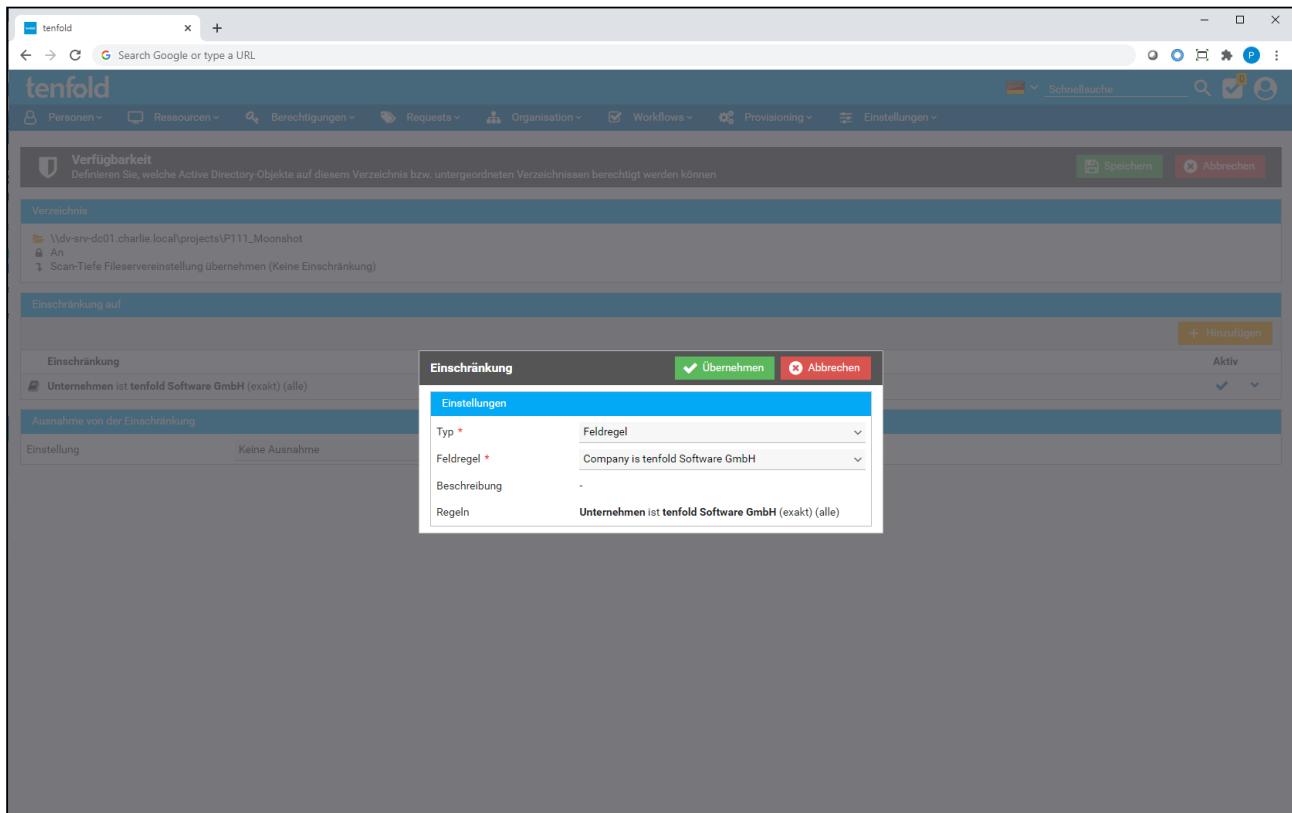
Wenn Sie eine Auswertung starten, so wird das Ergebnis der Auswertung in der Datenbank gespeichert. Sie können jederzeit auf alte Berichte zugreifen, indem Sie auf das Box-Symbol in der Toolbar klicken. Hier können Sie nun diese archivierten Ergebnisse erneut als PDF oder Excel-Datei exportieren.

7.3.8 Verfügbarkeit festlegen

Durch Festlegen der Verfügbarkeit lässt sich einschränken, welchen Benutzern mittels tenfold auf einem Verzeichnis Berechtigungen erteilt werden können.



Sie erreichen diese Maske über die Aktion "Verfügbarkeit" unter dem Menüpunkt "Aktion" eines Verzeichnisses. Im Bereich "Einschränkung auf" können Sie mehrere Einschränkungen hinzufügen. Um eine Einschränkung hinzuzufügen, klicken Sie auf die Schaltfläche "Hinzufügen". Es öffnet sich ein Dialog, in welchem sich die Bedingungen bearbeiten lassen.



Es lassen sich folgende Einschränkungen treffen:

- Feldregel
- Organisationseinheit
- Active Directory Gruppe

Nachdem Sie im Dropdown einen der Einschränkungstypen ausgewählt haben, erscheinen die entsprechenden Einstellungen dazu.

Einstellung	Beschreibung
Typ "Feldregel"	
Feldregel	Mit dieser Feldregel wird eingeschränkt, dass nur Benutzerkonten, die zu Personen gehören, die auf diese Regel zutreffen, Berechtigungen für dieses Verzeichnis erhalten können.
Beschreibung	Die Beschreibung, welche bei der Feldregel hinterlegt wurde (nur lesend).
Regeln	Die textuelle Beschreibung der Bedingungen, welche in der Regel hinterlegt sind. Diese wird automatisch von tenfold generiert (nur lesend).
Typ "Organisationseinheit"	
Organisationseinheit	Das Objekt muss in der ausgewählten Organisationseinheit oder darunter liegen.

Berücksichtigte AD-Objekte	Hier können Sie auswählen, ob Berechtigungen an alle Objekte oder nur an Benutzerkonten vergeben werden können.
Typ "Active Directory-Gruppe"	
Active Directory-Gruppe	Nur Mitglieder dieser AD-Gruppe können Berechtigungen auf dem Verzeichnis erhalten. Es werden nur direkte Mitglieder der Gruppe akzeptiert.
Berücksichtigte AD-Objekte	Legt fest, ob alle Mitglieder der Gruppe berücksichtigt werden oder nur Benutzerkonten.

Nachdem Sie die Einschränkungen gespeichert haben, können in tenfold Berechtigungen für dieses Verzeichnis nur noch an Objekte, die zumindest eine der Bedingungen erfüllen, vergeben werden.

Berechtigungsvergabe außerhalb von tenfold

Die oben angeführten Einstellungen verhindern nicht, dass Berechtigungen auch außerhalb von tenfold vergeben werden können.

Im Bereich "Ausnahme von der Einschränkung" kann festgelegt werden, welche tenfold-Benutzer diese Einschränkungen ignorieren dürfen. Wenn Sie im Dropdown die Option "Personen mit Berechtigung" wählen, erscheint eine weitere Option, in welcher Sie die gewünschte Berechtigung auswählen können. Sämtliche tenfold-Benutzer mit dieser Berechtigung können Verzeichnisberechtigungen auf diesem Verzeichnis erteilen, ohne Rücksicht auf die hier getroffenen Einschränkungen.

7.3.9 Weitere Aktionen

Die nachfolgenden Aktionen sind allesamt über den Menüpunkt "Aktion" zu erreichen.

Berechtigungen

Die Verfügbarkeit der genannten Aktionen ist von den tenfold-Berechtigungen des jeweiligen angemeldeten Benutzers abhängig.

Verzeichnis anlegen

Mit dieser Option kann ein neues Verzeichnis als Unterverzeichnis des aktuell ausgewählten Verzeichnisses angelegt werden. Es müssen folgende Daten erfasst werden:

- Name: Der gewünschte Name des Verzeichnisses
- Vorlage: Eine Vorlage nach welcher das Verzeichnis angelegt wird. Damit diese Einstellung angezeigt wird, muss für das Verzeichnis eine Vorlage definiert sein.
- Vererbung: Bestimmt, ob das Verzeichnis die Berechtigungen des übergeordneten Verzeichnisses übernehmen soll (empfohlen).
- Scan-Tiefe: definiert eine abweichende Scan-Tiefe zur Einstellung auf dem Fileserver. Es wird empfohlen, diese Einstellung nicht zu verändern.
- Bemerkung: hier kann eine Begründung für das neue Verzeichnis eingegeben werden. Je nach Konfiguration (Systemparameter "Fileserver > Verzeichnis erstellen - Kommentar verpflichtend") ist die Angabe verpflichtend oder optional.

- Ticketnummer: Ticketnummer, die im Request abgelegt werden soll. Hier kann beispielweise eine Referenz zu einem Helpdesk-Ticket hinterlegt werden, welches die Änderung veranlasst hat.

Je nach Konfiguration führt das Speichern des Dialogs nicht automatisch dazu, dass die gewünschte Aktion ausgelöst wird. Ist ein Genehmigungsworkflow vorgesehen, ist gegebenenfalls zuerst die Genehmigung des Dateneigentümer erforderlich. Je nach Konfiguration wird dieser automatisch von tenfold informiert.

Verzeichnis umbenennen

Diese Aktion erlaubt es, den Namen eines Verzeichnisses über tenfold zu ändern.

Verfügbarkeit

Diese Funktion steht aktuell nur in der Administratoransicht zur Verfügung. Dateneigentümer können diese Funktion nicht nutzen, da die Umbenennung weitreichende Folgen im Active Directory nach sich ziehen kann.

Soll ein Verzeichnis umbenannt werden, so muss der neue Name sowie - konfigurationsabhängig - ein Kommentar als Begründung angegeben werden. Je nach Konfiguration führt das Speichern des Dialogs nicht automatisch dazu, dass die gewünschte Aktion ausgelöst wird. Ist ein Workflow vorgesehen, ist gegebenenfalls zuerst die Genehmigung des Dateneigentümer erforderlich. Je nach Konfiguration wird dieser automatisch von tenfold informiert.

Als Folge der Umbenennung werden auch alle etwaige Berechtigungsgruppen für den Ordner sowie für alle Unterordner entsprechend dem neuen Namen und der hinterlegten Namenskonvention (siehe dazu auch [Verwaltung der Fileserver-Berechtigungen](#)(see page 269)) umbenannt. Da diese Aufgabe bei vielen Berechtigungsgruppen einige Minuten Verarbeitungszeit in Anspruch nehmen kann, wird der Request als geplanter Request im Hintergrund ausgeführt. Der Benutzer erhält sofort eine Rückmeldung und kann weiterarbeiten.

Verzeichnis löschen

Mit dieser Option kann das aktuell ausgewählte Verzeichnis gelöscht werden. Es muss - konfigurationsabhängig (Systemparameter "Fileserver > Verzeichnis löschen - Kommentar erforderlich") - eine Begründung angegeben werden. Je nach Konfiguration führt das Speichern des Dialogs nicht automatisch dazu, dass die gewünschte Aktion ausgelöst wird. Ist ein Workflow vorgesehen, ist gegebenenfalls zuerst die Genehmigung des Dateneigentümer erforderlich. Je nach Konfiguration wird dieser automatisch von tenfold informiert.

Vererbung ändern

Diese Funktion ermöglicht es, die aktuelle Einstellung der Vererbung zu ändern.

- Für Verzeichnisse mit aktiverter Vererbung ist es möglich, diese aufzuheben. Es gelten dann für diese Verzeichnisse neue Berechtigungen.
- Für Verzeichnisse, in denen die Vererbung deaktiviert wurde, besteht die Möglichkeit, diese wiederherzustellen und dies für alle untergeordneten Verzeichnisse ebenfalls zu übernehmen. Damit wird die Vererbung für den Ordner samt aller Unterordner wiederhergestellt.

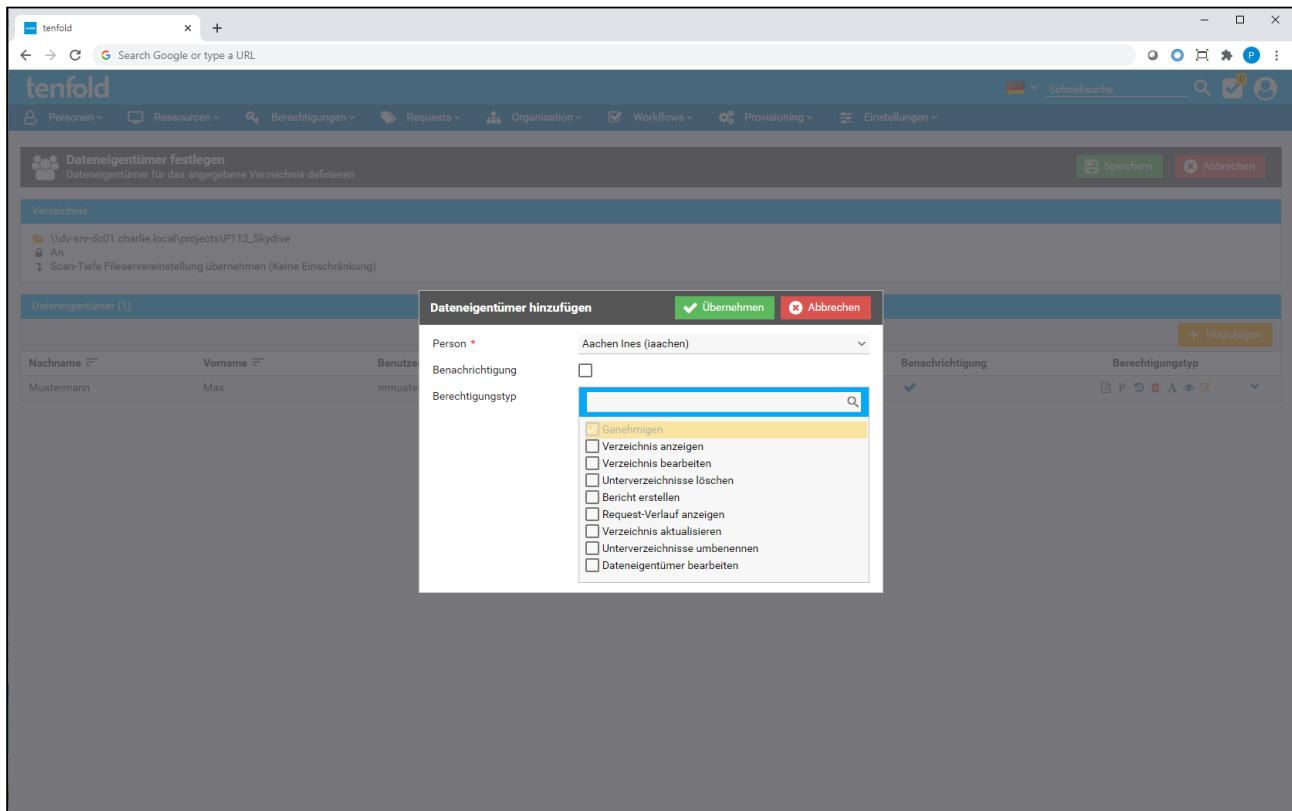
Vererbung

Für die Ordnung auf den Fileservern ist es dringend empfohlen, Unterbrechungen in der Vererbung zu vermeiden. In fast allen Fällen kann der gewünschte Effekt durch eine bessere Strukturierung der Ordner und Berechtigungen erzielt werden.

Dateneigentümer festlegen

Nachname	Vorname	Benutzername	Personalnummer	Abteilung	Benachrichtigung	Berechtigungstyp
Mustermann	Max	mmusterm	656471	Information technology	<input checked="" type="checkbox"/>	

Über diese Funktion können die Verantwortlichen für einen Ordner festgelegt werden. Um einen neuen Dateneigentümer festzulegen, klicken Sie auf den Button "Hinzufügen". Über das Suchfeld können Personen ausgewählt werden. Durch Klick auf den Button "Übernehmen" wird die ausgewählte Person als neuer bzw. zusätzlicher Dateneigentümer definiert. Der Dateneigentümer kann, je nach Konfiguration, die Aufgabe übernehmen, Berechtigungsänderungen auf dem Ordner zu genehmigen. Das Kontrollkästchen "Benachrichtigung" steuert, ob der jeweilige Dateneigentümer bei Anlage eines neuen Requests für den Ordner automatisch benachrichtigt wird. Darüber hinaus kann eingestellt werden, welche besonderen Berechtigungen Dateieigentümer auf ihren Verzeichnissen in tenfold erhalten.



Die Berechtigungen haben folgende Auswirkungen auf die Aktionen, welche der Dateneigentümer in seiner Ansicht in tenfold durchführen kann.

Berechtigung	Beschreibung
Genehmigen	Erlaubt es Dateneigentümern (sofern sie im Genehmigungsworkflow hinterlegt sind), ihre Genehmigungsschritte zu genehmigen. Alle Dateneigentümer verfügen über diese Berechtigung. Sie kann nicht entzogen werden.
Verzeichnis anzeigen	Diese Berechtigung erlaubt es Dateneigentümern, die Dateneigentümeransicht für dieses Verzeichnis zu benutzen. Sie ist Grundvoraussetzung für alle anderen Berechtigungen und wird automatisch aktiviert und kann nicht mehr abgewählt werden, sobald eine andere Berechtigung erteilt wird. Dateneigentümer, die diese Berechtigung nicht haben, können zwar Requests genehmigen, haben jedoch keine Einsicht in die Daten.
Verzeichnis bearbeiten	Erlaubt es dem Dateneigentümer, die Berechtigungen für sein Verzeichnis sowie für die darunter liegenden Verzeichnisse zu bearbeiten. Außerdem darf der Dateneigentümer mit dieser Berechtigung neue Unterverzeichnisse anlegen.

Berechtigung	Beschreibung
Unterverzeichnisse löschen	Mit dieser Berechtigung darf ein Dateneigentümer Verzeichnisse, welche unterhalb seines Verzeichnisses liegen, löschen. Das Verzeichnis, auf welchem der Dateneigentümer gesetzt ist, kann vom Dateneigentümer nicht gelöscht werden. Wird diese Berechtigung ausgewählt, wird automatisch "Verzeichnis bearbeiten" mit ausgewählt und kann nicht mehr abgewählt werden.
Bericht erstellen	Erlaubt es Dateneigentümern, Berichte zu den Verzeichnisberechtigungen zu erstellen.
Request-Verlauf anzeigen	Mit dieser Berechtigung ist es Dateneigentümern gestattet, die Historie erzeugter Requests für das Verzeichnis und dessen Unterverzeichnisse anzuzeigen.
Verzeichnis aktualisieren	Diese Berechtigung erlaubt es Dateneigentümern, die Aktion "Aktualisieren" zu verwenden, welche tenfold anweist, die Berechtigungen des gewählten Verzeichnisses neu einzulesen.
Unterverzeichnisse umbenennen	Mit dieser Berechtigung darf ein Dateneigentümer Verzeichnisse, welche unterhalb seines Verzeichnisses liegen, umbenennen. Das Verzeichnis, auf welchem der Dateneigentümer gesetzt ist, kann vom Dateneigentümer nicht umbenannt werden. Wird diese Berechtigung ausgewählt, wird automatisch "Verzeichnis bearbeiten" mit ausgewählt und kann nicht mehr abgewählt werden.
Dateneigentümer bearbeiten	Wird diese Berechtigung ausgewählt, kann der Dateneigentümer weitere Dateneigentümer hinzufügen oder bestehende Dateneigentümer entfernen.
Vererbung aufheben oder wiederherstellen	Erlaubt es dem Dateneigentümer, die Funktionen zur Veränderung der Vererbungseinstellungen zu benutzen.

Dateneigentümberechtigungen auf dem Dateisystem

Beachten Sie, dass die Dateneigentümberechtigungen **keine** Auswirkungen darauf haben, welche Operationen der Dateneigentümer auf dem Dateisystem durchführen darf. Diese Einstellungen wirken sich nur auf mögliche Aktionen in tenfold aus.

Vererbung

Dateneigentümer werden standardmäßig auf Unterordner vererbt. Wird auf einem Unterordner jedoch ein neuer Dateneigentümer hinterlegt, so endet die Kompetenz des übergeordneten Dateneigentümers an diesem Ordner. Soll der übergeordnete Dateneigentümer auch für diesen untergeordneten Ordner als Dateneigentümer fungieren, so muss er an dieser Stelle zusätzlich hinterlegt werden.

Lassen Sie, nach Möglichkeit, Ihre Dateneigentümer Stellvertreter (siehe [Stellvertretungen](#)(see page 372)) eintragen, damit es, im Falle von Abwesenheiten, nicht zu starken Verzögerungen kommt. Zur Not können auch tenfold-Administratoren Stellvertreter für andere Benutzer festlegen.

Administration

Nur durch Festlegen des Dateneigentümers wird dieser nicht in den Workflow mit eingebunden. Der Dateneigentümer muss auch eine entsprechende Stellung im gewählten Genehmigungsworkflow einnehmen. Dieser Workflow regelt global die Verfahrensmuster für Genehmigungen auf Fileservern.

Ein bestehender Dateneigentümer kann, im Kontextmenü der Tabelle, mit dem Eintrag "Löschen" wieder entfernt werden. Mit der Aktion "Bearbeiten" im Kontextmenü, können die Einstellungen des Dateneigentümers angepasst werden.

Einstellungen

Bei dieser Funktion können folgende Einstellungen für das ausgewählte Verzeichnis festgelegt werden:

- Scan-Tiefe: Setzt für das Verzeichnis eine von der Konfiguration des Fileservers abweichende Scan-Tiefe. Es wird empfohlen, diese Einstellung unverändert zu lassen, wenn es keinen dringenden Grund zur Anpassung gibt.
- Self-Service erlauben: Diese Einstellung steuert, ob das Verzeichnis auf der Self-Service-Oberfläche zur Verfügung steht. Sie können hiermit die allgemeinen Einstellungen für den Fileserver überschreiben.
- Genehmigungsworkflow: Legt einen individuellen Genehmigungsworkflow für dieses Verzeichnis fest. Mit "Fileserver-Einstellung übernehmen" wird der Genehmigungsworkflow beibehalten, welcher beim Fileserver hinterlegt wurde. Ist auch dort keiner hinterlegt, wird der Standardworkflow "Fs request approval" verwendet.

Ablaufdatum setzen

Über den Menüpunkt "Ablaufdatum setzen" kann für den Ordner ein Ablaufdatum in tenfold hinterlegt werden. Zum Zeitpunkt des Ablaufdatums wird der Ordner automatisch (mittels eines Requests) von tenfold gelöscht.

Dateisystem

Da diese Einstellung rein von tenfold verwaltet wird und auf dem Dateisystem keine entsprechende Einstellung dafür existiert, scheint das Ablaufdatum nur in tenfold auf. Es ist nirgendwo sonst einsehbar.

Aktualisieren

Diese Funktion startet einen Scan des ausgewählten Verzeichnisses (mitsamt aller Unterverzeichnisse) und aktualisiert die Verzeichnisstruktur bzw. die Berechtigungen in tenfold mit den tatsächlich am Fileserver vorhandenen Strukturen. Die Funktion wird dann benötigt, wenn eine Aktualisierung akut erforderlich ist (zum Beispiel, wenn ein gerade am Fileserver direkt angelegtes Verzeichnis berechtigt werden soll).

Periodische Scans

Konfigurationsabhängig werden alle Fileserver periodisch (üblicherweise täglich) gescannt und die zugehörigen Daten in tenfold aktualisiert.

7.3.10 Microsoft DFS

Wie normale Dateifreigaben auch unterstützt tenfold das Einlesen und Verwalten von Microsoft DFS-Namespaces. Es gibt hier jedoch Besonderheiten, auf die zu achten ist.

DFS Support

In tenfold werden nur domänenbasierte Namespaces mit aktiviertem Windows Server 2008-Modus unterstützt.

Eine als DFS konfigurierte Dateifreigabe kann im Netzwerk über verschiedene Pfade angesprochen werden. Zum Beispiel:

- \\<Domänenname>\<DFS-Namespace>
- \\<Domänen-FQDN\<DFS-Namespace>
- \\<Fileserver-Name>\<DFS-Namespace>

Wenn man einen Fileserver in tenfold einrichtet, kann prinzipiell jeder dieser Pfade verwendet werden, um die Dateifreigabe einzulesen (auch Pfade unterhalb des Namespaces können verwendet werden). Fileserver werden jedoch nur als DFS erkannt, wenn der Domänenname oder FQDN für den Pfad verwendet wird.

Beispiel:

In der Domäne my-domain.local auf dem Fileserver dfs.my-domain.local soll ein DFS-Namespace mit dem Namen "data" eingerichtet und in tenfold eingelesen werden. Er enthält einen Ordner, "public", in welchem eine Freigabe unter dem Link "departments" eingehängt wird. Im Folgenden sehen Sie Beispiele, wie der Namespace über einen UNC-Pfad angesprochen werden kann und ob tenfold diesen Pfad korrekt als DFS-Pfad interpretieren kann:

\\my-domain\data	
\\my-domain.local\data	
\\dfs\data	
\\dfs.my-domain.local\data	

\my-domain\data\public	
\my-domain.local\data\public	
\dfs.my-domain.local\data	

Wenn ein DFS-Namespace mit der korrekten Schreibweise als Fileserver in tenfold eingerichtet wurde, wird dieser durch den Fileserver-Scan erkannt und entsprechend verarbeitet.

DFS in älteren Versionen

Sollten Sie ein DFS bereits in einer tenfold-Version vor 2022 R2 Update 2 eingescannt haben, müssen Sie nach dem Update einen Scan durchführen, bevor tenfold Ihr DFS korrekt erkennt. Sie müssen den Fileserver jedoch nicht erneut einrichten.

Sobald das DFS erfolgreich gescannt und erkannt wurde werden Ihnen in der Spalte "Eigenschaften" im Verzeichnisbaum Symbole angezeigt, die Ihnen veranschaulichen, ob es sich bei dem Verzeichnis um ein DFS-Verzeichnis handelt (DFS-Namespace, DFS-Ordner oder DFS-Link). Diese Informationen werden Ihnen auch im Detail-Bereich angezeigt, wenn Sie ein DFS-Verzeichnis auswählen.

Berechtigungen auf DFS-Ordnern

Da die Verwaltung von DFS-Verzeichnissen oberhalb von DFS-Links nur über die DFS-Verwaltung stattfinden sollte (und nicht über UNC-Freigabepfade) sind sämtliche Bearbeitungsmöglichkeiten auf Verzeichnissen im DFS oberhalb des Links deaktiviert. Bei der Vergabe von Berechtigungen wird die Anlage und Berechtigung von LST-Gruppen auf DFS-Ordnern und DFS-Namespace übersprungen.

7.4 Verwaltung der Exchange-Berechtigungen

7.4.1 Allgemeines

Benötigte Berechtigung

Für den Zugriff auf die Exchange Berechtigungsverwaltung, muss eine Ihrer Rollen für zumindest einen Exchange-Bereich freigegeben sein.

Aufbau

Die Maske zur Verwaltung der Fileserver-Berechtigungen ist analog zu allen tenfold-Masken aufgebaut, welche Funktionen für das Berechtigungsmanagement in Microsoft® Systemen bereitstellen:

- Auf der linken Seite befindet sich ein Baum der Ressourcen. Im Falle der Exchange Server ist das der Objektbaum der Postfächer auf den eingerichteten Exchange Servern. Der Wurzelknoten ist der Server selbst (es wird der Anzeigename bei der Serverkonfiguration hinterlegt wurde angezeigt). Darunter befinden sich Knoten welche die einzelnen Postfachtypen, sowie die öffentlichen Ordner, darstellen (zu diesen gibt es keine Berechtigungen). Darunter befinden sich die Postfächer des jeweiligen Typs, bzw. die öffentlichen Ordner. Unterhalb der Postfächer erhalten Sie einen Einblick auf die einzelnen Ordner der jeweiligen Postfächer. Inhalte der einzelnen Ordner werden nicht dargestellt.

- Auf der rechten Seite befindet sich der Berechtigungsbaum, der über eine übersichtliche Baumstruktur die Berechtigungen auf dem auf der linken Seite ausgewählten Objekt (Postfach, Ordner) darstellt.

Dateneigentümeransicht

Eine Ansicht für Dateneigentümer, in welcher diese nur ihre eigenen Objekte sehen können, existiert für Exchange-Berechtigungen in der aktuellen Version von tenfold nicht. Dateneigentümer für Exchange Objekte sind nur für Genehmigungsprozesse angedacht.

7.4.2 Berechtigungen Anzeigen

Name	Berechtigungen	Aktion
Mailbox Baer, Marco	Alle Berechtigungen	
Datenbank Mailbox DB		
Berechtigungen		
Zusammenfassung		
Name		
> Alle Berechtigungen		
Details für Alle Berechtigungen (6)		
> Baer, Marco	1	
> svc-demosuser	2	⚠
> svc-fs	1	
> svc-sql	1	
> svc-tenfold	1	
> ten-admin	3	⚠

Objektbaum

Um die Berechtigungen für ein bestimmtes Objekt anzuzeigen, navigieren Sie auf der linken Seite zum gewünschten Objekt und klicken Sie es an. Sobald Sie das Objekt angeklickt haben, erscheint auf der rechten Seite ein Ladehinweis. Das System lädt nun die Berechtigungen, welche auf diesem Objekt gesetzt sind.

Wie greift tenfold zu?

Wie auch bei den Fileserver-Berechtigungen erfolgt die Abfrage der Berechtigungen nur über die in der tenfold-Datenbank vorhandenen Daten. Der Vorgang wird von dem Job "Exchange Sync" durchgeführt. Über die Konfiguration dieses Jobs lässt sich das Intervall steuern (siehe [Jobs\(see page 443\)](#)).

Anzeige - Berechtigungsbaum

Sobald die Berechtigungen im rechten Bereich geladen sind, werden folgende Informationen angezeigt, je nachdem ob ein Postfach oder ein Verzeichnis ausgewählt wurde.

Wenn ein Postfach ausgewählt wurde:

The screenshot shows a user interface titled 'Mailbox'. At the top, there are two buttons: 'Berechtigungen' (Permissions) and 'Aktion' (Action). Below these, a list of items is displayed:

- Mailbox** Ackermann, Gabriele
- Datenbank** Mailbox DB

- Name des Postfachs
- Datenbank in welcher sich das Postfach befindet

Falls ein Verzeichnis ausgewählt wurde:

The screenshot shows a user interface titled 'Verzeichnis'. At the top, there are two buttons: 'Berechtigungen' (Permissions) and 'Aktion' (Action). Below these, a list of items is displayed:

- Mailbox** Ackermann, Gabriele
- Pfad** Oberste Ebene des Informationsspeichers\Dateien

- Das Postfach zu welchem das Verzeichnis gehört
- Der vollständige Pfad des Verzeichnisses

Postfachberechtigungen

Für die Anzeige des Berechtigungsbaumes eines Postfaches gibt es zwei mögliche Ansichten:

- Listenansicht
- Zusammenfassung

Berechtigungen	
	Zusammenfassung
Name	
▼ Alle Berechtigungen	
▼ Vollzugriff	
Ackermann, Gabriele	
> Administrators	
▼ Senden als	
Ackermann, Gabriele	
> Berechtigungen anzeigen	
> Erhalten als	

Beim Laden der Maske ist die Listenansicht standardmäßig ausgewählt.

In der Listenansicht werden die Berechtigungen in einer Baumstruktur angezeigt, beginnend mit dem Wurzelknoten "Alle Berechtigungen" welcher die einzelnen Berechtigungen als Kindelemente enthält. Unterhalb der Berechtigungen befinden sich die jeweiligen Besitzer der Berechtigungen und im Falle von Gruppen lassen sich diese auf die einzelnen Mitglieder weiter aufbrechen.

Berechtigungen	
	Listenansicht
Name	
Ackermann, Gabriele	✓ ✓ ✓ ✓
▼ Administrators	✓
> Domain Admins	✓
> Enterprise Admins	✓
svc-demouser	✓
ten-admin	✓

Durch die Schaltfläche "Zusammenfassung" wechseln Sie in die Zusammenfassungsansicht.

Diese stellt die Berechtigungen in Form einer Matrix dar. In jeder Zeile befindet sich hierbei ein Berechtigungsinhaber, mit den Berechtigungen welche vergeben wurden. Die Spalten stellen hierbei von links nach rechts folgende Berechtigungen dar:

1. Vollzugriff
2. Externer Zugang
3. Objekt löschen

4. Berechtigungen anzeigen
5. Berechtigungen ändern
6. Besitzer ändern
7. Erhalten als
8. Senden als
9. Senden im Auftrag von

Durch betätigen der Schaltfläche "Listenansicht" wechseln Sie wieder zurück zur Standardansicht.

Ordnerberechtigungen

Berechtigungen	
Name	
▼	Alle Berechtigungen
▼	Autor
>	Administrators
▼	Bearbeiter
>	Beich, Maximilian
▼	Prüfer
>	Domain Users
>	Kappel, Susanne

Die Ansicht der Ordnerberechtigungen funktioniert analog zur Listenansicht der Postfachberechtigungen. Ausgehend vom Wurzelknoten "Alle Berechtigungen" können Sie hier über die einzelnen Unterknoten von den Berechtigungen zu den einzelnen Inhabern navigieren. Es unterscheiden sich hier lediglich die aufgeführten Berechtigungen, da diese für Postfächer und Verzeichnisse unterschiedlich sind. Eine Zusammenfassungsansicht wie bei den Postfächern existiert für Verzeichnisse nicht.

Anzegebereich - Berechtigungspfade

Die untere Hälfte des Berechtigungsbereichs zeigt die Liste aller effektiv berechtigten Benutzer für das ausgewählte Objekt an. Gruppenmitgliedschaften sind in dieser Ansicht bereits komplett aufgebrochen. Standardmäßig werden alle berechtigten Benutzer angezeigt. Durch einen Klick auf die entsprechende Berechtigung im Berechtigungsbau im oberen Teil des Bereiches lässt sich die Ansicht jedoch auf nur jene Benutzer einschränken, welche die ausgewählte Berechtigung besitzen.

Zusammenfassungsansicht

In der Zusammenfassungsansicht der Postfachberechtigungen lässt sich die Anzeige der berechtigten Benutzer nicht einschränken. Wechseln Sie zuerst in die Listenansicht um eine Filterung vornehmen zu können.

Mehrfache Berechtigungen

Verfügt ein Benutzer über mehrere Zugriffsmöglichkeiten (zum Beispiel über Mitgliedschaft in verschiedene Gruppen), so wird der Benutzer lediglich ein Mal angezeigt. Die Zahl neben dem Benutzer zeigt dann die Anzahl der Zugriffspfade an. Wenn die Anzahl den Wert 1 überschreitet wird dies mit einem Warnhinweis verdeutlicht. Dieser zeigt an, dass ein potenzielles Problem beim Entzug der Berechtigung vorliegen könnte, da das Entfernen des Benutzers aus einer Gruppe nicht ausreicht, um die effektiven Berechtigungen zu entziehen.

Um die konkreten Berechtigungspfade für einen Benutzer anzuzeigen, klappen Sie den Eintrag für den jeweiligen Benutzer auf. Das System zeigt Ihnen an, welche Gruppen für die Berechtigung auf diesem Objekt ausschlaggebend sind.

7.4.3 Postfach- und Ordnerberechtigungen bearbeiten

Um die Berechtigungen für ein Postfach zu bearbeiten, selektieren Sie zuerst das gewünschte Postfach und klicken Sie auf den Button "Berechtigungen" im Berechtigungsbereich (rechte Bildschirmseite).

Die Maske "Berechtigungen bearbeiten" besteht aus drei Teilen:

- Suche nach Benutzern und Gruppen (links)
- Berechtigungsfelder (Mitte)
- Detailinformationen (Rechts, wird erst nach Klick auf ein berechtigtes Objekt angezeigt)

Änderungen speichern

Alle Änderungen, die auf dieser Maske vorgenommen werden, werden erst als Request gesichert, wenn der Speichern-Button in der Toolbar betätigt wird. Alle Änderungen, die bis dahin ausgeführt werden, sind lediglich vorgemerkt. Um die Änderungen zu verwerfen, nutzen Sie den Abbrechen-Button in der Toolbar.

Berechtigungen anzeigen

In den Berechtigungsfeldern werden die aktuell gesetzten Berechtigungen angezeigt. Je Berechtigungsstufe existiert ein Feld. Die auf der jeweiligen Berechtigungsstufe zugeordneten Benutzer und Gruppen werden innerhalb des jeweiligen Berechtigungsfelds angezeigt. Das Icon kennzeichnet Benutzer mit einem Personensymbol und Gruppen mit dem Gruppensymbol. Das Symbol neben dem Personen- oder Gruppensymbol kennzeichnet den aktuellen Status der Berechtigung:

- Häkchen: Die Berechtigung ist aktuell zugeordnet.
- Stift: Die Berechtigung wird aktuell bearbeitet (zum Beispiel das Ablaufdatum wird angepasst)
- Plus: Die Berechtigung ist für eine neue Zuordnung vorgesehen
- Kreuz: Die Berechtigung ist zur Löschung vorgesehen

Neben der Bezeichnung des Objekts (Benutzer- oder Gruppenname) befinden sich zwei Buttons:

- Papierkorb: Diese Berechtigung löschen
- Kalender: Diese Berechtigung zeitlich befristen
- Rückgängig (kreisförmiger Pfeil): Die aktuelle Bearbeitung (zum Beispiel die Anpassung des Ablaufdatums) rückgängig machen

Detailinformationen anzeigen

Details	
	Ackermann, Gabriele
	tenfold\gackerman
	S-1-5-21-566901642-699043585-1907573982-1111
	CN=Gabriele\, Ackermann,OU=Zürich,OU=tenfold,DC=tenfold,DC=local
	tenfold
Mitglied von	
Name	
	Domain Users
	Org.IT
	org_toronto
	Users

Klickt man in einem Berechtigungsfeld auf ein Objekt (Benutzer- oder Gruppenname) so öffnet sich auf der rechten Seite die Anzeige der Detailinformationen. Hier werden folgende Informationen zum Benutzer oder der Gruppe angezeigt:

- Anzeigename
- Windows-2000-Anmeldename
- Security Identifier (SID)
- CN (Canonical Name)
- Domäne
- Mitglieder (für Gruppen) / Mitgliedschaften (für Benutzer)