One Identity Manager 8.1.4

# Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung

**Legende**

**WARNUNG: Das Symbol WARNUNG weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.**

**VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.**

One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung
Aktualisiert - 19. Oktober 2020, 07:27 Uhr
Version - 8.1.4

# Inhalt

# 1

# Verwalten einer Azure Active Directory-Umgebung

Der One Identity Manager bietet eine vereinfachte Administration der Benutzerkonten einer Azure Active Directory-Umgebung. Der One Identity Manager konzentriert sich auf die Einrichtung und Bearbeitung von Benutzerkonten und die Versorgung mit den benötigten Berechtigungen. Um die Benutzer mit den benötigten Berechtigungen auszustatten, werden Abonnements, Dienstpläne, Gruppen und Administratorrollen im One Identity Manager abgebildet. Damit ist es möglich, die Identity und Access Governance Prozesse wie Attestierung, Identity Audit, Management von Benutzerkonten und Systemberechtigungen, IT Shop oder Berichtsabonnements für Azure Active Directory Mandanten zu nutzen.

Im One Identity Manager werden die Personen eines Unternehmens mit den benötigten Benutzerkonten versorgt. Dabei können Sie unterschiedliche Mechanismen für die Verbindung der Personen mit ihren Benutzerkonten nutzen. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten und somit administrative Benutzerkonten einrichten.

Durch die Datensynchronisation werden zusätzliche Informationen zum Azure Active Directory Unternehmensverzeichnis, wie Mandant und verifizierten Domänen in die One Identity Manager-Datenbank eingelesen. Aufgrund der komplexen Zusammenhänge und weitreichenden Auswirkungen von Änderungen ist die Anpassung dieser Informationen im One Identity Manager nur in geringem Maße möglich.

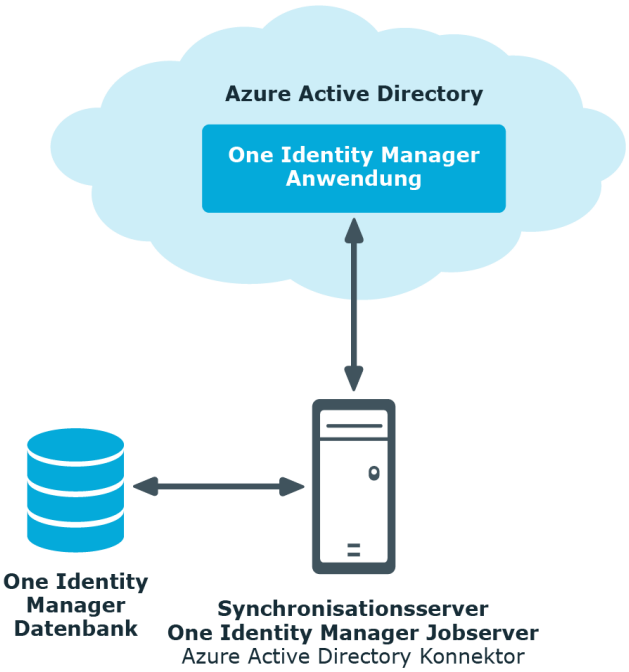
Ausführliche Informationen zur Azure Active Directory Struktur finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

## Architekturüberblick

Um auf die Daten des Azure Active Directory Mandanten zuzugreifen, wird auf einem Synchronisationsserver der Azure Active Directory Konnektor installiert. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und dem Azure Active Directory. Der Azure Active Directory Konnektor verwendet die Microsoft Graph-API für den Zugriff auf Azure Active Directory Daten.

Für den Zugriff auf die Daten eines Azure Active Directory Mandanten, muss sich der Azure Active Directory Konnektor am Azure Active Directory Mandanten authentifizieren. Die Authentifizierung erfolgt über eine One Identity Manager Anwendung, die im Azure Active Directory Mandanten integriert wird und mit den entsprechenden Zugriffsberechtigungen auszustatten ist.

**Abbildung 1: Architektur für die Synchronisation**




# One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung

In die Verwaltung einer Azure Active Directory-Umgebung sind folgende Benutzer eingebunden.

**Tabelle 1: Benutzer**

| Benutzer | Aufgaben |
|---|---|
| Zielsystemadministratoren | Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme \| Administratoren** zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle: |

| Benutzer | Aufgaben |
| --- | --- |
| | • Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen.<br>• Legen die Zielsystemverantwortlichen fest.<br>• Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein.<br>• Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen.<br>• Berechtigen weitere Personen als Zielsystemadministratoren.<br>• Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme. |
| Zielsystemverantwortliche | Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme \| Azure Active Directory** oder einer untergeordneten Anwendungsrolle zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle:<br>• Übernehmen die administrativen Aufgaben für das Zielsystem.<br>• Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen.<br>• Bearbeiten Kennwortrichtlinien für das Zielsystem.<br>• Bereiten Gruppen zur Aufnahme in den IT Shop vor.<br>• Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**.<br>• Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.<br>• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.<br>• Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen. |
| One Identity Manager Administratoren | • Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen.<br>• Erstellen bei Bedarf im Designer Systembenutzer und |

| Benutzer | Aufgaben |
| --- | --- |
| | Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen.<br>• Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter.<br>• Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse.<br>• Erstellen und konfigurieren bei Bedarf Zeitpläne.<br>• Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien. |
| Administratoren für den IT Shop | Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment \| IT Shop \| Administratoren** zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle:<br>• Weisen Gruppen an IT Shop-Strukturen zu. |
| Produkteigner für den IT Shop | Die Produkteigner müssen der Anwendungsrolle **Request & Fulfillment \| IT Shop \| Produkteigner** oder einer untergeordneten Anwendungsrolle zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle:<br>• Entscheiden über Bestellungen.<br>• Bearbeiten die Leistungspositionen und Servicekategorien, für die sie verantwortlich sind. |
| Administratoren für Organisationen | Die Administratoren müssen der Anwendungsrolle **Identity Management \| Organisationen \| Administratoren** zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle:<br>• Weisen Gruppen an Abteilungen, Kostenstellen und Standorte zu. |
| Administratoren für Geschäftsrollen | Die Administratoren müssen der Anwendungsrolle **Identity Management \| Geschäftsrollen \| Administratoren** zugewiesen sein.<br>Benutzer mit dieser Anwendungsrolle:<br>• Weisen Gruppen an Geschäftsrollen zu. |

# Einrichten der Synchronisation mit einem Azure Active Directory Mandanten

***Um die Objekte eines Azure Active Directory Mandanten initial in die One Identity Manager-Datenbank einzulesen***

1. Stellen Sie im Azure Active Directory Mandanten ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Integrieren Sie den One Identity Manager als Anwendung für ihren Mandanten im Azure Active Directory .
3. Die One Identity Manager Bestandteile für die Verwaltung von Azure Active Directory Mandanten sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | AzureAD** aktiviert ist.
   - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.
   - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
4. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
5. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

HINWEIS: Die Synchronisation von Microsoft Azure China mit dem Azure Active Directory Konnektor wird nicht unterstützt.

Weitere Informationen finden Sie unter https://support.oneidentity.com/KB/312379.

## Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit dem Azure Active Directory auf Seite 14

- Integrieren des One Identity Manager als Unternehmensanwendung im Azure Active Directory auf Seite 15
- Einrichten des Synchronisationsservers auf Seite 16
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure Active Directory Mandanten auf Seite 20
- Synchronisation deaktivieren auf Seite 37
- Anpassen einer Synchronisationskonfiguration auf Seite 27
- Konfigurationsparameter für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 171
- Standardprojektvorlage für Azure Active Directory auf Seite 174

# Benutzer und Berechtigungen für die Synchronisation mit dem Azure Active Directory

Bei der Synchronisation des One Identity Manager mit einem Azure Active Directory Mandanten spielen folgende Benutzer eine Rolle.

**Tabelle 2: Benutzer für die Synchronisation**

| Benutzer | Berechtigungen |
|---|---|
| Benutzer für den Zugriff auf das Azure Active Directory | Für eine vollständige Synchronisation von Objekten eines Azure Active Directory Mandanten mit der ausgelieferten One Identity Manager Standardkonfiguration stellen Sie ein Benutzerkonto bereit, das die folgenden Berechtigungen besitzt.<br>• Mitglied in der Organisationsrolle **Globaler Administrator** |
| Benutzerkonto des One Identity Manager Service | Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Rechte vergeben, Verzeichnisse und Dateien anlegen und bearbeiten.<br>Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören.<br>Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**.<br>Das Benutzerkonto benötigt Rechte für den internen Webservice.<br>HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Rechte für den internen Webservice über |

| Benutzer | Berechtigungen |
| --- | --- |
| | folgenden Kommandozeilenaufruf vergeben:<br>`netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"`<br>Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis.<br>In der Standardinstallation wird der One Identity Manager installiert unter:<br>• `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen)<br>• `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen) |
| Benutzer für den Zugriff auf die One Identity Manager-Datenbank | Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt. |

# Integrieren des One Identity Manager als Unternehmensanwendung im Azure Active Directory

Um die Daten zwischen One Identity Manager und Azure Active Directory zu synchronisieren, müssen Sie den One Identity Manager als Anwendung im Azure Active Directory Mandanten integrieren. Der Azure Active Directory Konnektor authentifiziert sich über die One Identity Manager Anwendung am Azure Active Directory Mandanten.

HINWEIS: Beim Hinzufügen des One Identity Manager als Anwendung im Azure Active Directory wird eine Anwendungs-ID erzeugt. Diese Anwendungs-ID benötigen Sie für die Einrichtung des Synchronisationsprojektes.

Ausführliche Informationen zum Integrieren von Anwendungen in Azure Active Directory finden Sie in der Azure Active Directory Dokumentation von Microsoft.

***Um den One Identity Manager als Anwendung im Azure Active Directory zu konfigurieren***

1. Melden Sie sich am Microsoft Azure Management Portal an (https://manage.windowsazure.com) und erstellen Sie für Ihr Verzeichnis eine neue Anwendung für den One Identity Manager.

   Folgenden Einstellungen werden empfohlen:

- Wählen Sie den Link **Eine von meinem Unternehmen entwickelte Anwendung hinzufügen**.
- Richten Sie den One Identity Manager als **öffentlicher Client/nativ (mobil und Desktop)** ein.

2. Konfigurieren Sie für die Anwendung folgende Berechtigungen für die Anwendung **Microsoft Graph**.
   - Berechtigungen vom Typ **Delegiert**:
     - User.Read (Sign in and read user profile)
     - User.ReadWrite (Read and write access to user profile)
     - User.ReadWrite.All (Read and write all users' full profile)
     - Group.ReadWrite.All (Read and write all groups)
     - Directory.ReadWrite.All (Read and write directory data)
     - Directory.AccessAsUser.All (Access directory as the signed in user)
     - openid (Sign users in)

Die Einrichtung der One Identity Manager als Webanwendung kann zu eingeschränktem Funktionsumfang führen und wird daher nicht empfohlen. So werden beispielsweise das Zurücksetzen von Kennwörtern oder Zuweisungen von Administratorrollen an Benutzer nicht unterstützt. Wenn die Registrierung als Webanwendung erfolgen soll, konfigurieren Sie für die Anwendung folgende Berechtigungen für die Anwendung **Windows Azure Active Directory**.

- Berechtigungen vom Typ **Anwendung**:
  - Device.ReadWrite.All (Read and write devices)
  - Directory.Read.All (Read directory data)
  - Member.Read.Hidden (Read all hidden memberships)
  - Directory.ReadWrite.All (Read and write directory data)
  - Domain.ReadWrite.All (Read and write domains)
  - Application.ReadWrite.OwnedBy (Manage apps that this app creates or owns)
  - Application.ReadWrite.All (Read and write all applications)

### Verwandte Themen

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure Active Directory Mandanten auf Seite 20

# Einrichten des Synchronisationsservers

Für die Einrichtung der Synchronisation mit einem Azure Active Directory Mandanten muss ein Server zur Verfügung gestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- Windows Betriebssystem

  Unterstützt werden die Versionen:

  - Windows Server 2008 R2 (nicht-Itanium 64-Bit) ab Service Pack 1
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- One Identity Manager Service, Azure Active Directory Konnektor
  - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.
    1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
    2. Wählen Sie die Maschinenrolle **Server | Jobserver | Azure Active Directory**.

Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

HINWEIS: Wenn mehrere gleichartige Zielsystemumgebungen über den selben Synchronisationsserver synchronisiert werden sollen, ist es aus Performancegründen günstig, für jedes einzelne Zielsystem einen eigenen Jobserver einzurichten. Dadurch wird ein unnötiger Wechsel der Verbindungen zum Zielsystem vermieden, da stets nur gleichartige Aufträge von einem Jobserver zu verarbeiten sind (Nachnutzung bestehender Verbindungen).

Um den One Identity Manager Service zu installieren, nutzen Sie das Programm Server Installer. Das Programm führt folgende Schritte aus:

- Erstellen eines Jobservers.
- Festlegen der Maschinenrollen und Serverfunktionen für den Jobserver.
- Remote-Installation der One Identity Manager Service-Komponenten entsprechend der Maschinenrollen.
- Konfigurieren des One Identity Manager Service.
- Starten des One Identity Manager Service.

HINWEIS: Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen

zum Einrichten des Jobservers finden Sie im *One Identity Manager Konfigurationshandbuch*.

HINWEIS: Das Programm führt eine Remote-Installation des One Identity Manager Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich. Die Remote-Installation wird nur innerhalb einer Domäne oder in Domänen mit Vertrauensstellung unterstützt.

Für die Remote-Installation des One Identity Manager Service benötigen Sie eine administrative Arbeitsstation, auf der die One Identity Manager-Komponenten installiert sind. Ausführliche Informationen zur Installation einer Arbeitsstation finden Sie im *One Identity Manager Installationshandbuch*.

***Um den One Identity Manager Service remote auf einem Server zu installieren und zu konfigurieren***

1. Starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation.
2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.
    a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.

       - ODER -

       Um einen neuen Jobserver zur erstellen, klicken Sie **Hinzufügen**.

    b. Bearbeiten Sie folgende Informationen für den Jobserver.
        - **Server**: Bezeichnung des Jobservers.
        - **Queue**: Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
        - **Vollständiger Servername**: Vollständiger Servername gemäß DNS Syntax.

          Syntax:

          `<Name des Servers>.<Vollqualifizierter Domänenname>`

    HINWEIS: Über die Option **Erweitert** können Sie weitere Eigenschaften für den Jobserver bearbeiten. Sie können die Eigenschaften auch zu einem späteren Zeitpunkt mit dem Designer bearbeiten.
4. Auf der Seite **Maschinenrollen** wählen Sie **Azure Active Directory**.
5. Auf der Seite **Serverfunktionen** wählen Sie **Azure Active Directory Konnektor (via Microsoft Graph)**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

HINWEIS: Die initiale Konfiguration des Dienstes ist bereits vordefiniert. Sollte eine erweiterte Konfiguration erforderlich sein, können Sie diese auch zu einem späteren Zeitpunkt mit dem Designer durchführen. Ausführliche Informationen zur Konfiguration des Dienstes finden Sie im *One Identity Manager Konfigurationshandbuch*.

- Für eine direkte Verbindung zu Datenbank:
  a. Wählen Sie **Prozessabholung | sqlprovider**
  b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
  c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
- Für eine Verbindung zum Anwendungsserver:
  a. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
  b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
  c. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
  d. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
  e. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.
10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.

    HINWEIS: Diese Seite wird nur angezeigt, wenn die Datenbank verschlüsselt ist.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Name oder IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
    - **Dienstkonto**: Angaben zum Benutzerkonto des One Identity Manager Service.
      - Um den Dienst unter dem Konto **NT AUTHORITY\SYSTEM** zu starten, aktivieren Sie die Option **Lokales Systemkonto**.
      - Um den Dienst unter einem anderen Konto zu starten, deaktivieren Sie

die Option **Lokales Systemkonto** und erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung.

- **Installationskonto**: Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.
  - Um das Benutzerkonto des angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Angemeldeter Benutzer**.
  - Um ein anderes Benutzerkonto zu verwenden, deaktivieren Sie die Option **Angemeldeter Benutzer** und geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.
- Um das Installationsverzeichnis, den Namen, den Anzeigenamen oder die Beschreibung für den One Identity Manager Service zu ändern, nutzen Sie die weiteren Optionen.

12. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

    Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.

13. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

    HINWEIS: In einer Standardinstallation wird der Dienst mit der Bezeichnung **One Identity Manager Service** in der Dienstverwaltung des Servers eingetragen.

# Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure Active Directory Mandanten

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und Azure Active Directory-Umgebung einzurichten. Nachfolgend sind die Schritte für die initiale Einrichtung eines Synchronisationsprojektes beschrieben. Ausführliche Informationen zur Einrichtung der Synchronisation finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Nach der initialen Einrichtung können Sie innerhalb des Synchronisationsprojektes die Workflows anpassen und weitere Workflows konfigurieren. Nutzen Sie dazu den Workflow-Assistenten im Synchronization Editor. Der Synchronization Editor bietet zusätzlich verschiedene Konfigurationsmöglichkeiten für ein Synchronisationsprojekt an.

Für die Einrichtung des Synchronisationsprojektes sollten Sie die folgenden Informationen bereit halten.

**Tabelle 3: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes**

| Angaben | Erläuterungen |
|---|---|
| Anwendungs-ID | Anwendungs-ID, die beim Hinzufügen des One Identity Manager als Anwendung des Mandanten erzeugt wird. |
| Anmeldedomäne | Name der Domäne zur Anmeldung am Azure Active Directory. Sie können die Basisdomäne oder eine verifizierte Domäne Ihres Mandanten verwenden. |
| Benutzerkonto und Kennwort zur Anmeldung | Benutzerkonto und Kennwort zur Authentifizierung am Azure Active Directory über die One Identity Manager Anwendung. Stellen Sie ein Benutzerkonto mit ausreichenden Berechtigungen bereit. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit dem Azure Active Directory auf Seite 14. |
| Schlüssel für Authentifizierung als Webanwendung | Haben Sie den One Identity Manager als Webanwendung in Ihrem Mandanten registriert, benötigen Sie den erzeugten Schlüssel.<br>HINWEIS: Der Schlüssel ist nur begrenzte Zeit gültig und muss nach Ablauf ausgetauscht werden. |
| Synchronisationsserver für das Azure Active Directory | Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet.<br>Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Azure Active Directory Konnektor installiert sein.<br>Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften.<br>**Tabelle 4: Zusätzliche Eigenschaften für den Jobserver**<br>Eigenschaft: Serverfunktion — Wert: Azure Active Directory Konnektor (via Microsoft Graph)<br>Eigenschaft: Maschinenrolle — Wert: Server \| Jobserver \| Azure Active Directory<br>Weitere Informationen finden Sie unter Einrichten des |

| Angaben | Erläuterungen |
| --- | --- |
| | Synchronisationsservers auf Seite 16. |
| Verbindungsdaten zur One Identity Manager-Datenbank | • Datenbankserver<br>• Datenbank<br>• SQL Server Anmeldung und Kennwort<br>• Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt. |
| Remoteverbindungsserver | Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden.<br><br>Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen.<br><br>Konfiguration des Remoteverbindungsservers:<br>• One Identity Manager Service ist gestartet<br>• **RemoteConnectPlugin** ist installiert<br>• Azure Active Directory Konnektor ist installiert<br><br>Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt.<br><br>TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software sowie der Berechtigungen des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie lediglich das `RemoteConnectPlugin` zusätzlich installieren.<br><br>Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*. |

HINWEIS: Der folgende Ablauf beschreibt die Einrichtung eines Synchronisationsprojekts, wenn der Synchronization Editor

- im Standardmodus ausgeführt wird und
- aus dem Launchpad gestartet wird.

Wenn der Projektassistent im Expertenmodus ausgeführt wird oder direkt aus dem Synchronization Editor gestartet wird, können zusätzliche Konfigurationseinstellungen vorgenommen werden. Folgen Sie in diesen Schritten den Anweisungen des Projektassistenten.

***Um ein initiales Synchronisationsprojekt für einen Azure Active Directory Mandanten einzurichten***

1. Starten Sie das Launchpadund melden Sie sich an der One Identity Manager-Datenbank an.

   HINWEIS: Wenn die Synchronisation über einen Anwendungsserver ausgeführt werden soll, stellen Sie die Datenbankverbindung über den Anwendungsserver her.

2. Wählen Sie den Eintrag **Zielsystemtyp Azure Active Directory** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors wird gestartet.

3. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.
   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, möglich, nehmen Sie keine Einstellungen vor.
   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, nicht möglich, können Sie eine Remoteverbindung herstellen.

     Aktivieren Sie die Option **Verbindung über einen Remoteverbindungsserver herstellen** und wählen Sie unter **Jobserver** den Server, über den die Verbindung hergestellt werden soll.

4. Auf der Seite **Azure Active Directory Mandant** geben Sie die Basisinformationen zu Ihrem Mandanten an.
   - Erfassen Sie unter **Client ID**, die Anwendungs-ID, die der Integration des One Identity Manager als Anwendung des Mandanten erzeugt wurde.
   - Erfassen Sie unter **Anmeldedomäne**, die Basisdomäne oder eine verifizierte Domäne Ihres Mandanten.

5. Auf der Seite **Authentifizierung** wählen Sie die Art der Anmeldung und erfassen die benötigten Anmeldeinformationen.
   a. Wenn Sie den One Identity Manager als systemeigene Clientanwendung in Ihrem Mandanten integriert haben, wählen Sie die Option **Authentifizierung als native Clientanwendung** und erfassen Sie das Benutzerkonto und das Kennwort zur Anmeldung am Zielsystem.
   b. Wenn Sie den One Identity Manager als Webanwendung in Ihrem Mandanten integriert haben, wählen Sie die Option **Authentifizierung als Webanwendung** und erfassen Sie den Schlüssel, der bei der Registrierung des One Identity Manager als Anwendung des Mandanten erzeugt wurde.

6. Auf der Seite **One Identity Manager Verbindung** überprüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank. Die Daten werden aus der verbundenen Datenbank geladen. Geben Sie das Kennwort erneut ein.

   HINWEIS: Wenn Sie mit einer unverschlüsselten One Identity Manager-Datenbank arbeiten und noch kein Synchronisationsprojekt in der Datenbank gespeichert ist, erfassen Sie alle Verbindungsdaten neu. Wenn bereits ein Synchronisationsprojekt gespeichert ist, wird diese Seite nicht angezeigt.

7. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.

8. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

   **Tabelle 5: Zielsystemzugriff festlegen**

| Option | Bedeutung |
|---|---|
| Das Zielsystem soll nur eingelesen werden. | Angabe, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager-Datenbank eingerichtet werden soll.<br>Der Synchronisationsworkflow zeigt folgende Besonderheiten:<br>• Die Synchronisationsrichtung ist **In den One Identity Manager**.<br>• In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung **In den One Identity Manager** definiert. |
| Es sollen auch Änderungen im Zielsystem durchgeführt werden. | Angabe, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll.<br>Der Provisionierungsworkflow zeigt folgende Besonderheiten:<br>• Die Synchronisationsrichtung ist **In das Zielsystem**.<br>• In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung **In das Zielsystem** definiert.<br>• Synchronisationsschritte werden nur für solche Schemaklassen erstellt, deren Schematypen schreibbar sind. |

9. Auf der Seite **Synchronisationsserver** wählen Sie den Synchronisationsserver, der die Synchronisation ausführen soll.

Wenn der Synchronisationsserver noch nicht als Jobserver in der One Identity Manager-Datenbank bekannt gegeben wurde, können Sie einen neuen Jobserver anlegen.

a. Klicken Sie , um einen neuen Jobserver anzulegen.

b. Erfassen Sie die Bezeichnung des Jobservers und den vollständigen Servernamen gemäß DNS-Syntax.

c. Klicken Sie **OK**.

Der Synchronisationsserver wird als Jobserver für das Zielsystem in der One Identity Manager-Datenbank bekannt gegeben.

HINWEIS: Stellen Sie nach dem Speichern des Synchronisationsprojekts sicher, dass dieser Server als Synchronisationsserver eingerichtet ist.

10. Um den Projektassistenten zu beenden, klicken Sie **Fertig**.

Es wird ein Standardzeitplan für regelmäßige Synchronisationen erstellt und zugeordnet. Aktivieren Sie den Zeitplan für die regelmäßige Synchronisation.

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

HINWEIS:Beim Aktivieren wird eine Konsistenzprüfung durchgeführt. Wenn dabei Fehler auftreten, erscheint eine Meldung. Sie können entscheiden, ob das Synchronisationsprojekt dennoch aktiviert werden soll.

Bevor Sie das Synchronisationsprojekt nutzen, prüfen Sie die Fehler. In der Ansicht **Allgemein** auf der Startseite des Synchronization Editor klicken Sie dafür **Projekt prüfen**.

HINWEIS: Wenn das Synchronisationsprojekt nicht sofort aktiviert werden soll, deaktivieren Sie die Option **Synchronisationsprojekt speichern und sofort aktivieren**. In diesem Fall speichern Sie das Synchronisationsprojekt manuell vor dem Beenden des Synchronization Editor.

HINWEIS: Die Verbindungsdaten zum Zielsystem werden in einem Variablenset gespeichert und können bei Bedarf im Synchronization Editor in der Kategorie **Konfiguration | Variablen** angepasst werden.

HINWEIS:

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für den Mandanten bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

Um die Benutzerkonten über Kontendefinitionen zu verwalten, weisen Sie diesen Benutzerkonten eine Kontendefinition und einen Automatisierungsgrad zu.

***Um die Benutzerkonten über Kontendefinitionen zu verwalten***

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie dem Mandanten die Kontendefinition zu.

3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten | Verbunden aber nicht konfiguriert | <Mandant>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.
    c. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.
    d. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.
    e. Speichern Sie die Änderungen.

### Verwandte Themen

- Integrieren des One Identity Manager als Unternehmensanwendung im Azure Active Directory auf Seite 15
- Einrichten des Synchronisationsservers auf Seite 16
- Benutzer und Berechtigungen für die Synchronisation mit dem Azure Active Directory auf Seite 14
- Synchronisationsergebnisse anzeigen auf Seite 26
- Anpassen einer Synchronisationskonfiguration auf Seite 27
- Standardprojektvorlage für Azure Active Directory auf Seite 174
- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 41
- Automatische Zuordnung von Personen zu Azure Active Directory Benutzerkonten auf Seite 108

# Synchronisationsergebnisse anzeigen

Die Ergebnisse der Synchronisation werden im Synchronisationsprotokoll zusammengefasst. Der Umfang des Synchronisationsprotokolls kann für jede Systemverbindung separat festgelegt werden. Der One Identity Manager stellt verschiedene Berichte bereit, in denen die Synchronisationsergebnisse nach verschiedenen Kriterien aufbereitet sind.

***Um das Protokoll einer Synchronisation anzuzeigen***

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht ▶.

   In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.

Die Auswertung der Synchronisation wird als Bericht angezeigt. Sie können diesen Bericht speichern.

***Um das Protokoll einer Provisionierung anzuzeigen***

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht .

   In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.

   Die Auswertung der Provisionierung wird als Bericht angezeigt. Sie können diesen Bericht speichern.

Die Protokolle sind in der Navigationsansicht farblich gekennzeichnet. Die Kennzeichnung gibt den Ausführungsstatus der Synchronisation/Provisionierung wieder.

TIPP: Die Protokolle werden auch im Manager unter der Kategorie **<Zielsystemtyp> | Synchronisationsprotokolle** angezeigt.

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

***Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen***

- Aktivieren Sie im Designer den Konfigurationsparameter **DPR | Journal | LifeTime** und tragen Sie die maximale Aufbewahrungszeit ein.

# Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation eines Azure Active Directory Mandanten eingerichtet. Mit diesem Synchronisationsprojekt können Sie Azure Active Directory Objekte in die One Identity Manager-Datenbank einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in die Azure Active Directory-Umgebung provisioniert.

Um die Datenbank und die Azure Active Directory-Umgebung regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als Mastersystem zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um allgemeingültige Synchronisationskonfigurationen zu erstellen, die erst beim Start der Synchronisation die notwendigen Informationen über die zu synchronisierenden Objekte erhalten, können Variablen eingesetzt werden. Variablen können beispielsweise in den Basisobjekten, den Schemaklassen oder den Verarbeitungsmethoden eingesetzt werden.

- Mit Hilfe von Variablen kann ein Synchronisationsprojekt für die Synchronisation verschiedener Domänen eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an den Domänen als Variablen.
- Um festzulegen, welche Azure Active Directory Objekte und Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschema geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.

WICHTIG: Solange eine Synchronisation ausgeführt wird, sollte keine weitere Synchronisation für dasselbe Zielsystem gestartet werden. Das gilt insbesondere, wenn dieselben Synchronisationsobjekte verarbeitet werden.

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus **Frozen**. Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.
    - Stellen Sie sicher, dass Startkonfigurationen, die in Startfolgen verwendet werden, nicht gleichzeitig einzeln gestartet werden. Weisen Sie den Startfolgen und Startkonfigurationen unterschiedliche Zeitpläne zu.
- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Legen Sie an den Startkonfigurationen fest, wie sich der One Identity Manager in diesem Fall verhalten soll.
    - Stellen Sie über den Zeitplan sicher, dass die Startkonfigurationen nacheinander ausgeführt werden.
    - Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten.

Ausführliche Informationen zum Konfigurieren einer Synchronisation finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

## Detaillierte Informationen zum Thema

- Synchronisation in den Azure Active Directory Mandanten konfigurieren auf Seite 29
- Synchronisation verschiedener Azure Active Directory Mandanten konfigurieren auf Seite 29
- Schema aktualisieren auf Seite 30

# Synchronisation in den Azure Active Directory Mandanten konfigurieren

Das Synchronisationsprojekt für die initiale Synchronisation stellt je einen Workflow zum initialen Einlesen der Zielsystemobjekte (Initial Synchronization) und für die Provisionierung von Objektänderungen aus der One Identity Manager-Datenbank in das Zielsystem (Provisioning) bereit. Um bei der Synchronisation den One Identity Manager als Mastersystem zu nutzen, benötigen Sie zusätzlich einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.

***Um eine Synchronisationskonfiguration für die Synchronisation in den Azure Active Directory Mandanten zu erstellen***

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Prüfen Sie, ob die bestehenden Mappings für die Synchronisation in das Zielsystem genutzt werden können. Erstellen Sie bei Bedarf neue Mappings.
3. Erstellen Sie mit dem Workflowassistenten einen neuen Workflow.

   Es wird ein Workflow mit der Synchronisationsrichtung **In das Zielsystem** angelegt.
4. Erstellen Sie eine neue Startkonfiguration. Nutzen Sie dabei den neu angelegten Workflow.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

### Verwandte Themen

- Synchronisation verschiedener Azure Active Directory Mandanten konfigurieren auf Seite 29

# Synchronisation verschiedener Azure Active Directory Mandanten konfigurieren

***Um ein Synchronisationsprojekt für die Synchronisation eines weiteren Mandanten anzupassen***

1. Stellen Sie im weiteren Mandanten ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
3. Erstellen Sie für den weiteren Mandanten ein neues Basisobjekt. Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.

- Wählen Sie im Assistenten den Azure Active Directory Konnektor und geben Sie die Verbindungsparameter bekannt. Die Verbindungsparameter werden in einem spezialisierten Variablenset gespeichert.

  Es wird eine Startkonfiguration erstellt, die das neu angelegte Variablenset verwendet.

4. Passen Sie bei Bedarf weitere Komponenten der Synchronisationskonfiguration an.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

### Verwandte Themen

- Synchronisation in den Azure Active Directory Mandanten konfigurieren auf Seite 29

# Schema aktualisieren

Während ein Synchronisationsprojekt bearbeitet wird, stehen alle Schemadaten (Schematypen und Schemaeigenschaften) des Zielsystemschemas und des One Identity Manager Schemas zur Verfügung. Für eine Synchronisationskonfiguration wird jedoch nur ein Teil dieser Daten benötigt. Wenn ein Synchronisationsprojekt fertig gestellt wird, werden die Schemas komprimiert, um die nicht benötigten Daten aus dem Synchronisationsprojekt zu entfernen. Dadurch kann das Laden des Synchronisationsprojekts beschleunigt werden. Die entfernten Schemadaten können zu einem späteren Zeitpunkt wieder in die Synchronisationskonfiguration aufgenommen werden.

Wenn sich das Zielsystemschema oder das One Identity Manager Schema geändert hat, müssen diese Änderungen ebenfalls in die Synchronisationskonfiguration aufgenommen werden. Anschließend können die Änderungen in das Mapping der Schemaeigenschaften eingearbeitet werden.

Um Schemadaten, die beim Komprimieren entfernt wurden, und Schemaänderungen in der Synchronisationskonfiguration berücksichtigen zu können, aktualisieren Sie das jeweilige Schema im Synchronisationsprojekt. Das kann erforderlich sein, wenn:

- ein Schema geändert wurde, durch:
  - Änderungen am Zielsystemschema
  - unternehmensspezifische Anpassungen des One Identity Manager Schemas
  - eine Update-Migration des One Identity Manager
- ein Schema im Synchronisationsprojekt komprimiert wurde, durch:
  - die Aktivierung des Synchronisationsprojekts
  - erstmaliges Speichern des Synchronisationsprojekts
  - Komprimieren eines Schemas

***Um das Schema einer Systemverbindung zu aktualisieren***

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.

   - ODER -

   Wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.
3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

   Die Schemadaten werden neu geladen.

***Um ein Mapping zu bearbeiten***

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Mappings**.
3. Wählen Sie in der Navigationsansicht das Mapping.

   Der Mappingeditor wird geöffnet. Ausführliche Informationen zum Bearbeiten von Mappings finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

HINWEIS: Wenn das Schema eines aktivierten Synchronisationsprojekts aktualisiert wird, wird das Synchronisationsprojekt deaktiviert. Damit Synchronisationen ausgeführt werden, aktivieren Sie das Synchronisationsprojekt erneut.

# Ausstehende Objekte nachbehandeln

Objekte, die im Zielsystem nicht vorhanden sind, können bei der Synchronisation in den One Identity Manager als ausstehend gekennzeichnet werden. Damit kann verhindert werden, dass Objekte aufgrund einer fehlerhaften Datensituation oder einer fehlerhaften Synchronisationskonfiguration gelöscht werden.

Ausstehende Objekte

- können im One Identity Manager nicht bearbeitet werden,
- werden bei jeder weiteren Synchronisation ignoriert,
- werden bei der Vererbungsberechnung ignoriert.

Das heißt, sämtliche Mitgliedschaften und Zuweisungen bleiben solange erhalten, bis die ausstehenden Objekte nachbearbeitet wurden.

Führen Sie dafür einen Zielsystemabgleich durch.

***Um ausstehende Objekte nachzubearbeiten***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Zielsystemabgleich: Azure Active Directory**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **Azure Active Directory** als Synchronisationstabellen zugewiesen sind.

2. Öffnen Sie auf dem Formular **Zielsystemabgleich**, in der Spalte **Tabelle/Objekt** den Knoten der Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

   Es werden alle Objekte angezeigt, die als ausstehend markiert sind. Die Spalten **Letzter Protokolleintrag** und **Letzte ausgeführte Methode** zeigen den Zeitpunkt für den letzten Eintrag im Synchronisationsprotokoll und die dabei ausgeführte Verarbeitungsmethode. Der Eintrag **Kein Protokoll verfügbar** hat folgende Bedeutungen:

   - Das Synchronisationsprotokoll wurde bereits gelöscht.

     - ODER -

   - Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.

     Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.

   - Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.

     Bei der Synchronisation werden das Objekt und alle zugehörigen Einträge in Zuordnungstabellen als ausstehend markiert. Ein Eintrag im Synchronisationsprotokoll erscheint jedoch nur für das gelöschte Objekt.

   TIPP:

   ***Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen***

   a. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.

   b. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.

3. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.

4. Klicken Sie in der Formularsymbolleiste eins der folgenden Symbole, um die jeweilige Methode auszuführen.

**Tabelle 6: Methoden zur Behandlung ausstehender Objekte**

| Symbol | Methode | Beschreibung |
|---|---|---|
| | Löschen | Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Die Markierung **Ausstehend** wird für das Objekt entfernt.<br>Indirekte Mitgliedschaften können nicht gelöscht werden. |

| Symbol | Methode | Beschreibung |
|---|---|---|
| | Publizieren | Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt.<br>Die Methode löst das Ereignis `HandleOutstanding` aus. Dadurch wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt.<br>Voraussetzungen:<br>• Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen.<br>• Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen. |
| | Zurücksetzen | Die Markierung **Ausstehend** wird für das Objekt entfernt. |

5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

HINWEIS: Standardmäßig werden die ausgewählten Objekte parallel verarbeitet. Damit wird die Ausführung der ausgewählten Methode beschleunigt. Wenn bei der Verarbeitung ein Fehler auftritt, wird die Aktion abgebrochen und alle Änderungen werden rückgängig gemacht.

Um den Fehler zu lokalisieren, muss die Massenverarbeitung der Objekte deaktiviert werden. Die Objekte werden damit nacheinander verarbeitet. Das fehlerhafte Objekt wird in der Fehlermeldung benannt. Alle Änderungen, die bis zum Auftreten des Fehlers vorgenommen wurden, werden gespeichert.

***Um die Massenverarbeitung zu deaktivieren***

- Deaktivieren Sie in der Formularsymbolleiste .

Für die Synchronisation in kundenspezifische Tabellen müssen Sie den Zielsystemabgleich anpassen.

***Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Azure Active Directory**.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifischen Tabellen zu, für die Sie ausstehende Objekte behandeln möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifischen Tabellen, für die ausstehende Objekte in das Zielsystem publiziert werden dürfen und aktivieren Sie die Option **Publizierbar**.
8. Speichern Sie die Änderungen.

HINWEIS: Damit ausstehende Objekte in der Nachbehandlung publiziert werden können, muss der Zielsystemkonnektor schreibend auf das Zielsystem zugreifen können. Das heißt, an der Zielsystemverbindung ist die Option **Verbindung darf nur gelesen werden** deaktiviert.

# Provisionierung von Mitgliedschaften konfigurieren

Mitgliedschaften, beispielsweise von Benutzerkonten in Gruppen, werden in der One Identity Manager-Datenbank in Zuordnungstabellen gespeichert. Bei der Provisionierung von geänderten Mitgliedschaften werden möglicherweise Änderungen, die im Zielsystem vorgenommen wurden, überschrieben. Dieses Verhalten kann unter folgenden Bedingungen auftreten:

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert (Beispiel: Liste von Benutzerkonten in der Eigenschaft `Members` einer Azure Active Directory Gruppen (`Group`)).
- Änderungen von Mitgliedschaften sind in beiden verbundenen Systemen zulässig.
- Ein Provisionierungsworkflow und Provisionierungsprozesse sind eingerichtet.

Wird eine Mitgliedschaft im One Identity Manager geändert, wird standardmäßig die komplette Mitgliederliste in das Zielsystem übertragen. Mitgliedschaften, die zuvor im Zielsystem hinzugefügt wurden, werden dabei entfernt; zuvor gelöschte Mitgliedschaften werden wieder eingefügt.

Um das zu verhindern, kann die Provisionierung so konfiguriert werden, dass nur die einzelne geänderte Mitgliedschaft in das Zielsystem provisioniert wird. Das entsprechende Verhalten wird für jede Zuordnungstabelle separat konfiguriert.

***Um die Einzelprovisionierung von Mitgliedschaften zu ermöglichen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Azure Active Directory**.
3. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
4. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
    - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` oder `CCC_XDateSubItem` hat.
    - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden (beispielsweise `AADUserInGroup` und `AADGroupInGroup`).
5. Klicken Sie **Merge-Modus**.
6. Speichern Sie die Änderungen.

Für jede Zuordnungstabelle, die so gekennzeichnet ist, werden Änderungen, die im One Identity Manager vorgenommen werden, in einer separaten Tabelle gespeichert. Bei der Provisionierung der Änderungen wird die Mitgliederliste im Zielsystem mit den Einträgen in dieser Tabelle abgeglichen. Damit wird nicht die gesamte Mitgliederliste überschrieben, sondern nur die einzelne geänderte Mitgliedschaft provisioniert.

HINWEIS: Bei einer Synchronisation wird immer die komplette Mitgliederliste aktualisiert. Dabei werden Objekte mit Änderungen, deren Provisionierung noch nicht abgeschlossen ist, nicht verarbeitet. Diese Objekte werden im Synchronisationsprotokoll aufgezeichnet.

Die Einzelprovisionierung von Mitgliedschaften kann durch eine Bedingung eingeschränkt werden. Wenn für eine Tabelle der Merge-Modus deaktiviert wird, dann wird auch die Bedingung gelöscht. Tabellen, bei denen die Bedingung bearbeitet oder gelöscht wurde, sind durch folgendes Icon gekennzeichnet:  . Die originale Bedingung kann jederzeit wiederhergestellt werden.

***Um die Standardbedingung wiederherzustellen***

1. Wählen Sie die Zuordnungstabelle, für welche Sie die Bedingung wiederherstellen möchten.
2. Klicken Sie mit der rechten Maustaste auf die gewählte Zeile und wählen Sie im Kontextmenü **Originalwerte wiederherstellen**.
3. Speichern Sie die Änderungen.

Ausführliche Informationen zur Provisionierung von Mitgliedschaften finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

# Beschleunigung der Provisionierung und Einzelobjektsynchronisation

Um Lastspitzen aufzufangen, kann die Verarbeitung der Prozesse zur Provisionierung und Einzelobjektsynchronisation auf mehrere Jobserver verteilt werden. Damit können die Provisionierung und Einzelobjektsynchronisation beschleunigt werden.

HINWEIS: Die Lastverteilung sollte nicht permanent für Provisionierungen oder Einzelobjektsynchronisationen eingesetzt werden. Durch die parallele Verarbeitung der Objekte kann es beispielsweise vorkommen, dass Abhängigkeiten nicht aufgelöst werden, da die referenzierten Objekte von einem anderen Jobserver noch nicht vollständig verarbeitet wurden.

Sobald die Lastverteilung nicht mehr benötigt wird, stellen Sie sicher, dass der Synchronisationsserver die Prozesse zur Provisionierung und Einzelobjektsynchronisation ausführt.

***Um die Lastverteilung zu konfigurieren***

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.
   - Weisen Sie diesen Jobservern die Serverfunktion **Azure Active Directory Konnektor** zu.

   Alle Jobserver müssen auf den gleichen Azure Active Directory Mandanten zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.
2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

   Über diese Serverfunktion werden alle Jobserver identifiziert, welche für die Lastverteilung genutzt werden sollen.

   Wenn für das Basisobjekt noch keine kundendefinierte Serverfunktion vorhanden ist, erstellen Sie hier eine neue.

   Ausführliche Informationen zur Bearbeitung von Basisobjekten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
3. Weisen Sie diese Serverfunktion im Manager an alle Jobserver zu, welche die Prozesse zur Provisionierung und Einzelobjektsynchronisation für das Basisobjekt verarbeiten sollen.

   Wählen Sie nur die Jobserver, welche die gleiche Konfiguration wie der Synchronisationsserver des Basisobjekts haben.

Sobald alle Prozesse verarbeitet wurden, soll wieder der Synchronisationsserver die Provisionierung und Einzelobjektsynchronisation ausführen.

***Um den Synchronisationsserver ohne Lastverteilung zu nutzen***

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

Ausführliche Informationen zur Lastverteilung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

### Detaillierte Informationen zum Thema

- Bearbeiten eines Servers auf Seite 76

# Unterstützung bei der Analyse von Synchronisationsproblemen

Für die Analyse von Problemen während der Synchronisation, beispielsweise unzureichender Performance, kann ein Bericht erzeugt werden. Der Bericht enthält Informationen wie beispielsweise:

- Ergebnisse der Konsistenzprüfung
- Einstellungen zur Revisionsfilterung
- Verwendeter Scope
- Analyse des Synchronisationspuffers
- Zugriffszeiten auf die Objekte in der One Identity Manager-Datenbank und im Zielsystem

***Um den Synchronisationsanalysebericht zu erstellen***

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie das Menü **Hilfe | Synchronisationsanalysebericht erstellen** und beantworten Sie die Sicherheitsabfrage mit **Ja**.

   Die Generierung des Berichts nimmt einige Zeit in Anspruch. Er wird in einem separaten Fenster angezeigt.
3. Drucken Sie den Bericht oder Speichern Sie ihn in einem der verschiedenen Ausgabeformate.

# Synchronisation deaktivieren

Regelmäßige Synchronisationen können nur gestartet werden, wenn das Synchronisationsprojekt und der Zeitplan aktiviert sind.

***Um regelmäßige Synchronisationen zu verhindern***

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Startkonfiguration und deaktivieren Sie den hinterlegten Zeitplan.

   Synchronisationen können nun nur noch manuell gestartet werden.

Ein aktiviertes Synchronisationsprojekt kann nur eingeschränkt bearbeitet werden. Sind Schemaänderungen notwendig, muss das Schema im Synchronisationsprojekt aktualisiert werden. Dabei wird das Synchronisationsprojekt deaktiviert und kann erneut bearbeitet werden.

Des Weiteren muss das Synchronisationsprojekt deaktiviert werden, wenn keinerlei Synchronisationen gestartet werden dürfen (auch nicht manuell).

***Um das Synchronisationsprojekt zu deaktivieren***

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie auf der Startseite die Ansicht **Allgemein**.
3. Klicken Sie **Projekt deaktivieren**.

## Verwandte Themen

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure Active Directory Mandanten auf Seite 20

# 3

# Basisdaten für die Verwaltung einer Azure Active Directory-Umgebung

Für die Verwaltung einer Azure Active Directory-Umgebung im One Identity Manager sind folgende Basisdaten relevant.

- Konfigurationsparameter

  Über Konfigurationsparameter konfigurieren Sie die Grundeinstellungen zum Systemverhalten. Der One Identity Manager stellt für verschiedene Konfigurationsparameter Standardeinstellungen zur Verfügung. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.

  Die Konfigurationsparameter sind in den One Identity Manager Modulen definiert. Jedes One Identity Manager Modul kann zusätzliche Konfigurationsparameter installieren. Einen Überblick über alle Konfigurationsparameter finden Sie im Designer in der Kategorie **Basisdaten | Allgemein | Konfigurationsparameter**.

  Weitere Informationen finden Sie unter Konfigurationsparameter für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 171.

- Kontendefinitionen

  Um im laufenden Betrieb Benutzerkonten automatisch an Personen zu vergeben, kennt der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem erzeugt werden. Hat eine Person noch kein Benutzerkonto in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Person ein neues Benutzerkonto erzeugt.

  Weitere Informationen finden Sie unter Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 41.

- Kennwortrichtlinien

  Der One Identity Manager unterstützt Sie beim Erstellen von komplexen Kennwortrichtlinien beispielsweise für Systembenutzerkennwörter, das zentrale Kennwort von Personen sowie für Kennwörter für die einzelnen Zielsysteme. Kennwortrichtlinien werden sowohl bei der Eingabe eines Kennwortes durch den Anwender als auch bei der Generierung von Zufallskennwörtern angewendet.

In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

Weitere Informationen finden Sie unter Kennwortrichtlinien für Azure Active Directory Benutzerkonten auf Seite 61.

- Initiales Kennwort für neue Benutzerkonten

  Um das initiale Kennwort für Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Es kann das zentrale Kennwort der zugeordneten Person auf das Kennwort des Benutzerkontos abgebildet werden, es kann ein fest vorgegebenes Kennwort verwendet werden oder ein zufällig generiertes initiales Kennwort vergeben werden.

  Weitere Informationen finden Sie unter Initiales Kennwort für neue Azure Active Directory Benutzerkonten auf Seite 72.

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

  Bei Erstellung eines neuen Benutzerkontos werden die Anmeldeinformationen an definierte Empfänger versendet. Dabei werden zwei Benachrichtigungen versendet, die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt.

  Weitere Informationen finden Sie unter E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 73.

- Zielsystemtypen

  Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können.

  Weitere Informationen finden Sie unter Ausstehende Objekte nachbehandeln auf Seite 31.

- Zielsystemverantwortliche

  Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, alle Mandanten im One Identity Manager zu bearbeiten.

  Wenn Sie die Bearbeitungsrechte der Zielsystemverantwortlichen auf einzelne Mandanten einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

  Weitere Informationen finden Sie unter Zielsystemverantwortliche auf Seite 74.

- Server

  Für die Verarbeitung der Azure Active Directory spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehört beispielsweise der Synchronisationsserver.

  Weitere Informationen finden Sie unter Bearbeiten eines Servers auf Seite 76.

# Kontendefinitionen für Azure Active Directory Benutzerkonten

Um im laufenden Betrieb Benutzerkonten automatisch an Personen zu vergeben, kennt der One Identity Manager Kontendefinitionen. Kontendefinitionen können für jedes Zielsystem erzeugt werden. Hat eine Person noch kein Benutzerkonto in einem Zielsystem, wird durch die Zuweisung der Kontendefinition an eine Person ein neues Benutzerkonto erzeugt.

Aus den Personenstammdaten resultieren die Daten für das Benutzerkonto im jeweiligen Zielsystem. Die Personen müssen ein zentrales Benutzerkonto besitzen. Über die primäre Zuordnung der Person zu einem Standort, einer Abteilung, einer Kostenstelle oder einer Geschäftsrolle und die Zuweisung der IT Betriebsdaten zu diesen Unternehmensstrukturen wird automatisch die Zuteilung der IT Betriebsdaten zum Benutzerkonto der Person geregelt. Die Verarbeitung erfolgt über Bildungsregeln. In der Standardinstallation sind vordefinierte Bildungsregeln zur Ermittlung der benötigten Daten für die Benutzerkonten enthalten. Bei Bedarf können Sie die Bildungsregeln kundenspezifisch anpassen.

Ausführliche Informationen zu Kontendefinitionen finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- Kontendefinitionen erstellen
- Automatisierungsgrade erstellen
- Abbildungsvorschriften für IT Betriebsdaten erstellen
- IT Betriebsdaten erfassen
- Zuweisen der Kontendefinition an Personen
- Kontendefinitionen an ein Zielsystem zuweisen

# Kontendefinitionen erstellen

***Um eine Kontendefinition zu erstellen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Kontendefinition.
4. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- Stammdaten einer Kontendefinition auf Seite 42

# Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

**Tabelle 7: Stammdaten einer Kontendefinition**

| Eigenschaft | Beschreibung |
|---|---|
| Kontendefinition | Bezeichnung der Kontendefinition. |
| Benutzerkontentabelle | Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet. |
| Zielsystem | Zielsystem für das die Kontendefinition gelten soll. |
| Vorausgesetzte Kontendefinition | Vorausgesetzte Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch mitbestellt oder zugeordnet.<br>Für einen Azure Active Directory Mandanten lassen Sie die Angabe leer. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |
| Automatisierungsgrad (initial) | Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll. |
| Risikoindex | Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Personen. Erfassen Sie einen Wert zwischen 0 und 1. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER \| CalculateRiskIndex** aktiviert ist.<br>Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*. |
| Leistungsposition | Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an. |
| IT Shop | Angabe, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden. |

| Eigenschaft | Beschreibung |
|---|---|
| Verwendung nur im IT Shop | Angabe, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig. |
| Automatische Zuweisung zu Personen | Angabe, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Kontendefinition an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition.<br>WICHTIG: Aktivieren Sie diese Option nur, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen!<br>Um die automatische Zuweisung der Kontendefinition an alle Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten. |
| Kontendefinition bei dauerhafter Deaktivierung beibehalten | Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen.<br>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.<br>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht. |
| Kontendefinition bei zeitweiliger Deaktivierung beibehalten | Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen.<br>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.<br>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht. |
| Kontendefinition bei verzögertem Löschen beibehalten | Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen.<br>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.<br>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht. |

| Eigenschaft | Beschreibung |
|---|---|
| Kontendefinition bei Sicherheitsgefährdung beibehalten | Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen.<br>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.<br>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht. |
| Ressourcentyp | Ressourcentyp zur Gruppierung von Kontendefinitionen. |
| Freies Feld 01- Freies Feld 10 | Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen. |

# Automatisierungsgrade erstellen

Für eine Kontendefinition legen Sie Automatisierungsgrade für die Behandlung der Benutzerkonten fest. Der Automatisierungsgrad eines Benutzerkontos entscheidet über den Umfang der vererbten Eigenschaften der Person an das Benutzerkonto. So kann beispielsweise eine Person mehrere Benutzerkonten in einem Zielsystem besitzen:

- Standardbenutzerkonto, welches alle Eigenschaften über die Person erbt
- Administratives Benutzerkonto, das zwar mit der Person verbunden ist, aber keine Eigenschaften von der Person erben soll

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- **Unmanaged**: Benutzerkonten mit dem Automatisierungsgrad **Unmanaged** erhalten eine Verbindung zur Person, erben jedoch keine weiteren Eigenschaften. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Person werden initial einige der Personeneigenschaften übernommen. Werden die Personeneigenschaften zu einem späteren Zeitpunkt geändert, dann werden diese Änderungen nicht an das Benutzerkonto weitergereicht.
- **Full managed**: Benutzerkonten mit dem Automatisierungsgrad **Full managed** erben definierte Eigenschaften der zugeordneten Person. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Person werden initial die Personeneigenschaften übernommen. Werden die Personeneigenschaften zu einem späteren Zeitpunkt geändert, dann werden diese Änderungen an das Benutzerkonto weitergereicht.

HINWEIS: Die Automatisierungsgrade **Full managed** und **Unmanaged** werden in Bildungsregeln ausgewertet. Die mitgelieferten Bildungsregeln können Sie im Designer unternehmensspezifisch anpassen.

Abhängig von Ihren Anforderungen können Sie weitere Automatisierungsgrade definieren. Die Bildungsregeln müssen Sie um die Vorgehensweise für die zusätzlichen Automatisierungsgrade erweitern.

Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll. Ausführliche Informationen zu Automatisierungsgraden finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

- Um die Berechtigungen zu entziehen, wenn eine Person deaktiviert, gelöscht oder als sicherheitsgefährdend eingestuft wird, können die Benutzerkonten der Person gesperrt werden. Wird die Person zu einem späteren Zeitpunkt wieder aktiviert, werden ihre Benutzerkonten ebenfalls wieder freigeschaltet.
- Zusätzlich kann die Vererbung der Gruppenmitgliedschaften definiert werden. Die Unterbrechung der Vererbung kann beispielsweise gewünscht sein, wenn die Benutzerkonten einer Person gesperrt sind und somit auch nicht in Gruppen Mitglied sein dürfen. Während dieser Zeit sollen keine Vererbungsvorgänge für diese Personen berechnet werden. Bestehende Gruppenmitgliedschaften werden dann gelöscht!

***Um Automatisierungsgrade an eine Kontendefinition zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Automatisierungsgrade zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Automatisierungsgrade zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Automatisierungsgrade.
5. Speichern Sie die Änderungen.

WICHTIG: Der Automatisierungsgrad **Unmanaged** wird beim Erstellen einer Kontendefinition automatisch zugewiesen und kann nicht entfernt werden.

***Um einen Automatisierungsgrad zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
4. Speichern Sie die Änderungen.

### Verwandte Themen

- Stammdaten eines Automatisierungsgrades auf Seite 46

# Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

**Tabelle 8: Stammdaten eines Automatisierungsgrades**

| Eigenschaft | Beschreibung |
|---|---|
| Automatisierungsgrad | Bezeichnung des Automatisierungsgrades. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |
| IT Betriebsdaten überschreibend | Angabe, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind:<br>• **Niemals**: Die Daten werden nicht aktualisiert.<br>• **Immer**: Die Daten werden immer aktualisiert.<br>• **Nur initial**: Die Daten werden nur initial ermittelt. |
| Gruppen bei zeitweiliger Deaktivierung beibehalten | Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen. |
| Benutzerkonten bei zeitweiliger Deaktivierung sperren | Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen. |
| Gruppen bei dauerhafter Deaktivierung beibehalten | Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen. |
| Benutzerkonten bei dauerhafter Deaktivierung sperren | Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen. |
| Gruppen bei verzögertem Löschen beibehalten | Angabe, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen. |
| Benutzerkonten bei verzögertem Löschen sperren | Angabe, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen. |
| Gruppen bei Sicherheitsgefährdung beibehalten | Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen. |

| Eigenschaft | Beschreibung |
|---|---|
| Benutzerkonten bei Sicherheitsgefährdung sperren | Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen. |
| Gruppen bei deaktiviertem Benutzerkonto beibehalten | Angabe, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen. |

# Abbildungsvorschriften für IT Betriebsdaten erstellen

Eine Kontendefinition legt fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über die primären Rollen einer Person ermittelt werden können.

Die folgenden IT Betriebsdaten werden in der Standardkonfiguration des One Identity Manager für das automatische Erzeugen und Ändern von Benutzerkonten für eine Person im Zielsystem verwendet.

- Gruppen erbbar
- Identität
- Privilegiertes Benutzerkonto
- Kennwort bei der nächsten Anmeldung ändern

***Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Abbildungsvorschrift bearbeiten** und erfassen Sie folgende Informationen.

**Tabelle 9: Abbildungsvorschrift für IT Betriebsdaten**

| Eigenschaft | Beschreibung |
|---|---|
| Spalte | Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*. |

| Eigenschaft | Beschreibung |
|---|---|
| Quelle | Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen:<br>• Primäre Abteilung<br>• Primärer Standort<br>• Primäre Kostenstelle<br>• Primäre Geschäftsrolle<br>HINWEIS: Verwenden Sie die primäre Geschäftsrolle nur, wenn das Geschäftsrollenmodul vorhanden ist.<br>• keine Angabe<br>Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen. |
| Standardwert | Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann. |
| Immer Standardwert verwenden | Angabe, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle. |
| Benachrichtigung bei Verwendung des Standards | Angabe, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkontos mit Standardwerten** verwendet. Um die Mailvorlage zu ändern, passen Sie den Konfigurationsparameter **TargetSystem \| AzureAD \| Accounts \| MailTemplateDefaultValues** an. |

4. Speichern Sie die Änderungen.

### Verwandte Themen

- IT Betriebsdaten erfassen auf Seite 48

# IT Betriebsdaten erfassen

Um für eine Person Benutzerkonten mit dem Automatisierungsgrad **Full managed** zu erzeugen, müssen die benötigten IT Betriebsdaten ermittelt werden. Welche IT Betriebsdaten für welches Zielsystem konkret verwendet werden sollen, wird an den Geschäftsrollen, Abteilungen, Kostenstellen oder Standorten definiert. Einer Person wird eine eine primäre Geschäftsrolle, eine primäre Abteilung, eine primäre Kostenstelle oder ein primärer Standort zugeordnet. Abhängig von dieser Zuordnung werden die gültigen IT

Betriebsdaten ermittelt und für die Erstellung des Benutzerkontos verwendet. Können über die primären Rollen keine gültigen IT Betriebsdaten ermittelt werden, werden die Standardwerte verwendet.

Wenn in einem Zielsystem mehrere Kontendefinitionen für die Abbildung der Benutzerkonten verwendet werden, können Sie die IT Betriebsdaten auch direkt für eine konkrete Kontendefinition festlegen.

**Beispiel**

In der Regel erhält jede Person der Abteilung A ein Standardbenutzerkonto im Mandanten A. Zusätzlich erhalten einige Personen der Abteilung A administrative Benutzerkonten im Mandanten A.

Erstellen Sie eine Kontendefinition A für die Standardbenutzerkonten des Mandanten A und eine Kontendefinition B für die administrativen Benutzerkonten des Mandanten A. In der Abbildungsvorschrift der IT Betriebsdaten für die Kontendefinitionen A und B legen Sie die Eigenschaft "Abteilung" zur Ermittlung der gültigen IT Betriebsdaten fest.

Für die Abteilung A legen Sie die wirksamen IT Betriebsdaten für den Mandanten A fest. Diese IT Betriebsdaten werden für die Standardbenutzerkonten verwendet. Zusätzlich legen Sie für die Abteilung A die wirksamen IT Betriebsdaten für die Kontendefinition B fest. Diese IT Betriebsdaten werden für administrative Benutzerkonten verwendet.

***Um IT Betriebsdaten festzulegen***

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.

3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.

**Tabelle 10: IT Betriebsdaten**

| Eigenschaft | Beschreibung |
|---|---|
| Wirksam für | Anwendungsbereich der IT Betriebsdaten. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.<br>Um den Anwendungsbereich festzulegen<br>a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.<br>b. Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder für eine Kontendefinition die Tabelle `TSBAccountDef`.<br>c. Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition.<br>d. Klicken Sie **OK**. |
| Spalte | Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.<br>In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*. |
| Wert | Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll. |

4. Speichern Sie die Änderungen.

### Verwandte Themen

- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 47

# IT Betriebsdaten ändern

Sobald sich die IT Betriebsdaten ändern, müssen Sie diese Änderungen für bestehende Benutzerkonten übernehmen. Dafür führen Sie die Bildungsregeln an den betroffenen Spalten erneut aus. Bevor Sie die Bildungsregeln ausführen, prüfen Sie, welche Auswirkungen eine Änderung der IT Betriebsdaten auf bestehende Benutzerkonten hat. Für jede betroffene Spalte an jedem betroffenen Benutzerkonto können Sie entscheiden, ob die Änderung in die One Identity Manager-Datenbank übernommen werden soll.

### Voraussetzungen

- Die IT Betriebsdaten einer Abteilung, einer Kostenstelle, einer Geschäftsrolle oder eines Standorts wurden geändert.

  - ODER -

- Die Standardwerte in der IT Betriebsdaten Abbildungsvorschrift für eine Kontendefinition wurden geändert.

HINWEIS: Ändert sich die Zuordnung einer Person zu einer primären Abteilung, Kostenstelle, Geschäftsrolle oder zu einem primären Standort, werden die Bildungsregeln automatisch ausgeführt.

***Um die Bildungsregeln auszuführen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Bildungsregeln ausführen**.

   Es wird eine Liste aller Benutzerkonten angezeigt, die über die gewählte Kontendefinition entstanden sind und deren Eigenschaften durch die Änderung der IT Betriebsdaten geändert werden.

   | | |
   |---|---|
   | Alter Wert: | Aktueller Wert der Objekteigenschaft. |
   | Neuer Wert: | Wert, den die Objekteigenschaft durch die Änderung an den IT Betriebsdaten annehmen würde. |
   | Auswahl: | Angabe, ob die Änderung für das Benutzerkonto übernommen werden soll. |

4. Markieren Sie in der Spalte **Auswahl** alle Objekteigenschaften, für die der neue Wert übernommen werden soll.
5. Klicken Sie **Übernehmen**.

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

# Zuweisen der Kontendefinition an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

Das Standardverfahren für die Zuweisung von Kontendefinitionen an Personen ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Personen werden gemäß ihrer Funktion im Unternehmen in diese Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet und erhalten so ihre Kontendefinitionen. Um auf Sonderanforderungen zu reagieren, können einzelne Kontendefinitionen direkt an Personen zugewiesen werden.

Kontendefinitionen können automatisch an alle Personen eines Unternehmens zugewiesen werden. Es ist möglich, die Kontendefinitionen als bestellbare Produkte dem IT Shop zuzuordnen. Der Abteilungsleiter kann dann für seine Mitarbeiter Benutzerkonten über das Web Portal bestellen. Zusätzlich ist es möglich, Kontendefinitionen in Systemrollen aufzunehmen. Diese Systemrollen können über hierarchische Rollen oder direkt an Personen zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

In den Prozessen der One Identity Manager Standardinstallation wird zunächst überprüft, ob die Person bereits ein Benutzerkonto im Zielsystem der Kontendefinition besitzt. Ist kein Benutzerkonto vorhanden, so wird ein neues Benutzerkonto mit dem Standardautomatisierungsgrad der zugewiesenen Kontendefinition erzeugt.

HINWEIS: Ist bereits ein Benutzerkonto vorhanden und ist es deaktiviert, dann wird dieses Benutzerkonto entsperrt. Den Automatisierungsgrad des Benutzerkontos müssen Sie in diesem Fall nachträglich ändern.

## Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

- Für die Rollenklasse (Abteilung, Kostenstelle, Standort oder Geschäftsrolle) ist die Zuweisung von Personen und Kontendefinitionen erlaubt.

HINWEIS: Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.

Ausführliche Informationen zur Vorbereitung der Rollenklassen für die Zuweisung finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

## Detaillierte Informationen zum Thema

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 53
- Kontendefinition an alle Personen zuweisen auf Seite 54
- Kontendefinition direkt an Personen zuweisen auf Seite 55
- Kontendefinition an Systemrollen zuweisen auf Seite 55
- Kontendefinition in den IT Shop aufnehmen auf Seite 56

# Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

***Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Organisationen entfernen.

   ***Um eine Zuweisung zu entfernen***
   - Wählen Sie die Organisation und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Kontendefinition an Geschäftsrollen zuweisen auf Seite 53
- Kontendefinition an alle Personen zuweisen auf Seite 54
- Kontendefinition direkt an Personen zuweisen auf Seite 55
- Kontendefinition an Systemrollen zuweisen auf Seite 55
- Kontendefinition in den IT Shop aufnehmen auf Seite 56

# Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

***Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.

***Um eine Zuweisung zu entfernen***

- Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

### Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Kontendefinition an alle Personen zuweisen auf Seite 54
- Kontendefinition direkt an Personen zuweisen auf Seite 55
- Kontendefinition an Systemrollen zuweisen auf Seite 55
- Kontendefinition in den IT Shop aufnehmen auf Seite 56

## Kontendefinition an alle Personen zuweisen

***Um eine Kontendefinition an alle Personen zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.

   WICHTIG: Aktivieren Sie diese Option nur, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen!

5. Speichern Sie die Änderungen.

Die Kontendefinition wird an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition. Die Zuweisung wird durch den DBQueue Prozessor berechnet.

HINWEIS: Um die automatische Zuweisung der Kontendefinition an alle Personen zu entfernen, deaktivieren Sie die Option **Automatische Zuweisung zu Personen**. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen bleiben jedoch erhalten.

### Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 53

- Kontendefinition direkt an Personen zuweisen auf Seite 55
- Kontendefinition an Systemrollen zuweisen auf Seite 55
- Kontendefinition in den IT Shop aufnehmen auf Seite 56

# Kontendefinition direkt an Personen zuweisen

***Um eine Kontendefinition direkt an Personen zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **An Personen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Personen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Person und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 53
- Kontendefinition an alle Personen zuweisen auf Seite 54
- Kontendefinition an Systemrollen zuweisen auf Seite 55
- Kontendefinition in den IT Shop aufnehmen auf Seite 56

# Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

HINWEIS: Kontendefinitionen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können Sie nur an Systemrollen zuweisen, bei denen diese Option ebenfalls aktiviert ist.

***Um Kontendefinitionen in eine Systemrolle aufzunehmen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.

3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 53
- Kontendefinition an alle Personen zuweisen auf Seite 54
- Kontendefinition direkt an Personen zuweisen auf Seite 55
- Kontendefinition in den IT Shop aufnehmen auf Seite 56

# Kontendefinition in den IT Shop aufnehmen

Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann sie von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Kontendefinition muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Kontendefinition muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Kontendefinition im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.
- Soll die Kontendefinition nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss sie zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Kontendefinitionen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Kontendefinition in den IT Shop aufzunehmen.

***Um eine Kontendefinition in den IT Shop aufzunehmen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).

2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

***Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinition aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

***Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

### Verwandte Themen

- Stammdaten einer Kontendefinition auf Seite 42
- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 53
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 53
- Kontendefinition an alle Personen zuweisen auf Seite 54
- Kontendefinition direkt an Personen zuweisen auf Seite 55
- Kontendefinition an Systemrollen zuweisen auf Seite 55

# Kontendefinitionen an ein Zielsystem zuweisen

Wenn Sie die automatische Zuordnung von Benutzerkonten und Personen einsetzen und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen, sind folgende Voraussetzungen zu gewährleisten:

- Die Kontendefinition ist dem Zielsystem zugewiesen.
- Die Kontendefinition besitzt einen Standardautomatisierungsgrad.

Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.

***Um die Kontendefinition an ein Zielsystem zuzuweisen***

1. Wählen Sie im Manager in der Kategorie **Azure Active Directory | Mandanten** den Mandanten.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- Automatische Zuordnung von Personen zu Azure Active Directory Benutzerkonten auf Seite 108

# Kontendefinitionen löschen

Sie können Kontendefinitionen löschen, wenn diese keinem Zielsystem, keiner Person, keiner hierarchischen Rolle und keiner anderen Kontendefinition als Vorgänger zugeordnet sind.

***Um eine Kontendefinition zu löschen***

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.
    e. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **An Personen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.
    e. Speichern Sie die Änderungen.
3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorten.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Organisationen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Abteilungen, Kostenstellen und Standorte.
    e. Speichern Sie die Änderungen.
4. Entfernen Sie die Zuordnung der Kontendefinition zu Geschäftsrollen.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

        Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
    d. Speichern Sie die Änderungen.
5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden.

    Ausführliche Informationen zum Abbestellen einer Bestellung finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

***Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen***

a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.

d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

e. Klicken Sie **OK**.

   Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.

6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden. Prüfen Sie alle Kontendefinitionen.

   a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   d. Entfernen Sie in der Auswahlliste **Vorausgesetzte Kontendefinition** die Kontendefinition.

   e. Speichern Sie die Änderungen.

7. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.

   a. Wählen Sie im Manager in der Kategorie **Azure Active Directory | Mandanten** den Mandanten.

   b. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   c. Entfernen Sie auf dem Tabreiter **Allgemein** die zugewiesenen Kontendefinitionen.

   d. Speichern Sie die Änderungen.

8. Löschen Sie die Kontendefinition.

   a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Klicken Sie  , um die Kontendefinition zu löschen.

# Kennwortrichtlinien für Azure Active Directory Benutzerkonten

Der One Identity Manager unterstützt Sie beim Erstellen von komplexen Kennwortrichtlinien beispielsweise für Systembenutzerkennwörter, das zentrale Kennwort von Personen sowie für Kennwörter für die einzelnen Zielsysteme. Kennwortrichtlinien werden sowohl bei der Eingabe eines Kennwortes durch den Anwender als auch bei der Generierung von Zufallskennwörtern angewendet.

In der Standardinstallation werden vordefinierte Kennwortrichtlinien mitgeliefert, die Sie nutzen können und bei Bedarf an Ihre Anforderungen anpassen können. Zusätzlich können Sie eigene Kennwortrichtlinien definieren.

### Detaillierte Informationen zum Thema



# Vordefinierte Kennwortrichtlinien

Die vordefinierte Kennwortrichtlinien können Sie bei Bedarf an Ihre Anforderungen anpassen.

### Kennwortrichtlinie für die Anmeldung am One Identity Manager

Für die Anmeldung am One Identity Manager wird die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** angewendet. Diese Kennwortrichtlinie definiert die Einstellung für die Kennwörter von Systembenutzern (`DialogUser.Password` und `Person.DialogUserPassword`) sowie für den Zugangscode für die einmalige Anmeldung am Web Portal (`Person.Passcode`).

> HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

Ausführliche Informationen zu Kennwortrichtlinien für Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

### Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

Bei entsprechender Konfiguration wird das zentrale Kennwort einer Person auf die Kennwörter der zielsystemspezifischen Benutzerkonten abgebildet. Die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** definiert die Einstellung für das zentrale Kennwort (`Person.CentralPassword`). Die Mitglieder der Anwendungsrolle **Identity Management | Personen | Administratoren** können diese Kennwortrichtlinie anpassen.

WICHTIG: Stellen Sie sicher, dass die Kennwortrichtlinie **Kennwortrichtlinie für zentrales Kennwort von Personen** nicht gegen die zielsystemspezifischen Anforderungen an Kennwörter verstößt.

Ausführliche Informationen zu Kennwortrichtlinien für Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

### Kennwortrichtlinien für Benutzerkonten

Es werden vordefinierte Kennwortrichtlinien bereitgestellt, die Sie auf die Kennwortspalten der Benutzerkonten anwenden können.

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.

HINWEIS: Bei der Aktualisierung von One Identity Manager Version 7.x auf One Identity Manager Version 8.1.4 werden die Einstellung der Konfigurationsparameter zur Bildung von Kennwörtern auf die zielsystemspezifischen Kennwortrichtlinien umgesetzt.

Für Azure Active Directory ist die Kennwortrichtlinie **Azure Active Directory Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Azure Active Directory Benutzerkonten (`AADUser.Password`) eines Azure Active Directory Mandanten anwenden.

Wenn die Kennwortanforderungen der Mandanten unterschiedlich sind, wird empfohlen, je Mandant eine eigene Kennwortrichtlinie einzurichten.

Des Weiteren können Sie Kennwortrichtlinien abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten anwenden.

# Kennwortrichtlinien anwenden

Für Azure Active Directory ist die Kennwortrichtlinie **Azure Active Directory Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Azure Active Directory Benutzerkonten (`AADUser.Password`) eines Azure Active Directory Mandanten anwenden.

Wenn die Kennwortanforderungen der Mandanten unterschiedlich sind, wird empfohlen, je Mandant eine eigene Kennwortrichtlinie einzurichten.

Des Weiteren können Sie Kennwortrichtlinien abhängig von der Kontendefinition der Benutzerkonten oder abhängig vom Automatisierungsgrad der Benutzerkonten anwenden.

Die anzuwendende Kennwortrichtlinie für ein Benutzerkonto wird in folgender Reihenfolge ermittelt:

1. Kennwortrichtlinie der Kontendefinition des Benutzerkontos
2. Kennwortrichtlinie des Automatisierungsgrades des Benutzerkontos
3. Kennwortrichtlinien des Mandanten des Benutzerkontos
4. Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** (Standardrichtlinie)

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.

***Um eine Kennwortrichtlinie neu zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Klicken Sie im Bereich **Zuweisungen** die Schaltfläche **Hinzufügen** und erfassen Sie folgende Daten.

**Tabelle 11: Zuweisen einer Kennwortrichtlinie**

| Eigenschaft | Beschreibung |
|---|---|
| Anwenden auf | Anwendungsbereich der Kennwortrichtlinie.<br>***Um den Anwendungsbereich festzulegen***<br>a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.<br>b. Wählen Sie unter **Tabelle** eine der folgenden Referenzen:<br>• Die Tabelle, die die Basisobjekte der Synchronisation enthält.<br>• Um die Kennwortrichtlinie abhängig von der Kontendefinition anzuwenden, wählen Sie die Tabelle `TSBAccountDef`.<br>• Um die Kennwortrichtlinie abhängig vom Automatisierungsgrad anzuwenden, wählen Sie die Tabelle `TSBBehavoir`.<br>c. Wählen Sie unter **Anwenden auf** die Tabelle, die die |

| Eigenschaft | Beschreibung |
|---|---|
| | Basisobjekte enthält.<br>• Wenn Sie die Tabelle mit den Basisobjekten der Synchronisation gewählt haben, dann wählen Sie das konkrete Zielsystem.<br>• Wenn Sie die Tabelle `TSBAccountDef` gewählt haben, dann wählen Sie die konkrete Kontendefinition.<br>• Wenn Sie die Tabelle `TSBBehavior` gewählt haben, dann wählen Sie den konkreten Automatisierungsgrad.<br>d. Klicken Sie **OK**. |
| Kennwortspalte | Bezeichnung der Kennwortspalte. |
| Kennwortrichtlinie | Bezeichnung der Kennwortrichtlinie, die angewendet werden soll. |

5. Speichern Sie die Änderungen.

***Um die Zuweisung einer Kennwortrichtlinie zu ändern***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Wählen Sie im Bereich **Zuweisungen** die Zuweisung, die Sie ändern möchten.
5. Wählen Sie in der Auswahlliste **Kennwortrichtlinie** die neu anzuwendende Kennwortrichtlinie.
6. Speichern Sie die Änderungen.

# Kennwortrichtlinien bearbeiten

***Um eine Kennwortrichtlinie zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie und wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Kennwortrichtlinie.
4. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Kennwortrichtlinie auf Seite 65
- Richtlinieneinstellungen auf Seite 65
- Zeichenklassen für Kennwörter auf Seite 67
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 68

# Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

**Tabelle 12: Stammdaten einer Kennwortrichtlinie**

| Eigenschaft | Bedeutung |
|---|---|
| Anzeigename | Bezeichnung der Kennwortrichtlinie. Übersetzen Sie den eingegebenen Text über die Schaltfläche. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen.Übersetzen Sie den eingegebenen Text über die Schaltfläche. |
| Fehlermeldung | Kundenspezifische Fehlermeldung, die ausgegeben wird, wenn die Richtlinie nicht erfüllt wird. Übersetzen Sie den eingegebenen Text über die Schaltfläche. |
| Eigentümer (Anwendungsrolle) | Anwendungsrolle, deren Mitglieder die Kennwortrichtlinie konfigurieren können. |
| Standardrichtlinie | Kennzeichnung als Standardrichtlinie für Kennwörter.<br>HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann. |

# Richtlinieneinstellungen

Auf dem Tabreiter **Kennwort** definieren Sie folgende Einstellungen für eine Kennwortrichtlinie.

**Tabelle 13: Richtlinieneinstellungen**

| Eigenschaft | Bedeutung |
|---|---|
| Initiales Kennwort | Initiales Kennwort für neu erzeugte Benutzerkonten. Wird beim Erstellen eines Benutzerkontos kein Kennwort |

| Eigenschaft | Bedeutung |
| --- | --- |
| | angegeben oder kein Zufallskennwort generiert, dann wird das initiale Kennwort benutzt. |
| Kennwortbestätigung | Kennwortwiederholung. |
| Min. Länge | Minimale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben muss. |
| Max. Länge | Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann. Der maximal zulässige Wert ist **256**. |
| Max. Fehlanmeldungen | Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Wird nur berücksichtigt, bei Anmeldung am One Identity Manager.<br>Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder Personen-basierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen erreicht, kann sich die Person oder der Systembenutzer nicht mehr am One Identity Manager anmelden.<br>Kennwörter gesperrter Personen und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*. |
| Max. Tage gültig | Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird. |
| Kennwortchronik | Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert. |
| Min. Kennwortstärke | Angabe, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert **0** wird die Kennwortstärke nicht geprüft. Die Werte **1**, **2**, **3** und **4** geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert **1** die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert **4** fordert die höchste Komplexität. |
| Namensbestandteile unzulässig | Angabe, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die Option **Enthält Namensbestandteile für die Kennwortprüfung** aktiviert ist. Die Option passen Sie im |

| Eigenschaft | Bedeutung |
| --- | --- |
| | Designer an der Spaltendefinition an. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*. |

# Zeichenklassen für Kennwörter

Auf dem Tabreiter **Zeichenklassen** legen Sie fest, welche Zeichen für ein Kennwort zulässig sind.

**Tabelle 14: Zeichenklassen für Kennwörter**

| Eigenschaft | Bedeutung |
| --- | --- |
| Min. Anzahl Buchstaben | Angabe, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss. |
| Min. Anzahl Kleinbuchstaben | Angabe, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss. |
| Min. Anzahl Großbuchstaben | Angabe, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss. |
| Min. Anzahl Ziffern | Angabe, wie viele Ziffern ein Kennwort mindestens enthalten muss. |
| Min. Anzahl Sonderzeichen | Angabe, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss. |
| Zulässige Sonderzeichen | Liste zulässiger Sonderzeichen. |
| Max. identische Zeichen insgesamt | Maximale Anzahl identischer Zeichen, die insgesamt im Kennwort vorkommen dürfen. |
| Max. identische Zeichen aufeinanderfolgend | Maximale Anzahl identischer Zeichen, die nacheinander wiederholt werden können. |
| Unzulässige Sonderzeichen | Liste unzulässiger Sonderzeichen. |
| Keine Klein-buchstaben erzeugen | Angabe, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt. |
| Keinen Großbuch-staben erzeugen | Angabe, ob ein generiertes Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt. |
| Keine Ziffern erzeugen | Angabe, ob ein generiertes Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berück- |

| Eigenschaft | Bedeutung |
|---|---|
| | sichtigt. |
| Keine Sonderzeichen erzeugen | Angabe, ob ein generiertes Kennwort Sonderzeichen enthalten darf. Ist die Option aktiviert, sind nur Buchstaben, Zahlen und Leerzeichen in Kennwörtern erlaubt. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt. |

# Kundenspezifische Skripte für Kennwortanforderungen

Kundenspezifische Skripte zum Prüfen und Generieren von Kennwörtern können Sie einsetzen, wenn die Anforderungen an Kennwörter mit den vorhandenen Einstellmöglichkeiten nicht abgebildet werden können. Skripte werden zusätzlich zu den anderen Einstellungen angewendet.

### Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 68
- Skript zum Generieren eines Kennwortes auf Seite 69

# Skript zum Prüfen eines Kennwortes

Ein Prüfskript können Sie einsetzen, wenn zusätzliche Richtlinien beim Prüfen eines Kennwortes angewendet werden sollen, die nicht mit den vorhandenen Einstellmöglichkeiten abgebildet werden können.

### Syntax für Prüfskripte

```
Public Sub CCC_CustomPwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As System.Security.SecureString)
```

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Kennwort, das zu prüfen ist

TIPP: Um das Basisobjekt zu verwenden, nutzen Sie die Eigenschaft `Entity` der `PasswordPolicy`-Klasse.

### Beispiel für ein Skript zum Prüfen eines Kennwortes

Ein Kennwort in darf nicht mit **?** oder **!** beginnen. Das Kennwort darf nicht mit drei identischen Zeichen beginnen. Das Skript prüft ein gegebenes Kennwort auf Zulässigkeit.

```
Public Sub CCC_PwdValidate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            Throw New Exception(#LD("Password can't start with '?' or '!'")#)
        End If
    End If
    If pwd.Length>2
        If pwd(0) = pwd(1) AndAlso pwd(1) = pwd(2)
            Throw New Exception(#LD("Invalid character sequence in password")#)
        End If
    End If
End Sub
```

***Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden***

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
    b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Prüfskript** den Namen des Skriptes ein, das zum Prüfen eines Kennwortes verwendet wird.
    e. Speichern Sie die Änderungen.

### Verwandte Themen

- Skript zum Generieren eines Kennwortes auf Seite 69

# Skript zum Generieren eines Kennwortes

Ein Generierungsskript können Sie einsetzen, wenn zusätzliche Richtlinien beim Generieren eines Zufallskennwortes angewendet werden sollen, die nicht mit den vorhandenen Einstellmöglichkeiten abgebildet werden können.

### Syntax für Generierungsskripte

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
```

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Generiertes Kennwort

TIPP: Um das Basisobjekt zu verwenden, nutzen Sie die Eigenschaft `Entity` der `PasswordPolicy`-Klasse.

## Beispiel für ein Skript zum Generieren eines Kennwortes

Das Skript ersetzt in Zufallskennwörtern die unzulässigen Zeichen **?** und **!** zu Beginn eines Kennwortes mit **_**.

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            spwd.SetAt(0, CChar("_"))
        End If
    End If
End Sub
```

### *Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden*

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
    b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Generierungsskript** den Namen des Skriptes ein, das zum Generieren eines Kennwortes verwendet wird.
    e. Speichern Sie die Änderungen.

## Verwandte Themen

- Skript zum Prüfen eines Kennwortes auf Seite 68

# Ausschlussliste für Kennwörter

Um bestimmte Begriffe im Kennwort zu verbieten, nehmen Sie den Begriff in die Ausschlussliste auf.

HINWEIS: Die Ausschlussliste ist global für alle Kennwortrichtlinien gültig.

***Um einen Begriff in die Ausschlussliste aufzunehmen***

1. Wählen Sie im Designer die Kategorie **Basisdaten | Sicherheitseinstellungen | Kennwort Ausschlussliste**.
2. Erstellen Sie einen neuen Eintrag über den Menüeintrag **Objekt | Neu** und erfassen Sie den auszuschließenden Begriff.
3. Speichern Sie die Änderungen.

# Kennwörter prüfen

Beim Prüfen eines Kennwortes werden alle definierten Einstellungen der Kennwortrichtlinie, kundenspezifische Skripte sowie die Ausschlussliste für Kennwörter berücksichtigt.

***Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Wählen Sie in der Auswahlliste **Basisobjekt für den Test** die Tabelle und das Objekt für die Prüfung.
6. Geben Sie im Eingabefeld **Kennwort überprüfen** das Kennwort ein.

   Neben dem Eingabefeld wird angezeigt, ob das Kennwort gültig ist.

# Generieren eines Kennwortes testen

Beim Generieren eines Kennwortes werden alle definierten Einstellungen der Kennwortrichtlinie, kundenspezifische Skripte sowie die Ausschlussliste für Kennwörter berücksichtigt.

***Um ein Kennwort zu generieren, das der Kennwortrichtlinie entspricht***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Klicken Sie auf die Schaltfläche **Generieren**.

   Das generierte Kennwort wird angezeigt.

# Initiales Kennwort für neue Azure Active Directory Benutzerkonten

Um das initiale Kennwort für neue Azure Active Directory Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung.

- Erstellen Sie Benutzerkonten manuell und tragen Sie in den Stammdaten der Benutzerkonten ein Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.
  - Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | Accounts | InitialRandomPassword**.
  - Verwenden Sie zielsystemspezifische Kennwortrichtlinien und definieren Sie in den Kennwortrichtlinien die Zeichenklassen, die das Kennwort enthalten muss.
  - Legen Sie fest, an welche Person das initiale Kennwort per E-Mail versendet wird.
- Verwenden Sie das zentrale Kennwort der Person. Das zentrale Kennwort der zugeordneten Person wird auf das Kennwort des Benutzerkontos abgebildet. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

## Verwandte Themen

- Kennwortrichtlinien für Azure Active Directory Benutzerkonten auf Seite 61
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 73

# E-Mail-Benachrichtigungen über Anmeldeinformationen

Die Anmeldeinformationen für neue Benutzerkonten können per E-Mail an eine festgelegte Person gesendet werden. Dabei werden zwei Benachrichtigungen versendet, die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt. In einer Mailvorlage sind die Mailtexte in verschiedenen Sprachen definiert. Somit wird bei Generierung einer E-Mail Benachrichtigung die Sprache des Empfängers berücksichtigt. In der Standardinstallation sind bereits Mailvorlagen enthalten, die Sie zur Konfiguration der Benachrichtigungsverfahren verwenden können.

Um Benachrichtigungen zu nutzen, sind folgende Voraussetzungen zu erfüllen:

1. Stellen Sie sicher, dass das E-Mail-Benachrichtungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im *One Identity Manager Installationshandbuch*.
2. Aktivieren Sie im Designer den Konfigurationsparameter **Common | MailNotification | DefaultSender** und geben Sie die Absenderadresse an, mit der die E-Mail Benachrichtigungen verschickt werden.
3. Stellen Sie sicher, dass alle Personen eine Standard-E-Mail-Adresse besitzen. An diese E-Mail Adresse werden die Benachrichtigungen versendet. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
4. Stellen Sie sicher, dass für alle Personen eine Sprachkultur ermittelt werden kann. Nur so erhalten die Personen die E-Mail Benachrichtigungen in ihrer Sprache. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Wenn bei der Neuanlage eines Benutzerkontos ein zufällig generiertes initiales Kennwort vergeben wird, werden die initialen Anmeldeinformationen für dieses Benutzerkonto per E-Mail an eine vorher festgelegt Person gesendet.

***Um die initialen Anmeldeinformationen per E-Mail zu versenden***

1. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | Accounts | InitialRandomPassword**.
2. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo** und erfassen Sie als Wert den Empfänger der Benachrichtigung.
3. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName**.

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Person - Erstellung neues Benutzerkonto** versendet. Die Benachrichtigung enthält den Namen des Benutzerkontos.

4. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword**.

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** versendet. Die Benachrichtigung enthält das initiale Kennwort für das Benutzerkonto.

HINWEIS: Um andere als die Standardmailvorlagen für diese Benachrichtigungen zu nutzen, ändern Sie die Werte der Konfigurationsparameter.

# Zielsystemverantwortliche

Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, alle Mandanten im One Identity Manager zu bearbeiten.

Wenn Sie die Bearbeitungsrechte der Zielsystemverantwortlichen auf einzelne Mandanten einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

Ausführliche Informationen zum Einsatz und zur Bearbeitung von Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

## Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

1. Der One Identity Manager Administrator legt Personen als Zielsystemadministratoren fest.
2. Die Zielsystemadministratoren nehmen die Personen in die Standardanwendungsrolle für die Zielsystemverantwortlichen auf.

   Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle Mandanten im One Identity Manager zu bearbeiten.
3. Zielsystemverantwortliche können innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen Mandanten zuweisen.

**Tabelle 15: Standardanwendungsrolle für Zielsystemverantwortliche**

| Benutzer | Aufgaben |
|---|---|
| Zielsystemverantwortliche | Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme \| Azure Active Directory** oder einer untergeordneten Anwendungsrolle zugewiesen sein.<br><br>Benutzer mit dieser Anwendungsrolle:<br><br>• Übernehmen die administrativen Aufgaben für das Zielsystem. |

| Benutzer | Aufgaben |
| --- | --- |
| | • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen.<br>• Bearbeiten Kennwortrichtlinien für das Zielsystem.<br>• Bereiten Gruppen zur Aufnahme in den IT Shop vor.<br>• Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**.<br>• Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.<br>• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.<br>• Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen. |

***Um initial Personen als Zielsystemadministrator festzulegen***

1. Melden Sie sich als One Identity Manager Administrator (Anwendungsrolle **Basisrollen | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration | Zielsysteme | Administratoren**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Person zu und speichern Sie die Änderung.

***Um initial Personen in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen***

1. Melden Sie sich als Zielsystemadministrator (Anwendungsrolle **Zielsysteme | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration | Zielsysteme | Azure Active Directory**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

***Um als Zielsystemverantwortlicher weitere Personen als Zielsystemverantwortliche zu berechtigen***

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie in der Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Zielsystemverantwortliche** die Anwendungsrolle.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Personen zu und speichern Sie die Änderungen.

***Um Zielsystemverantwortliche für einzelne Mandanten festzulegen***

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **Azure Active Directory | Mandanten**.
3. Wählen Sie in der Ergebnisliste den Mandanten.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Zielsystemverantwortliche** die Anwendungsrolle.

   - ODER -

   Klicken Sie neben der Auswahlliste **Zielsystemverantwortliche** auf , um eine neue Anwendungsrolle zu erstellen.

   a. Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | Azure Active Directory** zu.

   b. Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, den Mandanten im One Identity Manager zu bearbeiten.

### Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 10
- Azure Active Directory Mandant auf Seite 82

# Bearbeiten eines Servers

Für die Verarbeitung der Azure Active Directory spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehört beispielsweise der Synchronisationsserver.

Um die Funktion eines Servers zu definieren, haben Sie mehrere Möglichkeiten:

- Erstellen Sie im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** einen Eintrag für den Jobserver. Ausführliche Informationen dazu finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Wählen Sie im Manager in der Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Server** einen Eintrag für den Jobserver und bearbeiten Sie die Stammdaten des Jobservers.

  Nutzen Sie dieses Verfahren, wenn der Jobserver bereits im One Identity Manager bekannt ist und Sie für den Jobserver spezielle Funktionen konfigurieren möchten.

HINWEIS: Damit ein Server seine Funktion im One Identity Manager Netzwerk ausführen kann, muss ein One Identity Manager Service installiert, konfiguriert und gestartet sein. Gehen Sie dazu wie im *One Identity Manager Installationshandbuch* beschrieben vor.

***Um einen Jobserver und seine Funktionen zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Basisdaten zur Konfiguration | Server**.
2. Wählen Sie in der Ergebnisliste den Jobserver-Eintrag.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für den Jobserver.
5. Wählen Sie die Aufgabe **Serverfunktionen zuweisen** und legen Sie die Serverfunktionen fest.
6. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- Stammdaten eines Jobservers auf Seite 77
- Festlegen der Serverfunktionen auf Seite 80

# Stammdaten eines Jobservers

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** zur Verfügung.

HINWEIS: Abhängig von den installierten Modulen können weitere Eigenschaften verfügbar sein.

**Tabelle 16: Eigenschaften eines Jobservers**

| Eigenschaft | Bedeutung |
|---|---|
| Server | Bezeichnung des Jobservers. |
| Vollständiger Servername | Vollständiger Servername gemäß DNS Syntax.<br>Beispiel:<br>`<Name des Servers>.<Vollqualifizierter Domänenname>` |
| Zielsystem | Zielsystem des Computerkontos. |
| Sprachkultur | Sprache des Servers. |
| Server ist Cluster | Angabe, ob der Server einen Cluster abbildet. |
| Server gehört zu Cluster | Cluster, zu dem der Server gehört.<br>HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server** |

| Eigenschaft | Bedeutung |
| --- | --- |
| | **gehört zu Cluster** schließen einander aus. |
| IP-Adresse (IPv6) | Internet Protokoll Version 6 (IPv6)-Adresse des Servers. |
| IP-Adresse (IPv4) | Internet Protokoll Version 4 (IPv4)-Adresse des Servers. |
| Kopierverfahren (Quellserver) | Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme Robocopy und rsync unterstützt.<br>Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm Robocopy und zwischen Servern mit einem Linux Betriebssystem mit dem Programm rsync. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt, das beide Server unterstützen. |
| Kopierverfahren (Zielserver) | Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist. |
| Codierung | Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden. |
| Übergeordneter Jobserver | Bezeichnung des übergeordneten Jobservers. |
| Ausführender Server | Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden.<br>Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben. |
| Queue | Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen. |

| Eigenschaft | Bedeutung |
|---|---|
| Serverbetriebssystem | Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen. |
| Angaben zum Dienstkonto | Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen. |
| One Identity Manager Service installiert | Angabe, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur `QBM_PJobQueueLoad` aktiviert, sobald die Queue das erste Mal angefragt wird.<br>Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen. |
| Stopp One Identity Manager Service | Angabe, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten.<br>Den Dienst können Sie mit entsprechenden administrativen Rechten im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*. |
| Kein automatisches Softwareupdate | Angabe, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist.<br>HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren. |
| Softwareupdate läuft | Angabe, ob gerade eine Softwareaktualisierung ausgeführt wird. |
| Letzter Abrufzeitpunkt | Zeitpunkt der letzten Prozessabholung. |
| Letzte Timeout Prüfung | Zeitpunkt der letzten Prüfung für geladene Prozessschritte, deren Auslieferung den Wert im Konfigurationsparameter **Common \| Jobservice \| LoadedJobsTimeOut** überschreitet. |
| Serverfunktion | Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt. |

### Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 80

# Festlegen der Serverfunktionen

HINWEIS: Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** zur Verfügung.

Die Serverfunktion definiert die Funktion eines Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

HINWEIS: Abhängig von den installierten Modulen können weitere Serverfunktionen verfügbar sein.

**Tabelle 17: Zulässige Serverfunktionen**

| Serverfunktion | Anmerkungen |
|---|---|
| Azure Active Directory Konnektor (via Microsoft Graph) | Server, auf dem der Azure Active Directory Konnektor installiert ist. Der Server führt die Synchronisation mit dem Zielsystem Azure Active Directory aus. |
| CSV Konnektor | Server, auf dem der CSV Konnektor für die Synchronisation installiert ist. |
| Domänen-Controller | Active Directory Domänen-Controller. Server, die nicht als Domänen-Controller gekennzeichnet sind, werden als Memberserver betrachtet. |
| Druckserver | Server, der als Druckserver arbeitet. |
| Generischer Server | Server für die generische Synchronisation mit einem kundendefinierten Zielsystem. |
| Homeserver | Server zur Anlage von Homeverzeichnissen für Benutzerkonten. |
| Aktualisierungsserver | Der Server führt die automatische Softwareaktualisierung aller anderen Server aus. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Der Server kann SQL Aufträge ausführen.<br>Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet. |
| SQL Ausführungsserver | Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. |

| Serverfunktion | Anmerkungen |
| --- | --- |
| | Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion. |
| CSV Skriptserver | Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten. |
| Nativer Datenbankkonnektor | Der Server kann sich mit einer ADO.Net Datenbank verbinden. |
| One Identity Manager-Datenbankkonnektor | Server, auf dem der One Identity Manager Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Manager aus. |
| One Identity Manager Service installiert | Server, auf dem ein One Identity Manager Service installiert werden soll. |
| Primärer Domänen-Controller | Primärer Domänen-Controller. |
| Profilserver | Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten. |
| SAM Synchronisationsserver | Server für die Synchronisation mit einem SMB-basierten Zielsystem aus. |
| SMTP Host | Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host. |
| Standard Berichtserver | Server, auf dem die Berichte generiert werden. |
| Windows PowerShell Konnektor | Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen. |

## Verwandte Themen

- Stammdaten eines Jobservers auf Seite 77

# 4

# Azure Active Directory Unternehmensverzeichnis

Ausführliche Informationen zur Azure Active Directory Struktur finden Sie in der Azure Active Directory Dokumentation von Microsoft.

Bei der erstmaligen Registrierung für einen Microsoft Cloud-Dienst stellen Sie Details zu Ihrer Organisationen bereit. Mit diesen Informationen wird eine neue Azure Active Directory Verzeichnisinstanz erstellt. Die Organisation repräsentiert einen Azure Active Directory Mandanten. Sie können im One Identity Manager einzelne Stammdaten des Mandanten bearbeiten. Neue Mandanten können Sie im One Identity Manager nicht erstellen.

Mit dem Unternehmensverzeichnis in der Cloud ist eine Basisdomäne verbunden. Zusätzlich können Sie im Azure Active Directory weitere benutzerdefinierte Domänen hinzufügen, welchen Sie dann die Microsoft Cloud-Dienste zuordnen. One Identity Manager liest nur die Informationen verifizierter Domänen in die Datenbank ein. Die Bearbeitung der Informationen ist im One Identity Manager nicht möglich.

### Detaillierte Informationen zum Thema

- Azure Active Directory Mandant auf Seite 82
- Azure Active Directory Domänen auf Seite 87

# Azure Active Directory Mandant

Bei der erstmaligen Registrierung für einen Microsoft Cloud-Dienst stellen Sie Details zu Ihrer Organisationen bereit. Mit diesen Informationen wird eine neue Azure Active Directory Verzeichnisinstanz erstellt. Die Organisation repräsentiert einen Azure Active Directory Mandanten. Sie können im One Identity Manager einzelne Stammdaten des Mandanten bearbeiten. Neue Mandanten können Sie im One Identity Manager nicht erstellen.

***Um die Stammdaten eines Azure Active Directory Mandanten zu bearbeiten***

1. Wählen Sie die Kategorie **Azure Active Directory | Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für einen Mandanten.
5. Speichern Sie die Änderungen.

### Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Azure Active Directory Mandanten auf Seite 83
- Informationen zum lokalen Active Directory auf Seite 85
- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 85

# Allgemeine Stammdaten eines Azure Active Directory Mandanten

Auf dem Tabreiter **Allgemein** erfassen Sie folgende Stammdaten.

**Tabelle 18: Stammdaten eines Mandanten**

| Eigenschaft | Beschreibung |
|---|---|
| Anzeigename | Anzeigename des Mandanten. |
| Kontendefinition (initial) | Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diesen Mandanten die automatische Zuordnung von Personen zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet.<br>Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall. |
| Zielsystemverantwortliche | Anwendungsrolle, in der die Zielsystemverantwortlichen des Mandanten festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Mandanten, dem sie zugeordnet sind. Jedem Mandanten können somit andere Zielsystemverantwortliche zugeordnet werden. |

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>Wählen Sie die One Identity Manager Anwendungsrolle, deren Mitglieder verantwortlich für die Administration dieses Mandanten sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.</td></tr>
<tr><td>Standort</td><td>Standort des Mandanten.</td></tr>
<tr><td>Straße</td><td>Straße.</td></tr>
<tr><td>Ort</td><td>Ort.</td></tr>
<tr><td>Postleitzahl</td><td>Postleitzahl.</td></tr>
<tr><td>Land</td><td>Land.</td></tr>
<tr><td>Synchronisiert durch</td><td>Art der Synchronisation, über welche die Daten zwischen dem Mandanten und dem One Identity Manager synchronisiert werden. Sobald Objekte für diesen Mandaten im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden.<br>Beim Erstellen eines Mandanten mit dem Synchronization Editor wird One Identity Manager verwendet.<br>Tabelle 19: Zulässige Werte
<table>
<tr><th>Wert</th><th>Synchro-nisation durch</th><th>Provi-sionierung durch</th></tr>
<tr><td>One Identity Manager</td><td>Azure Active Directory Konnektor</td><td>Azure Active Directory Konnektor</td></tr>
<tr><td>Keine Synchronisation</td><td>keine</td><td>keine</td></tr>
</table>
HINWEIS: Wenn Sie Keine Synchronisation festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.</td></tr>
<tr><td>Empfänger (Marke-tingbenachrichtigungen)</td><td>Liste von Empfängern von Marketingbenachrichtigungen.</td></tr>
<tr><td>Empfänger (Technische Benach-</td><td>Liste von Empfängern von technischen</td></tr>
</table>

| Eigenschaft | Beschreibung |
|---|---|
| richtigungen) | Benachrichtigungen. |
| Empfänger (Sicher-heitsbenachrichtigungen) | Liste von Empfängern von Sicherheitsbenachrichtigungen. |
| Telefonnummern (Sicher-heitsbenachrichtigungen) | Telefonnummern für Sicherheitsbenachrichtigung. |

### Verwandte Themen

- Automatische Zuordnung von Personen zu Azure Active Directory Benutzerkonten auf Seite 108
- Zielsystemverantwortliche auf Seite 74

# Informationen zum lokalen Active Directory

Auf dem Tabreiter **Verbund** werden folgende Informationen zum lokalen Active Directory, welches mit dem Azure Active Directory Mandanten verbunden ist, abgebildet.

**Tabelle 20: Angaben zum lokalen Active Directory Benutzerkonto**

| Eigenschaft | Beschreibung |
|---|---|
| Synchronisation mit dem lokalen Active Directory aktiviert | Angabe, ob die Synchronisation mit einem lokalen Active Directory aktiviert ist. |
| Letzte Synchronisation | Zeitpunkt der letzten Synchronisation des Azure Active Directory Mandanten mit dem lokalen Active Directory. |

# Kategorien für die Vererbung von Berechtigungen definieren

Im One Identity Manager können Gruppen, Administratorrollen, Abonnements und unwirksame Dienstpläne selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen (Administratorrollen, Abonnements, unwirksame Dienstpläne) und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In den übrigen Tabellen geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen , Administratorrollen, Abonnements und

unwirksamen Dienstpläne an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

***Um Kategorien zu definieren***

1. Wählen Sie im Manager in der Kategorie **Azure Active Directory | Mandanten** den Mandanten.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wechseln Sie auf den Tabreiter **Abbildungsvorschrift Kategorien**.
4. Erweitern Sie den jeweiligen Basisknoten einer Tabelle.
5. Aktivieren Sie die Kategorie per Maus-Doppelklick auf das Symbol .
6. Tragen Sie eine beliebige Benennung der Kategorie für Benutzerkonten und Gruppen (Administratorrollen, Abonnements, unwirksamen Dienstpläne) in der verwendeten Anmeldesprache ein.
7. Speichern Sie die Änderungen.

### Verwandte Themen

- Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 130
- Vererbung von Azure Active Directory Administratorrollen anhand von Kategorien auf Seite 144
- Vererbung von Azure Active Directory Abonnements anhand von Kategorien auf Seite 156
- Vererbung von unwirksamen Azure Active Directory Dienstplänen anhand von Kategorien auf Seite 167

# Synchronisationsprojekt bearbeiten

Synchronisationsprojekte, in denen ein Mandant bereits als Basisobjekt verwendet wird, können auch über den Manager geöffnet werden. In diesem Modus können beispielsweise die Konfigurationseinstellungen überprüft oder die Synchronisationsprotokolle eingesehen werden. Der Synchronization Editor wird nicht mit seinem vollen Funktionsumfang gestartet. Verschiedene Funktionen, wie Simulieren oder Ausführen einer Synchronisation, Starten des Zielsystembrowsers und andere, können nicht ausgeführt werden.

HINWEIS: Der Manager ist währenddessen für die Bearbeitung gesperrt. Um Objekte im Manager bearbeiten zu können, schließen Sie den Synchronization Editor.

***Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen***

1. Wählen Sie die Kategorie **Azure Active Directory | Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten.Wählen Sie die Aufgabe

**Stammdaten bearbeiten**.

3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten**.

### Verwandte Themen

- Anpassen einer Synchronisationskonfiguration auf Seite 27

# Azure Active Directory Domänen

Mit dem Unternehmensverzeichnis in der Cloud ist eine Basisdomäne verbunden. Zusätzlich können Sie im Azure Active Directory weitere benutzerdefinierte Domänen hinzufügen, welchen Sie dann die Microsoft Cloud-Dienste zuordnen. One Identity Manager liest nur die Informationen verifizierter Domänen in die Datenbank ein. Die Bearbeitung der Informationen ist im One Identity Manager nicht möglich.

***Um einen Überblick über eine Domäne zu erhalten***

1. Wählen Sie die Kategorie **Azure Active Directory | Verifizierte Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Überblick über die Azure Active Directory Domäne**.

**Tabelle 21: Stammdaten einer Domäne**

| Eigenschaft | Beschreibung |
|---|---|
| Name der Domäne | Vollständiger Name der Domäne. |
| Mandant | Mandant, zu dem diese Domäne eingetragen ist. |
| Typ | Typ der Domäne. |
| Primäre Domäne | Angabe, ob es sich um die primäre Domäne handelt, beispielsweise zum Erstellen neuer Benutzerkonten. |
| Initiale Domäne | Angabe, ob es sich um die initiale Domäne handelt. Die initiale Domäne wird erstellt, wenn Sie einen Mandanten im Azure Active Directory registrieren. |
| Verfügbare Dienste | Liste der in dieser Domäne verfügbaren Dienste. |

# 5

# Azure Active Directory Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Benutzerkonten einer Azure Active Directory-Umgebung. Um auf die Dienstpläne im Azure Active Directory zuzugreifen, benötigen die Benutzer ein Abonnement. Über die Mitgliedschaft in Gruppen erhalten die Benutzerkonten die nötigen Rechte zum Zugriff auf die Ressourcen.

**Detaillierte Informationen zum Thema**



# Benutzerkonten mit Personen verbinden

Zentraler Bestandteil des One Identity Manager ist die Abbildung von Personen mit ihren Stammdaten sowie den Berechtigungen, über die sie in verschiedenen Zielsystemen verfügen. Zu diesem Zweck können Informationen über Benutzerkonten und Berechtigungen aus den Zielsystemen in die One Identity Manager-Datenbank eingelesen und mit den Personen verbunden werden. Für jede Person kann damit ein Überblick über ihre Berechtigungen in allen angebundenen Zielsystemen gewonnen werden. Der One Identity Manager bietet die Möglichkeit Benutzerkonten und ihre Berechtigungen zu verwalten. Änderungen können in die Zielsysteme provisioniert werden. Die Personen werden so entsprechend ihrer Funktion mit den benötigten Berechtigungen in den angebundenen Zielsystemen versorgt. Regelmäßige Synchronisationsprozesse halten die Daten zwischen den Zielsystemen und der One Identity Manager-Datenbank konsistent.

Da die Anforderungen von Unternehmen zu Unternehmen unterschiedlich sind, bietet der One Identity Manager verschiedene Verfahren zur Versorgung einer Person mit den benötigten Benutzerkonten an. Der One Identity Manager unterstützt die folgenden Vorgehensweisen, um Personen und ihre Benutzerkonten zu verknüpfen:

- Personen erhalten ihre Benutzerkonten automatisch über Kontendefinitionen. Hat eine Person noch kein Benutzerkonto in einem Mandanten, wird durch die Zuweisung der Kontendefinition an eine Person über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

  Wenn Sie Benutzerkonten über Kontendefinitionen verwalten, können Sie das Verhalten von Benutzerkonten beim Deaktivieren oder Löschen von Personen festlegen.
- Beim Einfügen eines Benutzerkontos wird automatisch eine vorhandene Person zugeordnet oder im Bedarfsfall eine neue Person erstellt. Dabei werden die Personenstammdaten anhand vorhandener Benutzerkontenstammdaten erzeugt. Dieser Mechanismus kann eingesetzt werden, wenn ein neues Benutzerkonto manuell oder durch eine Synchronisation erstellt wird. Dieses Vorgehen ist jedoch nicht das Standardverfahren für den One Identity Manager. Für die automatische Personenzuordnung definieren Sie Kriterien, anhand derer die Personen ermittelt werden sollen.
- Personen und Benutzerkonten können manuell erfasst und einander zugeordnet werden.

### Verwandte Themen

- Stammdaten für Azure Active Directory Benutzerkonten bearbeiten auf Seite 96
- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 41
- Automatische Zuordnung von Personen zu Azure Active Directory Benutzerkonten auf Seite 108
- Ausführliche Informationen zur Behandlung und Administration von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

# Unterstützte Typen von Benutzerkonten

Im One Identity Manager können unterschiedliche Typen von Benutzerkonten wie beispielsweise Standardbenutzerkonten, administrative Benutzerkonten, Dienstkonten oder privilegierte Benutzerkonten abgebildet werden.

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität

  Mit der Eigenschaft **Identität** (Spalte `IdentityType`) wird der Typ des Benutzerkontos beschrieben.

**Tabelle 22: Identitäten von Benutzerkonten**

| Identität | Beschreibung | Wert der Spalte IdentityType |
|---|---|---|
| Primäre Identität | Standardbenutzerkonto einer Person. | Primary |
| Organisatorische Identität | Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. | Organizational |
| Persönliche Administratoridentität | Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. | Admin |
| Zusatzidentität | Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird. | Sponsored |
| Gruppenidentität | Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. | Shared |
| Dienstidentität | Dienstkonto. | Service |

HINWEIS: Um mit Identitäten für Benutzerkonten zu arbeiten, benötigen die Personen ebenfalls Identitäten. Benutzerkonten, denen eine Identität zugeordnet ist, können Sie nur mit Personen verbinden, die dieselbe Identität haben.

Die primäre Identität, die organisatorische Identität und die persönliche Administratoridentität werden für die verschiedenen Benutzerkonten genutzt, mit denen ein und dieselbe Person ihre unterschiedlichen Aufgaben im Unternehmen ausführen kann.

Um Benutzerkonten mit einer persönlichen Administratoridentität oder einer organisatorische Identität für eine Person bereitzustellen, richten Sie für die Person Subidentitäten ein. Diese Subidentitäten verbinden Sie mit den Benutzerkonten. Somit können für die unterschiedlichen Benutzerkonten die erforderlichen Berechtigungen erteilt werden.

Benutzerkonten mit einer Zusatzidentität, einer Gruppenidentität oder einer Dienstidentität verbinden Sie mit Dummy-Personen, die keinen Bezug zu einer realen Person haben. Diese Dummy-Personen werden benötigt, um Berechtigungen an die Benutzerkonten vererben zu können. Bei der Auswertung von Berichten, Attestierungen oder Complianceprüfungen prüfen Sie, ob die Dummy-Personen gesondert betrachtet werden müssen.

Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

- Privilegiertes Benutzerkonto

Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

### Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 91
- Administrative Benutzerkonten auf Seite 92
- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 92
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 93
- Privilegierte Benutzerkonten auf Seite 95

# Standardbenutzerkonten

In der Regel erhält jede Person ein Standardbenutzerkonto, das die Berechtigungen besitzt, die für die tägliche Arbeit benötigt werden. Die Benutzerkonten haben eine Verbindung zur Person. Über eine Kontendefinition und deren Automatisierungsgrade kann die Auswirkung der Verbindung und der Umfang der vererbten Eigenschaften der Person an die Benutzerkonten konfiguriert werden.

***Um Standardbenutzerkonten über Kontendefinitionen zu erstellen***

1. Erstellen Sie eine Kontendefinition und weisen Sie die Automatisierungsgrade **Unmanaged** und **Full managed** zu.
2. Legen Sie für jeden Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.
3. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

   Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

   Welche IT Betriebsdaten erforderlich sind, ist abhängig vom Zielsystem. Für Standardbenutzerkonten werden folgende Einstellungen empfohlen:

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsGroupAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert verwenden**.
   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IdentityType` den Standardwert **Primary** und aktivieren Sie die Option **Immer Standardwert verwenden**.

4. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem. Wählen Sie unter **Wirksam für** das konkrete Zielsystem.

   Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.

5. Weisen Sie die Kontendefinition an die Personen zu.

   Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

### Verwandte Themen

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 41

# Administrative Benutzerkonten

Für bestimmte administrative Aufgaben, ist der Einsatz administrativer Benutzerkonten notwendig. Administrative Benutzerkonten werden in der Regel vom Zielsystem vorgegeben und haben feste Bezeichnungen und Anmeldenamen, wie beispielsweise **Administrator**.

Administrative Benutzerkonten werden durch die Synchronisation in den One Identity Manager eingelesen.

HINWEIS: Einige administrative Benutzerkonten können automatisch als privilegierte Benutzerkonten gekennzeichnet werden. Aktivieren Sie dazu im Designer den Zeitplan **Ausgewählte Benutzerkonten als privilegiert kennzeichnen**.

### Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 92
- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 93

# Administrative Benutzerkonten für eine Person bereitstellen

### Voraussetzungen

- Das Benutzerkonto muss als persönliche Administratoridentität gekennzeichnet sein.
- Die Person, die das Benutzerkonto nutzen soll, muss als persönliche Administratoridentität gekennzeichnet sein.
- Die Person, die das Benutzerkonto nutzen soll, muss mit einer Hauptidentität verbunden sein.

***Um ein administratives Benutzerkonto für eine Person bereitzustellen***

1. Kennzeichnen Sie das Benutzerkonto als persönliche Administratoridentität.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Persönliche Administratoridentität**.
2. Verbinden Sie das Benutzerkonto mit der Person, die dieses administrative Benutzerkonto nutzen soll.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Person, die dieses administrative Benutzerkonto nutzt.

    TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Person erstellen.

### Verwandte Themen

- Administrative Benutzerkonten für mehrere Personen bereitstellen auf Seite 93
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

# Administrative Benutzerkonten für mehrere Personen bereitstellen

### Voraussetzung

- Das Benutzerkonto muss als Gruppenidentität gekennzeichnet sein.
- Es muss eine Dummy-Person vorhanden sein. Die Dummy-Person muss als Gruppenidentität gekennzeichnet sein und muss einen Manager besitzen.
- Die Personen, die das Benutzerkonto nutzen dürfen, müssen als primäre Identitäten gekennzeichnet sein.

***Um ein administratives Benutzerkonto für mehrere Personen bereitzustellen***

1. Kennzeichnen Sie das Benutzerkonto als Gruppenidentität.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Gruppenidentität**.
2. Verbinden Sie das Benutzerkonto mit einer Dummy-Person.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Dummy-Person.

    TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Dummy-Person erstellen.
3. Weisen Sie dem Benutzerkonto die Personen zu, die dieses administrative Benutzerkonto nutzen sollen.
    a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Personen mit Nutzungsberechtigungen zuzuweisen**.
    d. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

    TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Personen entfernen.

    ***Um eine Zuweisung zu entfernen***

    - Wählen Sie die Person und doppelklicken Sie .

## Verwandte Themen

- Administrative Benutzerkonten für eine Person bereitstellen auf Seite 92
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

# Privilegierte Benutzerkonten

Privilegierte Benutzerkonten werden eingesetzt, um Personen mit zusätzlichen privilegierten Berechtigungen auszustatten. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Die Benutzerkonten werden mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) gekennzeichnet.

HINWEIS: Die Kriterien anhand derer Benutzerkonten automatisch als privilegiert erkannt werden, sind als Erweiterungen zur Sichtdefinition (ViewAddOn) an der Tabelle `TSBVAccountIsPrivDetectRule` (Tabelle vom Typ **Union**) definiert. Die Auswertung erfolgt im Skript `TSB_SetIsPrivilegedAccount`.

***Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen***

1. Erstellen Sie eine Kontendefinition. Erstellen Sie einen neuen Automatisierungsgrad für privilegierte Benutzerkonten und weisen Sie diesen Automatisierungsgrad an die Kontendefinition zu.
2. Wenn Sie verhindern möchten, dass die Eigenschaften für privilegierte Benutzerkonten überschrieben werden, setzen Sie für den Automatisierungsgrad die Eigenschaft **IT Betriebsdaten überschreibend** auf den Wert **Nur initial**. In diesem Fall werden die Eigenschaften einmalig beim Erstellen der Benutzerkonten befüllt.
3. Legen Sie für den Automatisierungsgrad fest, wie sich die zeitweilige Deaktivierung, die dauerhafte Deaktivierung, das Löschen und die Sicherheitsgefährdung einer Person auf deren Benutzerkonten und die Gruppenmitgliedschaften auswirken soll.
4. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

   Mit der Abbildungsvorschrift legen Sie fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden, und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über primären Rollen einer Person ermittelt werden können.

   Welche IT Betriebsdaten erforderlich sind, ist abhängig vom Zielsystem. Für privilegierte Benutzerkonten werden folgende Einstellungen empfohlen:

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsPrivilegedAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert verwenden**.
   - Zusätzlich können Sie eine Abbildungsvorschrift für die Spalte `IdentityType` festlegen. Die Spalte besitzt verschiedene zulässige Werte, die privilegierte Benutzerkonten repräsentieren.
   - Um zu verhindern, das privilegierte Benutzerkonten die Berechtigungen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschrift für die Spalte `IsGroupAccount` mit dem Standardwert **0** und aktivieren Sie die Option **Immer Standardwert verwenden**.
5. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem.

Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.

6. Weisen Sie die Kontendefinition direkt an die Personen zu, die mit privilegierten Benutzerkonten arbeiten sollen.

   Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

TIPP: Wenn es unternehmensspezifisch erforderlich ist, dass die Anmeldenamen privilegierter Benutzerkonten einem definierten Namensschema folgen, legen Sie die Bildungsregel fest, nach der die Anmeldenamen gebildet werden.

- Um ein Präfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | Accounts | PrivilegedAccount | AccountName_Prefix**.
- Um ein Postfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | Accounts | PrivilegedAccount | AccountName_Postfix**.

Diese Konfigurationsparameter werden in der Standardinstallation ausgewertet, wenn Sie ein Benutzerkonto, mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) kennzeichnen. Die Anmeldenamen der Benutzerkonten werden entsprechend der Bildungsregeln umbenannt. Dies erfolgt auch, wenn die Benutzerkonten über den Zeitplan **Ausgewählte Benutzerkonten als privilegiert kennzeichnen** als privilegiert gekennzeichnet werden.

### Verwandte Themen

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 41

# Stammdaten für Azure Active Directory Benutzerkonten bearbeiten

Ein Benutzerkonto kann im One Identity Manager mit einer Person verbunden sein. Ebenso können Sie die Benutzerkonten getrennt von Personen verwalten.

HINWEIS: Um Benutzerkonten für die Personen eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen. Einige der nachfolgend beschriebenen Stammdaten werden dabei über Bildungsregeln aus den Personenstammdaten gebildet.

HINWEIS:Sollen Personen ihre Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen ein zentrales Benutzerkonto besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.

TIPP: Damit eine Person automatisiert ein Benutzerkonto und ein Abonnement erhält,

können Sie die Kontendefinition zur Erstellung des Benutzerkontos und das zu verwendende Abonnement in einer Systemrolle zusammenfassen.

Eine Person kann diese Systemrolle direkt erhalten, über Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen erben oder über den IT Shop bestellen.

***Um ein Benutzerkonto zu erstellen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

***Um die Stammdaten eines Benutzerkontos zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

***Um ein Benutzerkonto für eine Person manuell zuzuweisen oder zu erstellen***

1. Wählen Sie im Manager die Kategorie **Personen | Personen**.
2. Wählen Sie in der Ergebnisliste die Person und führen Sie die Aufgabe **Azure Active Directory Benutzerkonten zuweisen** aus.
3. Weisen Sie ein Benutzerkonto zu.
4. Speichern Sie die Änderungen.

## Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Azure Active Directory Benutzerkontos auf Seite 98
- Kontaktdaten eines Azure Active Directory Benutzerkontos auf Seite 101
- Organisatorische Informationen eines Azure Active Directory Benutzerkontos auf Seite 102
- Informationen zum lokalen Active Directory Benutzerkonto auf Seite 103

## Verwandte Themen

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 41
- Unterstützte Typen von Benutzerkonten auf Seite 89
- Azure Active Directory Abonnements und Dienstpläne auf Seite 146

# Allgemeine Stammdaten eines Azure Active Directory Benutzerkontos

Auf dem Tabreiter **Allgemein** erfassen Sie folgende Stammdaten.

**Tabelle 23: Allgemeine Stammdaten eines Benutzerkontos**

| Eigenschaft | Beschreibung |
|---|---|
| Person | Person, die das Benutzerkonto verwendet. Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Person bereits eingetragen. Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Person aus der Auswahlliste wählen. Wenn Sie die automatische Personenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Person gesucht und in das Benutzerkonto übernommen.<br>Für ein Benutzerkonto mit einer Identität vom Typ **Organisatorische Identität**, **Persönliche Administratoridentität**, **Zusatzidentität**, **Gruppenidentität** oder **Dienstidentität** können Sie eine neue Person erstellen. Klicken Sie dafür neben dem Eingabefeld und erfassen Sie die erforderlichen Personenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp. |
| Kontendefinition | Kontendefinition, über die das Benutzerkonto erstellt wurde.<br>Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein.<br>HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden. |
| Automatisierungsgrad | Automatisierungsgrad des Benutzerkontos. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten. |
| Mandant | Mandant des Benutzerkontos. |
| Domäne | Domäne des Benutzerkontos. |
| Standort | Standort, an dem das Benutzerkonto genutzt wird. |
| Vorname | Vorname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automa- |

| Eigenschaft | Beschreibung |
|---|---|
| | tisierungsgrad automatisch ausgefüllt. |
| Nachname | Nachname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. |
| Benutzeranmeldename | Anmeldename des Benutzerkontos. Der Benutzeranmeldename wird gebildet aus dem Alias und der Domäne. Der Benutzeranmeldename entspricht dem Benutzernamen (User Principal Name) des Benutzers im Azure Active Directory. |
| Anzeigename | Anzeigename des Benutzerkontos. |
| Alias | E-Mail Alias für das Benutzerkonto. |
| Bevorzugte Sprache | Bevorzugte Sprache des Benutzers, beispielsweise **en-US**. |
| Kennwort | Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Person kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.<br>Wenn Sie ein initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen.<br>HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien beachtet. Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die Anforderungen des Zielsystems verstößt. |
| Kennwortbestätigung | Kennwortwiederholung. |
| Kennwort bei der nächsten Anmeldung ändern | Angabe, ob der Benutzer bei der nächsten Anmeldung das Kennwort anpassen muss. |
| Kennwortrichtlinien | Kennwortrichtlinien, die für das Benutzerkonto gelten. Zur Verfügung stehen die Optionen **Keine Einschränkungen**, **Kennwort läuft nie ab** und **Schwache Kennwörter zulassen**. |
| Risikoindex (berechnet) | Maximalwert der Risikoindexwerte aller zugeordneten Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER \| CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*. |
| Kategorie | Kategorien für die Vererbung von Gruppen an das |

| Eigenschaft | Beschreibung |
| --- | --- |
| | Benutzerkonto. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien. |
| Identität | Typ der Identität des Benutzerkontos. Zulässige Werte sind:<br>• **Primäre Identität**: Standardbenutzerkonto einer Person.<br>• **Organisatorische Identität**: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.<br>• **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.<br>• **Zusatzidentität**: Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird.<br>• **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen.<br>• **Dienstidentität**: Dienstkonto. |
| Privilegiertes Benutzerkonto | Angabe, ob es sich um ein privilegiertes Benutzerkonto handelt. |
| Gruppen erbbar | Angabe, ob das Benutzerkonto Gruppen über die Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt.<br>• Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen.<br>• Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist. |
| Benutzerkonto ist deaktiviert | Angabe, ob das Benutzerkonto deaktiviert ist. Wird ein Benutzerkonto vorübergehend nicht benötigt, können Sie das Benutzerkonto über die Option zeitweilig deaktivieren. |

### Verwandte Themen

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 41
- Kennwortrichtlinien für Azure Active Directory Benutzerkonten auf Seite 61
- Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 130
- Benutzerkonten mit Personen verbinden auf Seite 88
- Unterstützte Typen von Benutzerkonten auf Seite 89
- Azure Active Directory Benutzerkonten deaktivieren auf Seite 113

# Kontaktdaten eines Azure Active Directory Benutzerkontos

Auf dem Tabreiter **Kontakt** erfassen Sie folgende Adressinformationen zur Erreichbarkeit der Person, die das Benutzerkonto verwendet.

**Tabelle 24: Kontaktdaten**

| Eigenschaft | Beschreibung |
|---|---|
| Straße | Straße. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. |
| Bundesland | Bundesland. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. |
| Ort | Ort. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. Anhand des Ortes können automatisch Standorte erzeugt und den Personen zugeordnet werden. |
| Postleitzahl | Postleitzahl. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. |
| Land | Länderkennung. |
| Geschäftstelefone | Geschäftliche Telefonnummern. |
| Mobiltelefon | Mobiltelefonnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. |
| E-Mail-Adresse | E-Mail-Adresse des Benutzers. |
| Proxy Adressen | Weitere E-Mail-Adressen des Benutzers. Als Adresstyp können Sie zusätzlich zur Standardadressierung (SMTP, X400) weitere |

| Eigenschaft | Beschreibung |
|---|---|
| | Mailkonnektoren (beispielsweise CCMail, MS) nutzen.<br>Für die Erstellung weiterer Proxy Adressen ist die folgende Syntax einzuhalten:<br>`Adresstyp: neue E-Mail-Adresse` |

# Organisatorische Informationen eines Azure Active Directory Benutzerkontos

Auf dem Tabreiter **Organisatorisch** erfassen Sie folgende organisatorischen Stammdaten.

**Tabelle 25: Organisatorische Stammdaten**

| Eigenschaft | Beschreibung |
|---|---|
| Büro | Büro. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. |
| Firma | Firma der Person. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. |
| Abteilung | Abteilung der Person. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. Anhand der Abteilungsinformation können automatisch Abteilungen erzeugt und den Personen zugeordnet werden. |
| Berufsbezeichnung | Berufsbezeichnung. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. |
| Kontomanager | Verantwortlicher für das Benutzerkonto.<br>***Um einen Kontomanager festzulegen***<br>1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.<br>2. Wählen Sie unter **Tabelle** die Tabelle, welche die Konto-manager abbildet.<br>3. Wählen Sie unter **Kontomanager** den Verantwortlichen.<br>4. Klicken Sie **OK**. |

# Informationen zum lokalen Active Directory Benutzerkonto

Auf dem Tabreiter **Verbund** werden folgende Informationen zum lokalen Active Directory Benutzerkonto, welches mit dem Azure Active Directory Benutzerkonto verbunden ist, abgebildet.

**Tabelle 26: Angaben zum lokalen Active Directory Benutzerkonto**

| Eigenschaft | Beschreibung |
|---|---|
| Synchronisation mit dem lokalen Active Directory aktiviert | Angabe, ob die Synchronisation mit einem lokalen Active Directory aktiviert ist. |
| Letzte Synchronisation | Zeitpunkt der letzten Synchronisation des Azure Active Directory Benutzerkontos mit dem lokalen Active Directory. |
| SID des lokalen Kontos | Sicherheits-ID (SID) des lokalen Active Directory Benutzerkontos. |
| Unveränderlicher Bezeichner | Unveränderlicher Bezeichner, mit dem die Beziehung zwischen Active Directory und Azure Active Directory aufrechterhalten wird. |

# Zusätzliche Aufgaben für die Verwaltung von Azure Active Directory Benutzerkonten

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

# Überblick über das Azure Active Directory Benutzerkonto

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einem Benutzerkonto.

***Um einen Überblick über ein Benutzerkonto zu erhalten***

1. Wählen Sie die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das Azure Active Directory Benutzerkonto**.

### Verwandte Themen

- Azure Active Directory Abonnements und Dienstpläne auf Seite 146

# Automatisierungsgrad von Azure Active Directory Benutzerkonten ändern

Wenn Sie Benutzerkonten über die automatische Personenzuordnung erstellen, wird der Standardautomatisierungsgrad genutzt. Sie können den Automatisierungsgrad eines Benutzerkontos nachträglich ändern.

***Um den Automatisierungsgrad für ein Benutzerkonto zu ändern***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- Stammdaten für Azure Active Directory Benutzerkonten bearbeiten auf Seite 96

# Azure Active Directory Gruppen direkt an ein Azure Active Directory Benutzerkonto zuweisen

Gruppen können einem Benutzerkonto direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Benutzerkonto im Azure Active Directory, werden die Gruppen der Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Gruppen direkt zuweisen.

HINWEIS: Benutzerkonten können nicht manuell in dynamische Gruppen aufgenommen werden.

***Um Gruppen direkt an ein Benutzerkonto zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Gruppen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Gruppe und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- Azure Active Directory Gruppe an Azure Active Directory Benutzerkonten zuweisen auf Seite 120

# Azure Active Directory Administratorrollen direkt an ein Azure Active Directory Benutzerkonto zuweisen

Administratorrollen können einem Benutzerkonto direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Administratorrollen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Benutzerkonto im Azure Active Directory, werden die Administratorrollen der Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Administratorrollen direkt zuweisen.

***Um Administratorrollen direkt an ein Benutzerkonto zuzuweisen***

1. Wählen Sie die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administratorrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrollen zu.

- ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Administratorrollen.

5. Speichern Sie die Änderungen.

### Verwandte Themen

- Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten zuweisen auf Seite 137

# Azure Active Directory Abonnements direkt an Azure Active Directory Benutzerkonten zuweisen

Abonnements können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und Abonnements in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Besitzt die Person ein Benutzerkonto im Azure Active Directory, werden die Abonnements der Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Abonnements direkt zuweisen.

***Um Abonnements direkt an ein Benutzerkonto zuzuweisen***

1. Wählen Sie die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Abonnements zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Abonnements zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Abonnements entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie das Abonnement und doppelklicken Sie .

1. Speichern Sie die Änderungen.

### Verwandte Themen

- Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten zuweisen auf Seite 148

# Unwirksamen Azure Active Directory Dienstpläne direkt an Azure Active Directory Benutzerkonten zuweisen

Unwirksame Dienstpläne können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und unwirksame Dienstpläne in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Besitzt die Person ein Benutzerkonto im Azure Active Directory, werden die unwirksamen Dienstpläne der Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die unwirksamen Dienstpläne direkt zuweisen.

***Um unwirksame Dienstpläne direkt an ein Benutzerkonto zuzuweisen***

1. Wählen Sie die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Unwirksame Dienstpläne zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die unwirksamen Dienstpläne zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Dienstplänen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie den Dienstplan und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Unwirksame Azure Active Directory Dienstpläne an Azure Active Directory Benutzerkonten zuweisen auf Seite 158

# Zusatzeigenschaften an ein Azure Active Directory Benutzerkonto zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

***Um Zusatzeigenschaften für ein Benutzerkonto festzulegen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.

3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Zusatzeigenschaften entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Zusatzeigenschaft und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Ausführliche Informationen zum Verwenden von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

# Automatische Zuordnung von Personen zu Azure Active Directory Benutzerkonten

Beim Einfügen eines Benutzerkontos kann automatisch eine vorhandene Person zugeordnet und im Bedarfsfall neu erstellt werden. Dabei werden die Personenstammdaten anhand vorhandener Benutzerstammdaten erzeugt. Dieser Mechanismus kann auf die Erstellung eines neuen Benutzerkontos durch manuelle Anlage oder Synchronisation folgen. Für die automatische Personenzuordnung definieren Sie Kriterien für die Ermittlung der Personen. Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Person verbunden, so erhält das Benutzerkonto durch interne Verarbeitung den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

Schalten Sie das Verfahren im laufenden Betrieb ein, erfolgt ab diesem Zeitpunkt die automatische Zuordnung der Personen zu Benutzerkonten. Deaktivieren Sie das Verfahren zu einem späteren Zeitpunkt wieder, wirkt sich diese Änderung nur auf Benutzerkonten aus, die ab diesem Zeitpunkt angelegt oder aktualisiert werden. Bereits vorhandene Zuordnungen von Personen zu Benutzerkonten bleiben bestehen.

HINWEIS: Für administrative Benutzerkonten wird empfohlen, die Zuordnung der Personen nicht über die automatische Personenzuordnung vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.

Führen Sie folgende Aktionen aus, damit Personen automatisch zugeordnet werden können.

- Wenn Personen bei der Synchronisation von Benutzerkonten zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | PersonAutoFullsync** und wählen Sie den gewünschte Modus.

- Wenn Personen außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | PersonAutoDefault** und wählen Sie den gewünschten Modus.
- Legen Sie im Konfigurationsparameter **TargetSystem | AzureAD | PersonExcludeList** die Benutzerkonten fest, für die keine automatische Zuordnung zu Personen erfolgen soll.

  Beispiel:

  `ADMINISTRATOR`
- Legen Sie über den Konfigurationsparameter **TargetSystem | AzureAD | PersonAutoDisabledAccounts** fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
- Weisen Sie dem Mandanten eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Personenzuordnung am Mandanten.

HINWEIS:

Für die Synchronisation gilt:

- Die automatische Personenzuordnung wirkt, wenn Benutzerkonten neu angelegt oder aktualisiert werden.

Außerhalb der Synchronisation gilt:

- Die automatische Personenzuordnung wirkt, wenn Benutzerkonten neu angelegt werden.

HINWEIS:

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für den Mandanten bekannt, werden die Benutzerkonten mit den Personen verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

Um die Benutzerkonten über Kontendefinitionen zu verwalten, weisen Sie diesen Benutzerkonten eine Kontendefinition und einen Automatisierungsgrad zu.

***Um die Benutzerkonten über Kontendefinitionen zu verwalten***

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie dem Mandanten die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
   a. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten | Verbunden aber nicht konfiguriert | <Mandant>**.

b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

c. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.

d. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.

e. Speichern Sie die Änderungen.

Ausführliche Informationen zur automatischen Personenzuordnung finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

### Verwandte Themen

- Kontendefinitionen erstellen auf Seite 41
- Kontendefinitionen an ein Zielsystem zuweisen auf Seite 58
- Bearbeiten der Suchkriterien für die automatische Personenzuordnung auf Seite 110

# Bearbeiten der Suchkriterien für die automatische Personenzuordnung

Die Kriterien für die Personenzuordnung werden am Mandanten definiert. Dabei legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person dem Benutzerkonto zugeordnet werden kann. Die Suchkriterien können Sie durch Formatdefinitionen weiter einschränken. Das zusammengestellte Suchkriterium wird in XML-Notation in die Spalte **Suchkriterien für die automatische Personenzuordnung** (`AccountToPersonMatchingRule`) der Tabelle `AADOrganization` geschrieben.

Suchkriterien werden bei der automatischen Zuordnung von Personen zu Benutzerkonten ausgewertet. Darüber hinaus können Sie anhand der Suchkriterien eine Vorschlagsliste für die Personenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen.

HINWEIS: Bei der Zuordnung der Personen zu Benutzerkonten anhand der Suchkriterien erhalten die Benutzerkonten den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

Für administrative Benutzerkonten wird empfohlen, die Zuordnung nicht anhand der Suchkriterien vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.

HINWEIS: Der One Identity Manager liefert ein Standardmapping für die Personenzuordnung. Führen Sie die folgenden Schritte nur aus, wenn Sie das Standardmapping unternehmensspezifisch anpassen möchten.

***Um Kriterien für die Personenzuordnung festzulegen***

1. Wählen Sie die Kategorie **Azure Active Directory | Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person mit dem Benutzerkonto verbunden wird.

   **Tabelle 27: Standardsuchkriterien für Benutzerkonten und Kontakte**

   | Anwenden auf | Spalte an Person | Spalte am Benutzerkonto |
   |---|---|---|
   | Azure Active Directory Benutzerkonten | Zentrales Benutzerkonto (`CentralAccount`) | Alias (`MailNickName`) |

5. Speichern Sie die Änderungen.

## Direkte Zuordnung von Personen an Benutzerkonten anhand einer Vorschlagsliste

Im Bereich **Zuordnungen** können Sie anhand der Suchkriterien eine Vorschlagsliste für die Personenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen. Die Benutzerkonten sind dafür in verschiedenen Ansichten zusammengestellt.

**Tabelle 28: Ansichten zur manuellen Zuordnung**

| Ansicht | Beschreibung |
|---|---|
| Vorgeschlagene Zuordnungen | Die Ansicht listet alle Benutzerkonten auf, denen der One Identity Manager eine Person zuordnen kann. Dazu werden die Personen angezeigt, die durch die Suchkriterien ermittelt und zugeordnet werden können. |
| Zugeordnete Benutzerkonten | Die Ansicht listet alle Benutzerkonten auf, denen eine Person zugeordnet ist. |
| Ohne Personenzuordnung | Die Ansicht listet alle Benutzerkonten auf, denen keine Person zugeordnet ist und für die über die Suchkriterien keine passende Person ermittelt werden kann. |

TIPP: Mit Maus-Doppelklick auf einen Eintrag in den Ansichten werden das Benutzerkonto und die Person geöffnet und Sie können die Stammdaten einsehen.

***Um die Suchkriterien auf die Benutzerkonten anzuwenden***

- Klicken Sie **Neu laden**.

  Für alle Benutzerkonten im Zielsystem werden die möglichen Zuordnungen anhand der Suchkriterien ermittelt. Die drei Ansichten werden aktualisiert.

***Um Personen direkt über die Vorschlagsliste zuzuordnen***

1. Klicken Sie **Vorgeschlagene Zuordnungen**.
   a. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Person zugeordnet werden soll. Eine Mehrfachauswahl ist möglich.
   b. Klicken Sie **Ausgewählte zuweisen.**
   c. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

      Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet.

   – ODER –
2. Klicken Sie **Ohne Personenzuordnung**.
   a. Klicken Sie **Person auswählen** für das Benutzerkonto, dem eine Person zugeordnet werden soll. Wählen Sie eine Person aus der Auswahlliste.
   b. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Personen zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.
   c. Klicken Sie **Ausgewählte zuweisen**.
   d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

      Den ausgewählten Benutzerkonten werden die Personen zugeordnet, die in der Spalte **Person** angezeigt werden.

***Um Zuordnungen zu entfernen***

1. Klicken Sie **Zugeordnete Benutzerkonten**.
   a. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Personenzuordnung entfernt werden soll. Mehrfachauswahl ist möglich.
   b. Klicken Sie **Ausgewählte entfernen**.
   c. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

      Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

Ausführliche Informationen zur Definition der Suchkriterien finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

## Verwandte Themen

- Automatische Zuordnung von Personen zu Azure Active Directory Benutzerkonten auf Seite 108

# Azure Active Directory Benutzerkonten deaktivieren

Wie Sie Benutzerkonten deaktivieren, ist abhängig von der Art der Verwaltung der Benutzerkonten.

### Szenario:

- Die Benutzerkonten sind mit Personen verbunden und werden über Kontendefinitionen verwaltet.

Benutzerkonten, die über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Person dauerhaft oder zeitweilig deaktiviert wird. Das Verhalten ist abhängig vom Automatisierungsgrad des Benutzerkontos. Benutzerkonten mit dem Automatisierungsgrad **Full managed** werden entsprechend der Einstellungen an der Kontendefinition deaktiviert. Für Benutzerkonten mit einem anderen Automatisierungsgrad konfigurieren Sie das gewünschte Verhalten an der Bildungsregel der Spalte `AADUser.AccountDisabled`.

### Szenario:

- Die Benutzerkonten sind mit Personen verbunden. Es sind keine Kontendefinitionen zugeordnet.

Benutzerkonten, die mit Personen verbunden sind, jedoch nicht über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Person dauerhaft oder zeitweilig deaktiviert wird. Das Verhalten ist abhängig vom Konfigurationsparameter **QER | Person | TemporaryDeactivation**.

- Ist der Konfigurationsparameter aktiviert, werden die Benutzerkonten einer Person deaktiviert, wenn die Person zeitweilig oder dauerhaft deaktiviert wird.
- Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der Person keinen Einfluss auf die verbundenen Benutzerkonten.

***Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu deaktivieren***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Benutzerkonto ist deaktiviert**.
5. Speichern Sie die Änderungen.

### Szenario:

- Benutzerkonten sind nicht mit Personen verbunden.

***Um ein Benutzerkonto zu deaktivieren, das nicht mit einer Person verbunden ist***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Benutzerkonto ist deaktiviert**.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 41
- Automatisierungsgrade erstellen auf Seite 44
- Azure Active Directory Benutzerkonten löschen und wiederherstellen auf Seite 114
- Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

# Azure Active Directory Benutzerkonten löschen und wiederherstellen

HINWEIS: Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht.

***Um ein Benutzerkonto zu löschen***

1. Wählen Sie die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Löschen Sie das Benutzerkonto.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

***Um ein Benutzerkonto wiederherzustellen***

1. Wählen Sie die Kategorie **Azure Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste die Schaltfläche **Löschen rückgängig machen**.

## Konfigurieren der Löschverzögerung

Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Die Benutzerkonten werden zunächst deaktiviert. Bis zum Ablauf der Löschverzögerung besteht die Möglichkeit die Benutzerkonten wieder zu aktivieren. Nach Ablauf der Löschverzögerung werden die Benutzerkonten aus der Datenbank gelöscht und ein Wiederherstellen ist nicht mehr möglich. Eine abweichende Löschverzögerung konfigurieren Sie im Designer an der Tabelle AADUser.

## Verwandte Themen

- Azure Active Directory Benutzerkonten deaktivieren auf Seite 113
- Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

# Azure Active Directory Gruppen

Azure Active Directory kennt verschiedene Gruppentypen, in denen Benutzer und Gruppen zusammengefasst werden können, um beispielsweise den Zugriff auf Ressourcen oder die Verteilung von E-Mails zu regeln.

Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können einzelne Stammdaten der Gruppen bearbeiten. Im One Identity Manager können Sie neue Sicherheitsgruppen erstellen. Andere Gruppentypen können Sie im One Identity Manager nicht erstellen.

Um Benutzer in Gruppen aufzunehmen, können Sie die Gruppen direkt an die Benutzer zuweisen. Sie können Gruppen an Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder den IT Shop zuweisen.

Nachfolgend sind die im One Identity Manager unterstützten Gruppentypen aufgeführt.

**Tabelle 29: Unterstützte Gruppentypen**

| Gruppentyp | Beschreibung |
|---|---|
| Sicherheitsgruppe | Über Sicherheitsgruppen werden Berechtigungen auf Ressourcen erteilt. In Sicherheitsgruppen werden Benutzerkonten und andere Gruppen aufgenommen und somit die Administration erleichtert.<br>Sicherheitsgruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager Sicherheitsgruppen bearbeiten sowie neue Sicherheitsgruppen erstellen. |
| Office 365 Gruppe | Office 365 Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager Office 365 Gruppen bearbeiten. Neue Office 365 Gruppen können Sie im One Identity Manager nicht erstellen. |
| Verteilergruppe | Verteilergruppen werden eingesetzt, um E-Mails an die Mitglieder der Gruppe zu versenden. Verteilergruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager Verteilergruppen bearbeiten. Neue Verteilergruppen können Sie im One Identity Manager nicht erstellen. |
| E-Mail aktivierte | E-Mail aktivierte Sicherheitsgruppen sind Sicherheitsgruppen, die als |

| Gruppentyp | Beschreibung |
| --- | --- |
| Sicherheitsgruppe | Verteilergruppen eingesetzt werden.<br>E-Mail aktivierte Sicherheitsgruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager E-Mail aktivierte Sicherheitsgruppen bearbeiten. Neue E-Mail aktivierte Sicherheitsgruppen können Sie im One Identity Manager nicht erstellen. |
| Dynamische Gruppe | Die Mitglieder einer dynamischen Gruppe werden nicht fest zugewiesen, sondern über definierte Regeln ermittelt. Dynamische Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Dynamische Gruppen können Sie im One Identity Manager bearbeiten. Neue dynamische Gruppen können Sie im One Identity Manager nicht erstellen. |

# Stammdaten von Azure Active Directory Gruppen bearbeiten

Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager neue Sicherheitsgruppen erstellen. Andere Gruppentypen können Sie lediglich bearbeiten. Welche Stammdaten einer Gruppe Sie bearbeiten können, ist abhängig vom Gruppentyp.

***Um die Stammdaten einer Gruppe zu bearbeiten***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
4. Speichern Sie die Änderungen.

## Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Azure Active Directory Gruppe auf Seite 117
- Informationen zur lokalen Active Directory Gruppe auf Seite 119

# Allgemeine Stammdaten einer Azure Active Directory Gruppe

Auf dem Tabreiter **Allgemein** erfassen Sie folgende Stammdaten.

**Tabelle 30: Allgemeine Stammdaten**

| Eigenschaft | Beschreibung |
|---|---|
| Anzeigename | Anzeigename zur Anzeige der Gruppe in der Benutzeroberfläche der One Identity Manager Werkzeuge. |
| Mandant | Mandant der Gruppe. |
| Alias | E-Mail Alias für die Gruppe. |
| E-Mail-Adresse | E-Mail-Adresse der Gruppe. |
| Proxy Adressen | Weitere E-Mail-Adressen der Gruppe. Als Adresstyp können Sie zusätzlich zur Standardadressierung (SMTP, X400) weitere Mailkonnektoren (beispielsweise CCMail, MS) nutzen.<br>Für die Erstellung weiterer Proxy Adressen ist die folgende Syntax einzuhalten:<br>`Adresstyp: neue E-Mail-Adresse` |
| Gruppentyp | Angabe des Typs einer Gruppe. Für Office 365 Gruppen ist der Wert **Unified** eingetragen. Für Sicherheitsgruppen und Verteilergruppen ist der Wert leer. Für dynamische Gruppen ist der Wert **DynamicMembership** eingetragen. |
| Sicherheitsgruppe | Angabe, ob es sich um eine Sicherheitsgruppe handelt. Über Sicherheitsgruppen werden Berechtigungen auf Ressourcen erteilt. In Sicherheitsgruppen werden Benutzerkonten und andere Gruppen aufgenommen und somit die Administration erleichtert. |
| E-Mail aktiviert | Angabe, ob für die Gruppe E-Mail aktiviert ist. Ist die Option für eine Sicherheitsgruppe gesetzt, dann handelt es sich um eine E-Mail aktivierte Sicherheitsgruppe. Anderenfalls handelt es sich um eine Verteilergruppe. |
| IT Shop | Angabe, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden. |
| Verwendung nur im IT Shop | Angabe, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig. |
| Leistungsposition | Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen. |
| Risikoindex | Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an |

| Eigenschaft | Beschreibung |
|---|---|
| | Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER \| CalculateRiskIndex** aktiviert ist.<br>Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*. |
| Kategorie | Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |

### Verwandte Themen

- Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 130
- Ausführliche Informationen zur Vorbereitung der Gruppen für die Bestellung über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

# Informationen zur lokalen Active Directory Gruppe

Auf dem Tabreiter **Verbund** werden folgende Informationen zur lokalen Active Directory Gruppe, welche mit der Azure Active Directory Gruppe verbunden ist, abgebildet.

**Tabelle 31: Angaben zur lokalen Active Directory Gruppe**

| Eigenschaft | Beschreibung |
|---|---|
| Synchronisation mit dem lokalen Active Directory aktiviert | Angabe, ob die Synchronisation mit einem lokalen Active Directory aktiviert ist. |
| Letzte Synchronisation | Zeitpunkt der letzten Synchronisation der Azure Active Directory Gruppe mit dem lokalen Active Directory. |
| SID der lokalen Gruppe | Sicherheits-ID (SID) der lokalen Active Directory Gruppe. |

# Azure Active Directory Gruppe an Azure Active Directory Benutzerkonten zuweisen

Gruppen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Gruppen berechnet, die einer Person zugewiesen sind.

Wenn Sie eine Person in Rollen aufnehmen und die Person ein Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Gruppen aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Gruppen erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.

Des Weiteren können Gruppen über IT Shop-Bestellungen an Personen zugewiesen werden. Damit Gruppen über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Gruppen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Gruppen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

### Detaillierte Informationen zum Thema

- Azure Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 120
- Azure Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 122
- Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Gruppe zuweisen auf Seite 123
- Azure Active Directory Gruppe in Systemrollen aufnehmen auf Seite 124
- Azure Active Directory Gruppe in den IT Shop aufnehmen auf Seite 125

# Azure Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Gruppe an Abteilungen, Kostenstellen oder Standorte zu, damit die Gruppe über diese Organisationen an Benutzerkonten zugewiesen wird.

Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

***Um eine Gruppe an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Organisationen entfernen.

   ***Um eine Zuweisung zu entfernen***
   - Wählen Sie die Organisation und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

***Um Gruppen an eine Abteilung, eine Kostenstelle oder einen Standort zuzuweisen (bei rollenbasierter Anmeldung)***

1. Wählen Sie im Manager die Kategorie **Organisationen | Abteilungen**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen | Kostenstellen**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Azure Active Directory Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Gruppen entfernen.

   ***Um eine Zuweisung zu entfernen***
   - Wählen Sie die Gruppe und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Azure Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 122
- Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Gruppe zuweisen auf Seite 123
- Azure Active Directory Gruppe in Systemrollen aufnehmen auf Seite 124
- Azure Active Directory Gruppe in den IT Shop aufnehmen auf Seite 125

- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 10

# Azure Active Directory Gruppe an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie die Gruppe an Geschäftsrollen zu, damit die Gruppe über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

***Um eine Gruppe an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

***Um Gruppen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)***

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Azure Active Directory Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Gruppen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Gruppe und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- Azure Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 120
- Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Gruppe zuweisen auf Seite 123
- Azure Active Directory Gruppe in Systemrollen aufnehmen auf Seite 124
- Azure Active Directory Gruppe in den IT Shop aufnehmen auf Seite 125
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 10

# Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Gruppe zuweisen

Gruppen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Gruppen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Benutzerkonto im Azure Active Directory, werden die Gruppen der Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppe direkt an Benutzerkonten zuweisen.

HINWEIS: Benutzerkonten können nicht manuell in dynamische Gruppen aufgenommen werden.

***Um eine Gruppe direkt an Benutzerkonten zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Benutzerkonten entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie das Benutzerkonto und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- Azure Active Directory Gruppen direkt an ein Azure Active Directory Benutzerkonto zuweisen auf Seite 104
- Azure Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 120
- Azure Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 122
- Azure Active Directory Gruppe in Systemrollen aufnehmen auf Seite 124
- Azure Active Directory Gruppe in den IT Shop aufnehmen auf Seite 125

# Azure Active Directory Gruppe in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

Mit dieser Aufgabe nehmen Sie eine Gruppe in Systemrollen auf. Wenn Sie eine Systemrolle an Personen zuweisen, wird die Gruppe an alle Benutzerkonten vererbt, die diese Personen besitzen. Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

HINWEIS: Gruppen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen*.

***Um eine Gruppe an Systemrollen zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- Azure Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 120
- Azure Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 122

- Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Gruppe zuweisen auf Seite 123
- Azure Active Directory Gruppe in den IT Shop aufnehmen auf Seite 125

# Azure Active Directory Gruppe in den IT Shop aufnehmen

Mit der Zuweisung einer Gruppe an ein IT Shop Regal kann sie von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Gruppe ist keine dynamische Gruppe.
- Die Gruppe muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Gruppe muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Gruppe im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.
- Soll die Gruppe nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Gruppe zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen oder Benutzerkonten ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Gruppen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Gruppen in den IT Shop aufzunehmen.

***Um eine Gruppe in den IT Shop aufzunehmen***

1. Wählen Sie im Managerdie Kategorie **Azure Active Directory | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Azure Active Directory Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppe an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

***Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen | Azure Active Directory Gruppen** (bei rollenbasierter Anmeldung).

2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

***Um eine Gruppe aus allen Regalen des IT Shops zu entfernen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Gruppe**n (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Azure Active Directory Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Gruppe wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Gruppe abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

## Verwandte Themen

- Allgemeine Stammdaten einer Azure Active Directory Gruppe auf Seite 117
- Azure Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 120
- Azure Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 122
- Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Gruppe zuweisen auf Seite 123
- Azure Active Directory Gruppe in Systemrollen aufnehmen auf Seite 124

# Zusätzliche Aufgaben für die Verwaltung von Azure Active Directory Gruppen

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

# Überblick über die Azure Active Directory Gruppe

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Gruppe.

***Um einen Überblick über eine Gruppe zu erhalten***

1. Wählen Sie die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die Azure Active Directory Gruppe**.

# Azure Active Directory Gruppen in Azure Active Directory Gruppen aufnehmen

Mit dieser Aufgabe nehmen Sie eine Gruppe in andere Gruppen auf.

***Um Gruppen direkt an eine Gruppe zuzuweisen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die der ausgewählten Gruppe untergeordnet sind.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Gruppen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Gruppe und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

# Wirksamkeit von Gruppenmitgliedschaften

**Tabelle 32: Konfigurationsparameter für die bedingte Vererbung**

| Konfigurationsparameter | Wirkung bei Aktivierung |
|---|---|
| QER \| Structures \| Inherite \| GroupExclusion | Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Wirksamkeit von Gruppenmitgliedschaften. Ist der Parameter aktiviert, können aufgrund von Ausschlussdefinitionen die Gruppenmitgliedschaften reduziert werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. |

Bei der Zuweisung von Gruppen an Benutzerkonten kann es vorkommen, dass eine Person zwei oder mehr Gruppen erhält, die in dieser Kombination nicht auftreten dürfen. Um das zu verhindern, geben Sie die sich ausschließenden Gruppen bekannt. Dabei legen Sie für zwei Gruppen fest, welche der beiden Gruppen an Benutzerkonten wirksam werden soll, wenn beide zugewiesen sind.

Die Zuweisung einer ausgeschlossenen Gruppe ist jederzeit direkt, indirekt oder per IT Shop-Bestellung möglich. Anschließend ermittelt der One Identity Manager, ob diese Zuweisung wirksam ist.

HINWEIS:

- Ein wechselseitiger Ausschluss zweier Gruppen kann nicht definiert werden. Das heißt, die Festlegung "Gruppe A schließt Gruppe B aus" `UND` "Gruppe B schließt Gruppe A aus" ist nicht zulässig.
- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.
- Ob die Mitgliedschaft einer ausgeschlossenen Gruppe in einer anderen Gruppe zulässig ist (Tabelle), wird durch den One Identity Manager nicht überprüft.

Die Wirksamkeit der Zuweisungen wird in den Tabellen `AADUserInGroup` und `AADBaseTreeHasGroup` über die Spalte `XIsInEffect` abgebildet.

### Beispiel für die Wirksamkeit von Gruppenmitgliedschaften

- In einem Mandanten ist eine Gruppe A mit Berechtigungen zum Auslösen von Bestellungen definiert. Eine Gruppe B berechtigt zum Anweisen von Zahlungen. Eine Gruppe C berechtigt zum Prüfen von Rechnungen.
- Gruppe A wird über die Abteilung "Marketing", Gruppe B über die Abteilung "Finanzen" und Gruppe C wird über die Geschäftsrolle "Kontrollgruppe" zugewiesen.

Clara Harris hat ein Benutzerkonto in diesem Mandanten. Sie gehört primär der Abteilung "Marketing" an. Sekundär sind ihr die Geschäftsrolle "Kontrollgruppe" und die Abteilung "Finanzen" zugewiesen. Ohne Ausschlussdefinition erhält das Benutzerkonto alle Berechtigungen der Gruppen A, B und C.

Durch geeignete Maßnahmen soll verhindert werden, dass eine Person sowohl Bestellungen auslösen als auch Rechnungen zur Zahlung anweisen kann. Das heißt, die Gruppen A und B schließen sich aus. Eine Person, die Rechnungen prüft, darf ebenfalls keine Rechnungen zur Zahlung anweisen. Das heißt, die Gruppen B und C schließen sich aus.

**Tabelle 33: Festlegen der ausgeschlossenen Gruppen (Tabelle `AADGroupExclusion`)**

| Wirksame Gruppe | Ausgeschlossene Gruppe |
|---|---|
| Gruppe A | |
| Gruppe B | Gruppe A |
| Gruppe C | Gruppe B |

**Tabelle 34: Wirksame Zuweisungen**

| Person | Mitglied in Rolle | Wirksame Gruppe |
|---|---|---|
| Ben King | Marketing | Gruppe A |
| Jan Bloggs | Marketing, Finanzen | Gruppe B |
| Clara Harris | Marketing, Finanzen, Kontrollgruppe | Gruppe C |
| Jenny Basset | Marketing, Kontrollgruppe | Gruppe A, Gruppe C |

Für Clara Harris ist nur die Zuweisung der Gruppe C wirksam und wird ins Zielsystem publiziert. Verlässt Clara Harris die Geschäftsrolle "Kontrollgruppe" zu einem späteren Zeitpunkt, wird die Gruppe B ebenfalls wirksam.

Für Jenny Basset sind die Gruppen A und C wirksam, da zwischen beiden Gruppen kein Ausschluss definiert wurde. Das heißt, die Person ist berechtigt Bestellungen auszulösen und Rechnungen zu prüfen. Soll das verhindert werden, definieren Sie einen weiteren Ausschluss für die Gruppe C.

**Tabelle 35: Ausgeschlossene Gruppen und wirksame Zuweisungen**

| Person | Mitglied in Rolle | Zugewiesene Gruppe | Ausgeschlossene Gruppe | Wirksame Gruppe |
|---|---|---|---|---|
| Jenny Basset | Marketing | Gruppe A | | Gruppe C |
| | Kontrollgruppe | Gruppe C | Gruppe B<br>Gruppe A | |

### Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.
- Sich ausschließende Gruppen gehören zum selben Mandanten.

***Um Gruppen auszuschließen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste eine Gruppe.
3. Wählen Sie die Aufgabe **Gruppen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die sich mit der gewählten Gruppe ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

# Vererbung von Azure Active Directory Gruppen anhand von Kategorien

Im One Identity Manager können Gruppen, Administratorrollen, Abonnements und unwirksame Dienstpläne selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen (Administratorrollen, Abonnements, unwirksame Dienstpläne) und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In den übrigen Tabellen geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen , Administratorrollen, Abonnements und unwirksamen Dienstpläne an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

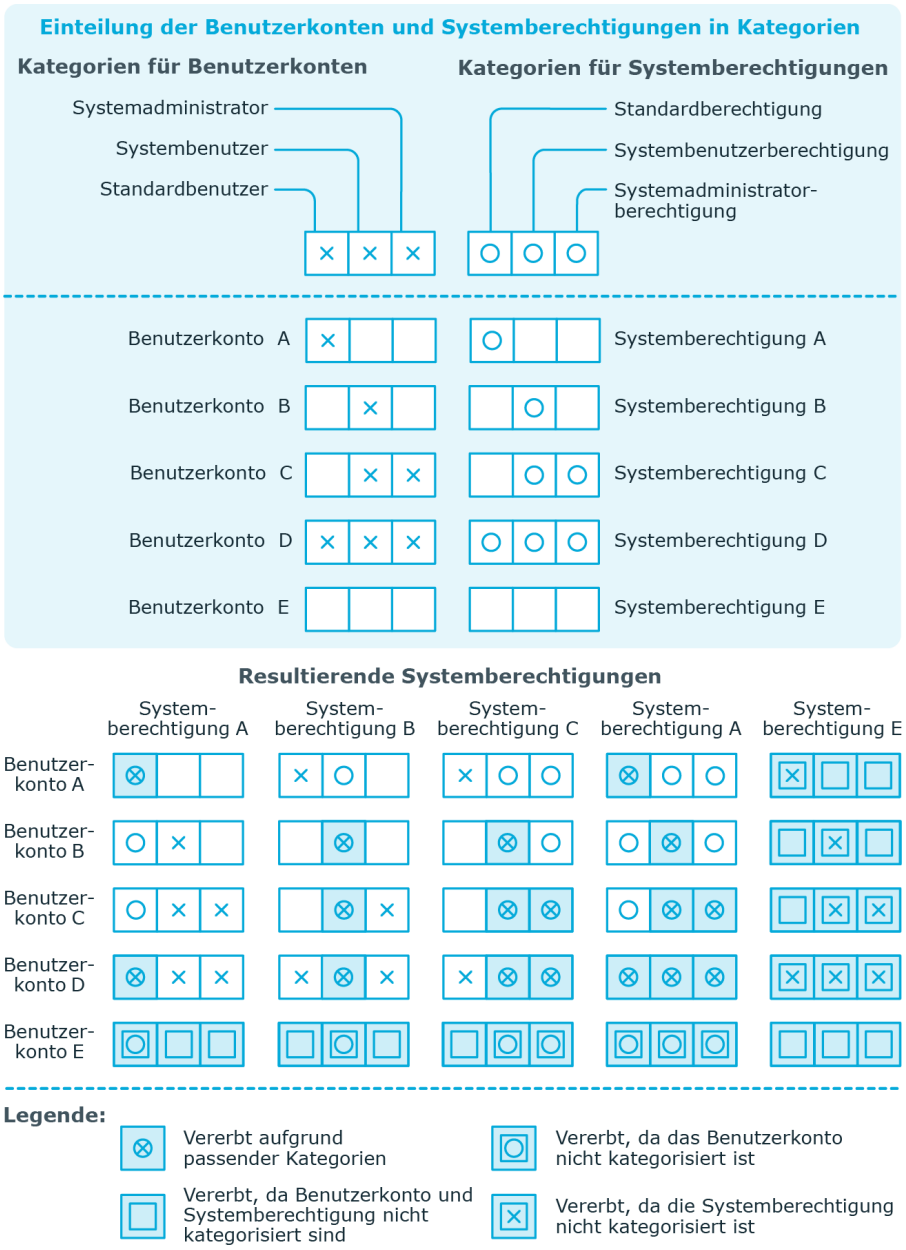
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist die Gruppe oder das Benutzerkonto nicht in Kategorien eingestuft, dann wird die Gruppe ebenfalls an das Benutzerkonto vererbt.

HINWEIS: Die Vererbung über Kategorien wird nur bei der indirekten Zuweisung von Gruppen über hierarchische Rollen berücksichtigt. Bei der direkten Zuweisung von Gruppen an Benutzerkonten werden die Kategorien nicht berücksichtigt.

**Tabelle 36: Beispiele für Kategorien**

| Kategorieposition | Kategorien für Benutzerkonten | Kategorien für Gruppen |
|---|---|---|
| 1 | Standardbenutzer | Standardberechtigung |
| 2 | Systembenutzer | Systembenutzerberechtigung |
| 3 | Systemadministrator | Systemadministratorberechtigung |

**Abbildung 2: Beispiel für die Vererbung über Kategorien**




### *Um die Vererbung über Kategorien zu nutzen*

- Definieren Sie am Mandanten die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Gruppen über ihre Stammdaten zu.

### Verwandte Themen

- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 85
- Allgemeine Stammdaten eines Azure Active Directory Benutzerkontos auf Seite 98
- Allgemeine Stammdaten einer Azure Active Directory Gruppe auf Seite 117
- Stammdaten von Azure Active Directory Abonnements bearbeiten auf Seite 147

# Eigentümer an Azure Active Directory Gruppen zuweisen

Die Eigentümer einer Gruppen können die Eigenschaften einer Gruppe bearbeiten.

***Um Eigentümer an eine Gruppe zuzuweisen***

1. Wählen Sie die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste **Tabelle** die Tabelle, welche die Eigentümer enthält. Zur Auswahl stehen:
    - Azure Active Directory Benutzerkonten
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Eigentümer zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Eigentümer.
6. Speichern Sie die Änderungen.

# Zusatzeigenschaften an eine Azure Active Directory Gruppe zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

***Um Zusatzeigenschaften für eine Gruppe festzulegen***

1. Wählen Sie im Manager die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Zusatzeigenschaften entfernen.

***Um eine Zuweisung zu entfernen***

- Wählen Sie die Zusatzeigenschaft und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Ausführliche Informationen zur Einrichtung von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

# Azure Active Directory Gruppen löschen

***Um eine Gruppe zu löschen***

1. Wählen Sie die Kategorie **Azure Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Löschen Sie die Gruppe über die Schaltfläche .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Gruppe wird endgültig aus der One Identity Manager-Datenbank und der Azure Active Directory-Umgebung gelöscht.

# Azure Active Directory Administratorrollen

Mithilfe von Administratorrollen können Sie Benutzern administrative Berechtigungen zuweisen. Azure Active Directory kennt verschiedene Administratorrollen, die unterschiedliche Funktionen erfüllen. Ausführliche Informationen zu Administratorrollen finden Sie in der Azure Active Directory Dokumentation von Microsoft.

Administratorrollen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können einzelne Stammdaten der Administratorrollen bearbeiten. Neue Administratorrollen können Sie im One Identity Manager nicht erstellen.

Um Benutzer in Administratorrollen aufzunehmen, können Sie die Administratorrollen direkt an die Benutzer zuweisen. Sie können Administratorrollen an Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder den IT Shop zuweisen.

## Stammdaten von Azure Active Directory Administratorrollen bearbeiten

Administratorrollen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können einzelne Stammdaten der Administratorrollen bearbeiten. Neue Administratorrollen können Sie im One Identity Manager nicht erstellen.

***Um die Stammdaten einer Administratorrolle zu bearbeiten***

1. Wählen Sie die Kategorie **Azure Active Directory | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten für eine Administratorrolle.
4. Speichern Sie die Änderungen.

**Tabelle 37: Stammdaten einer Administratorrolle**

| Eigenschaft | Beschreibung |
|---|---|
| Anzeigename | Anzeigename zur Anzeige der Administratorrolle in der Benutzeroberfläche der One Identity Manager Werkzeuge. |
| Mandant | Mandant der Administratorrolle. |
| ID der Vorlage | ID der Administratorrollenvorlage auf der diese Administratorrolle basiert. |
| IT Shop | Angabe, ob die Administratorrolle über den IT Shop bestellbar ist. Die Administratorrolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Administratorrolle kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden. |
| Verwendung nur im IT Shop | Angabe, ob die Administratorrolle ausschließlich über den IT Shop bestellbar ist. Die Administratorrolle kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Administratorrolle an hierarchische Rollen ist nicht zulässig. |
| Leistungsposition | Angabe einer Leistungsposition, um die Administratorrolle über den IT Shop zu bestellen. |
| Risikoindex | Wert zur Bewertung des Risikos von Zuweisungen der Administratorrolle an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER \| CalculateRiskIndex** aktiviert ist.<br>Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*. |
| Kategorie | Kategorien für die Vererbung von Administratorrollen. Administratorrollen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Administratorrollen und die Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie die Administratorrolle einer oder mehreren Kategorien zu. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |

## Verwandte Themen

- Vererbung von Azure Active Directory Administratorrollen anhand von Kategorien auf Seite 144
- Ausführliche Informationen zur Vorbereitung der Administratorrollen für die Bestellung über den IT Shop finden Sie im One Identity Manager Administrationshandbuch für IT Shop.

# Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten zuweisen

Administratorrollen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Administratorrollen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Administratorrollen berechnet, die einer Person zugewiesen sind.

Wenn Sie eine Person in Rollen aufnehmen und die Person ein Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Administratorrollen aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Administratorrollen erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.

Des Weiteren können Administratorrollen über IT Shop-Bestellungen an Personen zugewiesen werden. Damit Administratorrollen über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Administratorrollen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Administratorrollen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

### Detaillierte Informationen zum Thema

- Azure Active Directory Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 137
- Azure Active Directory Administratorrolle an Geschäftsrollen zuweisen auf Seite 139
- Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Administratorrolle zuweisen auf Seite 140
- Azure Active Directory Administratorrolle in Systemrollen aufnehmen auf Seite 141
- Azure Active Directory Administratorrolle in den IT Shop aufnehmen auf Seite 141

# Azure Active Directory Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Administratorrolle an Abteilungen, Kostenstellen oder Standorte zu, damit die Administratorrolle über diese Organisationen an Benutzerkonten zugewiesen wird.

***Um eine Administratorrolle an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Azure Active Directory | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Organisationen entfernen.

   ***Um eine Zuweisung zu entfernen***
   - Wählen Sie die Organisation und doppelklicken Sie .
5. Speichern Sie die Änderungen.

***Um Administratorrollen an eine Abteilung, eine Kostenstelle oder einen Standort zuzuweisen (bei rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**.

   - ODER -

   Wählen Sie die Kategorie **Organisationen | Kostenstellen**.

   - ODER -

   Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Azure Active Directory Administratorrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrollen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Administratorrollen.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Azure Active Directory Administratorrolle an Geschäftsrollen zuweisen auf Seite 139
- Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Administratorrolle zuweisen auf Seite 140
- Azure Active Directory Administratorrolle in Systemrollen aufnehmen auf Seite 141
- Azure Active Directory Administratorrolle in den IT Shop aufnehmen auf Seite 141
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 10

# Azure Active Directory Administratorrolle an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie die Administratorrolle an Geschäftsrollen zu, damit die Administratorrolle über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

***Um eine Administratorrolle an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Azure Active Directory | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

***Um Administratorrollen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Azure Active Directory Administratorrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrollen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Administratorrollen.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Azure Active Directory Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 137
- Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Administratorrolle zuweisen auf Seite 140
- Azure Active Directory Administratorrolle in Systemrollen aufnehmen auf Seite 141
- Azure Active Directory Administratorrolle in den IT Shop aufnehmen auf Seite 141

- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 10

# Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Administratorrolle zuweisen

Administratorrollen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Administratorrollen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Benutzerkonto im Azure Active Directory, werden die Administratorrollen der Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Administratorrolle direkt an Benutzerkonten zuweisen.

***Um eine Administratorrolle direkt an Benutzerkonten zuzuweisen***

1. Wählen Sie die Kategorie **Azure Active Directory | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Benutzerkonten entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie das Benutzerkonto und doppelklicken Sie .
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Azure Active Directory Administratorrollen direkt an ein Azure Active Directory Benutzerkonto zuweisen auf Seite 105
- Azure Active Directory Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 137
- Azure Active Directory Administratorrolle an Geschäftsrollen zuweisen auf Seite 139
- Azure Active Directory Administratorrolle in Systemrollen aufnehmen auf Seite 141
- Azure Active Directory Administratorrolle in den IT Shop aufnehmen auf Seite 141

# Azure Active Directory Administratorrolle in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

Mit dieser Aufgabe nehmen Sie eine Administratorrolle in Systemrollen auf. Wenn Sie eine Systemrolle an Personen zuweisen, wird die Administratorrolle an alle Benutzerkonten vererbt, die diese Personen besitzen.

HINWEIS: Administratorrollen, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist. Weitere Informationen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen*.

***Um eine Administratorrolle an Systemrollen zuzuweisen***

1. Wählen Sie die Kategorie **Azure Active Directory | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Systemrolle und doppelklicken Sie .
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Azure Active Directory Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 137
- Azure Active Directory Administratorrolle an Geschäftsrollen zuweisen auf Seite 139
- Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Administratorrolle zuweisen auf Seite 140
- Azure Active Directory Administratorrolle in den IT Shop aufnehmen auf Seite 141

# Azure Active Directory Administratorrolle in den IT Shop aufnehmen

Mit der Zuweisung einer Administratorrolle an ein IT Shop Regal kann diese von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Die Administratorrolle muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Administratorrolle muss eine Leistungsposition zugeordnet sein.
- Soll die Administratorrolle nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Administratorrolle zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Administratorrollen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Administratorrollen in den IT Shop aufzunehmen.

***Um eine Administratorrolle in den IT Shop aufzunehmen***

1. Wählen Sie die Kategorie **Azure Active Directory | Administratorrollen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Azure Active Directory Administratorrollen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrolle an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

***Um eine Administratorrolle aus einzelnen Regalen des IT Shops zu entfernen***

1. Wählen Sie die Kategorie **Azure Active Directory | Administratorrollen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Azure Active Directory Administratorrollen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Administratorrolle aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

***Um eine Administratorrolle aus allen Regalen des IT Shops zu entfernen***

1. Wählen Sie die Kategorie **Azure Active Directory | Administratorrollen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Azure Active Directory Administratorrollen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Administratorrolle.

3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Die Administratorrolle wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Administratorrolle abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

### Verwandte Themen

- Stammdaten von Azure Active Directory Administratorrollen bearbeiten auf Seite 135
- Azure Active Directory Administratorrolle an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 137
- Azure Active Directory Administratorrolle an Geschäftsrollen zuweisen auf Seite 139
- Azure Active Directory Benutzerkonten direkt an eine Azure Active Directory Administratorrolle zuweisen auf Seite 140
- Azure Active Directory Administratorrolle in Systemrollen aufnehmen auf Seite 141

# Zusätzliche Aufgaben für die Verwaltung von Azure Active Directory Administratorrollen

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

# Überblick über die Azure Active Directory Administratorrolle

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einer Administratorrolle.

***Um einen Überblick über eine Administratorrolle zu erhalten***

1. Wählen Sie die Kategorie **Azure Active Directory | Administratorrollen** .
2. Wählen Sie in der Ergebnisliste die Administratorrolle.

3. Wählen Sie die Aufgabe **Überblick über die Azure Active Directory Administratorrolle**.

# Vererbung von Azure Active Directory Administratorrollen anhand von Kategorien

Das unter Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 130 beschriebene Verhalten können Sie auch für Administratorrollen einsetzen.

***Um die Vererbung über Kategorien zu nutzen***

- Definieren Sie am Mandanten die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Administratorrollen über ihre Stammdaten zu.

## Verwandte Themen

- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 85
- Allgemeine Stammdaten eines Azure Active Directory Benutzerkontos auf Seite 98
- Stammdaten von Azure Active Directory Administratorrollen bearbeiten auf Seite 135

# Zusatzeigenschaften an eine Azure Active Directory Administratorrolle zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

***Um Zusatzeigenschaften für eine Administratorrolle festzulegen***

1. Wählen Sie die Kategorie **Azure Active Directory | Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Zusatzeigenschaften entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Zusatzeigenschaft und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Ausführliche Informationen zum Verwenden von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

# 8

# Azure Active Directory Abonnements und Dienstpläne

Um auf die Dienstpläne im Azure Active Directory zuzugreifen, benötigen die Benutzer ein Abonnement. Ein Benutzer erhält alle Dienstpläne, die mit einem Abonnement verknüpft sind. Um den Benutzern Abonnements zur Verfügung zu stellen, können Sie die Abonnements direkt an die Benutzer zuweisen. Sie können Abonnements an Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder den IT Shop zuweisen.

Um für die Benutzer die Nutzung einzelner Dienstpläne zu unterbinden, werden im One Identity Manager zusätzlich sogenannte "unwirksame Dienstpläne" abgebildet. Unwirksame Dienstpläne werden nach der Synchronisation der Abonnements automatisch im One Identity Manager erzeugt. Unwirksame Dienstpläne werden über den IT Shop bestellt oder über Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder Systemrollen den Benutzern zugewiesen.

Aus den Abonnements eines Benutzers mit den damit verbundenen Dienstplänen und der Zuweisung unwirksamer Dienstpläne ergeben sich die tatsächlich für den Benutzer im Azure Active Directory verfügbaren Dienstpläne.

## Azure Active Directory Abonnements

Die Informationen zu Abonnements und Dienstplänen innerhalb eines Mandanten werden durch die Synchronisation in den One Identity Manager eingelesen. Neue Abonnements und Dienstpläne können Sie im One Identity Manager nicht erstellen. Sie können im One Identity Manager einzelne Stammdaten der Abonnements für die Bestellung im IT Shop und die Zuweisung an Benutzerkonten bearbeiten.

# Stammdaten von Azure Active Directory Abonnements bearbeiten

***Um die Stammdaten eines Abonnements zu bearbeiten***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Abonnements.
5. Speichern Sie die Änderungen.

**Tabelle 38: Stammdaten eines Abonnements**

| Eigenschaft | Beschreibung |
|---|---|
| SKU Anzeigename | SKU Anzeigename des Abonnements, beispielsweise AAD_Premium oder RMSBASIC. |
| Mandant | Mandant, zu dem dieses Abonnement eingetragen ist. |
| Abonnementstatus | Angabe des Status des Abonnements, beispielsweise **enabled** (aktiv). |
| Gekaufte Lizenzen | Anzahl der gekauften Lizenzen. |
| Zugewiesene Lizenzen | Anzahl der aktiv genutzten Lizenzen. |
| Gesperrte Lizenzen | Anzahl der gesperrten Lizenzen. |
| Warnungseinheiten | Anzahl der Lizenzen, die im Warnungsstatus sind. |
| IT Shop | Angabe, ob das Abonnement über den IT Shop bestellbar ist. Das Abonnement kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Das Abonnement kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden. |
| Verwendung nur im IT Shop | Angabe, ob das Abonnement ausschließlich über den IT Shop bestellbar ist. Das Abonnement kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung des Abonnements an hierarchische Rollen ist nicht zulässig. |
| Leistungsposition | Angabe einer Leistungsposition, um das Abonnement über den IT Shop zu bestellen. |
| Risikoindex | Wert zur Bewertung des Risikos von Zuweisungen des Abonnement an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER** |

| Eigenschaft | Beschreibung |
|---|---|
| | **\| CalculateRiskIndex** aktiviert ist.<br>Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen.* |
| Kategorie | Kategorien für die Vererbung von Abonnements. Abonnements können selektiv an Benutzerkonten vererbt werden. Dazu werden die Abonnements und die Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie das Abonnement einer oder mehreren Kategorien zu. |

### Verwandte Themen

- Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 130
- Ausführliche Informationen zur Vorbereitung der Abonnements für die Bestellung über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

# Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten zuweisen

Abonnements können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und Abonnements in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Abonnements berechnet, die einer Person zugewiesen sind.

Besitzt die Person ein Benutzerkonto im Azure Active Directory, werden die Abonnements der Rollen an dieses Benutzerkonto vererbt.

Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Abonnements erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.

Des Weiteren können Abonnements über IT Shop-Bestellungen an Personen zugewiesen werden. Damit Abonnements über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Abonnements, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Abonnements werden nach erfolgreicher Genehmigung den Personen zugewiesen.

TIPP: Damit eine Person automatisiert ein Benutzerkonto und ein Abonnement erhält, können Sie die Kontendefinition zur Erstellung des Benutzerkontos und das zu verwendende Abonnement in einer Systemrolle zusammenfassen.

Eine Person kann diese Systemrolle direkt erhalten, über Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen erben oder über den IT Shop bestellen.

### Detaillierte Informationen zum Thema

- Azure Active Directory Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 149
- Azure Active Directory Abonnement an Geschäftsrollen zuweisen auf Seite 150
- Azure Active Directory Benutzerkonten direkt an ein Azure Active Directory Abonnement zuweisen auf Seite 151
- Azure Active Directory Abonnement in Systemrollen aufnehmen auf Seite 152
- Azure Active Directory Abonnement in den IT Shop aufnehmen auf Seite 153

# Azure Active Directory Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Abonnements an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen wird.

***Um ein Abonnement an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Organisationen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Organisation und doppelklicken Sie .
5. Speichern Sie die Änderungen.

***Um Abonnements an eine Abteilung, eine Kostenstelle oder einen Standort zuzuweisen (bei rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**.

   - ODER -

   Wählen Sie die Kategorie **Organisationen | Kostenstellen**.

   - ODER -

   Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Azure Active Directory Abonnement zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Abonnements zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Abonnements.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- Azure Active Directory Abonnement an Geschäftsrollen zuweisen auf Seite 150
- Azure Active Directory Benutzerkonten direkt an ein Azure Active Directory Abonnement zuweisen auf Seite 151
- Azure Active Directory Abonnement in Systemrollen aufnehmen auf Seite 152
- Azure Active Directory Abonnement in den IT Shop aufnehmen auf Seite 153
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 10

# Azure Active Directory Abonnement an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie die Abonnements an Geschäftsrollen zu, damit die sie über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

***Um ein Abonnement an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.

***Um eine Zuweisung zu entfernen***

- Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

***Um Abonnements an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Azure Active Directory Abonnements zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Abonnements zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Abonnements.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- Azure Active Directory Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 149
- Azure Active Directory Benutzerkonten direkt an ein Azure Active Directory Abonnement zuweisen auf Seite 151
- Azure Active Directory Abonnement in Systemrollen aufnehmen auf Seite 152
- Azure Active Directory Abonnement in den IT Shop aufnehmen auf Seite 153
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 10

# Azure Active Directory Benutzerkonten direkt an ein Azure Active Directory Abonnement zuweisen

Abonnements können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und Abonnements in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Besitzt die Person ein Benutzerkonto im Azure Active Directory, werden die Abonnements der Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Abonnements direkt zuweisen.

***Um ein Abonnement direkt an Benutzerkonten zuzuweisen***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Benutzerkonten entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie das Benutzerkonto und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

### Verwandte Themen

- Azure Active Directory Abonnements direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 106
- Azure Active Directory Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 149
- Azure Active Directory Abonnement an Geschäftsrollen zuweisen auf Seite 150
- Azure Active Directory Abonnement in Systemrollen aufnehmen auf Seite 152
- Azure Active Directory Abonnement in den IT Shop aufnehmen auf Seite 153

# Azure Active Directory Abonnement in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

Mit dieser Aufgabe nehmen Sie ein Abonnement in Systemrollen auf. Wenn Sie eine Systemrolle an Personen zuweisen, wird das Abonnement an alle Benutzerkonten vererbt, die diese Personen besitzen.

HINWEIS: Abonnements, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist. Weitere Informationen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen*.

***Um ein Abonnement an Systemrollen zuzuweisen***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

***Um eine Zuweisung zu entfernen***

- Wählen Sie die Systemrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

### Verwandte Themen

- Azure Active Directory Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 149
- Azure Active Directory Abonnement an Geschäftsrollen zuweisen auf Seite 150
- Azure Active Directory Benutzerkonten direkt an ein Azure Active Directory Abonnement zuweisen auf Seite 151
- Azure Active Directory Abonnement in den IT Shop aufnehmen auf Seite 153

# Azure Active Directory Abonnement in den IT Shop aufnehmen

Mit der Zuweisung eines Abonnements an ein IT Shop Regal kann dieses von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Das Abonnement muss mit der Option **IT Shop** gekennzeichnet sein.
- Dem Abonnement muss eine Leistungsposition zugeordnet sein.
- Soll das Abonnement nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss das Abonnement zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren Abonnements an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Abonnements in den IT Shop aufzunehmen.

***Um ein Abonnement in den IT Shop aufzunehmen***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Azure Active Directory Abonnements** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** das Abonnement an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

***Um ein Abonnement aus einzelnen Regalen des IT Shops zu entfernen***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Azure Active Directory Abonnements** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** das Abonnement aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

***Um ein Abonnement aus allen Regalen des IT Shops zu entfernen***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Azure Active Directory Abonnements** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Das Abonnement wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen dieses Abonnements abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

## Verwandte Themen

- Stammdaten von Azure Active Directory Abonnements bearbeiten auf Seite 147
- Azure Active Directory Abonnement an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 149
- Azure Active Directory Abonnement an Geschäftsrollen zuweisen auf Seite 150
- Azure Active Directory Benutzerkonten direkt an ein Azure Active Directory Abonnement zuweisen auf Seite 151
- Azure Active Directory Abonnement in Systemrollen aufnehmen auf Seite 152

# Zusätzliche Aufgaben für die Verwaltung von Azure Active Directory Abonnements

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

# Überblick über Azure Active Directory Abonnements

***Um einen Überblick über ein Abonnement zu erhalten***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Überblick über das Azure Active Directory Abonnement**.

***Um einen Überblick über einen Dienstplan zu erhalten***

1. Wählen Sie die Kategorie **Azure Active Directory | Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Überblick über den Azure Active Directory Dienstplan**.

***Um einen Überblick über einen unwirksamen Dienstpläne zu erhalten***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Überblick über den unwirksamen Azure Active Directory Dienstplan**.

# Wirksamkeit von Abonnementzuweisungen

Das unter Wirksamkeit von Gruppenmitgliedschaften auf Seite 128 beschriebene Verhalten können Sie auch für Abonnements einsetzen. Die Wirksamkeit der Zuweisungen wird in den Tabellen `AADUserHasSubSku` und `AADBaseTreeHasSubSku` über die Spalte `XIsInEffect` abgebildet.

## Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.

- Sich ausschließende Abonnements gehören zum selben Mandanten.

***Um Abonnements auszuschließen***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Abonnements ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Abonnements zu, die sich mit dem gewählten Abonnement ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Abonnements, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

# Vererbung von Azure Active Directory Abonnements anhand von Kategorien

Das unter Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 130 beschriebene Verhalten können Sie auch für Abonnements einsetzen.

***Um die Vererbung über Kategorien zu nutzen***

- Definieren Sie am Mandanten die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Abonnements über ihre Stammdaten zu.

### Verwandte Themen

- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 85
- Allgemeine Stammdaten eines Azure Active Directory Benutzerkontos auf Seite 98
- Stammdaten von Azure Active Directory Abonnements bearbeiten auf Seite 147

# Zusatzeigenschaften an ein Azure Active Directory Abonnement zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

***Um Zusatzeigenschaften für ein Abonnement festzulegen***

1. Wählen Sie die Kategorie **Azure Active Directory | Abonnements**.
2. Wählen Sie in der Ergebnisliste das Abonnement.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Zusatzeigenschaften entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Zusatzeigenschaft und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Ausführliche Informationen zum Verwenden von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

# Unwirksame Azure Active Directory Dienstpläne

Um für die Benutzer die Nutzung einzelner Dienstpläne zu unterbinden, werden im One Identity Manager zusätzlich sogenannte "unwirksame Dienstpläne" abgebildet. Unwirksame Dienstpläne werden nach der Synchronisation der Abonnements automatisch im One Identity Manager erzeugt. Unwirksame Dienstpläne werden über den IT Shop bestellt oder über Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder Systemrollen den Benutzern zugewiesen.

# Stammdaten von unwirksamen Azure Active Directory Dienstplänen bearbeiten

***Um die Stammdaten eines unwirksamen Dienstplans zu bearbeiten***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Dienstplans.
5. Speichern Sie die Änderungen.

**Tabelle 39: Stammdaten eines unwirksamen Dienstplans**

| Eigenschaft | Beschreibung |
|---|---|
| Abonnement | Bezeichnung des Abonnements. |
| Dienstplan | Bezeichnung des Dienstplans. |
| IT Shop | Angabe, ob der unwirksame Dienstplan über den IT Shop bestellbar ist. Der unwirksame Dienstplan kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Der unwirksame Dienstplan kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden. |
| Verwendung nur im IT Shop | Angabe, ob der unwirksame Dienstplan ausschließlich über den IT Shop bestellbar ist. Der unwirksame Dienstplan kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung des unwirksamen Dienstplans an hierarchische Rollen ist nicht zulässig. |
| Leistungsposition | Angabe einer Leistungsposition, um den unwirksamen Dienstplan über den IT Shop zu bestellen. |
| Kategorie | Kategorien für die Vererbung von unwirksamen Dienstplänen. Unwirksame Dienstpläne können selektiv an Benutzerkonten vererbt werden. Dazu werden die unwirksamen Dienstpläne und die Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie den unwirksamen Dienstplan einer oder mehreren Kategorien zu. |

### Verwandte Themen

- Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 130
- Ausführliche Informationen zur Vorbereitung der Dienstpläne für die Bestellung über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

# Unwirksame Azure Active Directory Dienstpläne an Azure Active Directory Benutzerkonten zuweisen

Unwirksame Dienstpläne können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und unwirksame Dienstpläne in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die unwirksamen Dienstplänen berechnet, die einer Person zugewiesen sind.

Besitzt die Person ein Benutzerkonto im Azure Active Directory, werden die unwirksamen Dienstpläne der Rollen an dieses Benutzerkonto vererbt.

Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und unwirksame Dienstpläne erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.

Des Weiteren können unwirksame Dienstpläne über IT Shop-Bestellungen an Personen zugewiesen werden. Damit unwirksame Dienstpläne über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle unwirksamen Dienstpläne, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte unwirksame Dienstpläne werden nach erfolgreicher Genehmigung den Personen zugewiesen.

### Detaillierte Informationen zum Thema

- Unwirksamen Azure Active Directory Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 159
- Unwirksamen Azure Active Directory Dienstplan an Geschäftsrollen zuweisen auf Seite 161
- Azure Active Directory Benutzerkonten direkt an unwirksamen Azure Active Directory Dienstplan zuweisen auf Seite 162
- Unwirksamen Azure Active Directory Dienstplan in Systemrollen aufnehmen auf Seite 163
- Unwirksamen Azure Active Directory Dienstplan in den IT Shop aufnehmen auf Seite 164

# Unwirksamen Azure Active Directory Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die unwirksamen Dienstpläne an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen wird.

***Um einen unwirksamen Dienstplan an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

    TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von

Organisationen entfernen.

***Um eine Zuweisung zu entfernen***

- Wählen Sie die Organisation und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

***Um unwirksame Dienstpläne an eine Abteilung, eine Kostenstelle oder einen Standort zuzuweisen (bei rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Organisationen | Abteilungen**.

   - ODER -

   Wählen Sie die Kategorie **Organisationen | Kostenstellen**.

   - ODER -

   Wählen Sie die Kategorie **Organisationen | Standorte**.
2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.
3. Wählen Sie die Aufgabe **Unwirksamen Azure Active Directory Dienstplan zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** das Azure Active Directory Abonnement und weisen die unwirksamen Dienstpläne zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Dienstplänen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie den Dienstplan und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Unwirksamen Azure Active Directory Dienstplan an Geschäftsrollen zuweisen auf Seite 161
- Azure Active Directory Benutzerkonten direkt an unwirksamen Azure Active Directory Dienstplan zuweisen auf Seite 162
- Unwirksamen Azure Active Directory Dienstplan in Systemrollen aufnehmen auf Seite 163
- Unwirksamen Azure Active Directory Dienstplan in den IT Shop aufnehmen auf Seite 164
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 10

# Unwirksamen Azure Active Directory Dienstplan an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie die unwirksamen Dienstpläne an Geschäftsrollen zu, damit die sie über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

***Um einen unwirksamen Dienstplan an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

***Um unwirksame Dienstpläne an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)***

1. Wählen Sie die Kategorie **Geschäftsrollen | <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.
3. Wählen Sie die Aufgabe **Unwirksamen Azure Active Directory Dienstplan zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** das Azure Active Directory Abonnement und weisen die unwirksamen Dienstpläne zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Dienstplänen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie den Dienstplan und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Unwirksamen Azure Active Directory Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 159

- Azure Active Directory Benutzerkonten direkt an unwirksamen Azure Active Directory Dienstplan zuweisen auf Seite 162
- Unwirksamen Azure Active Directory Dienstplan in Systemrollen aufnehmen auf Seite 163
- Unwirksamen Azure Active Directory Dienstplan in den IT Shop aufnehmen auf Seite 164
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 10

# Azure Active Directory Benutzerkonten direkt an unwirksamen Azure Active Directory Dienstplan zuweisen

Unwirksame Dienstpläne können Sie einem Benutzerkonto direkt oder indirekt zuweisen. Bei der indirekten Zuweisung werden Personen und unwirksame Dienstpläne in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Besitzt die Person ein Benutzerkonto im Azure Active Directory, werden die unwirksamen Dienstpläne der Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die unwirksamen Dienstpläne direkt zuweisen.

***Um einen unwirksamen Dienstplan direkt an Benutzerkonten zuzuweisen***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Benutzerkonten entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie das Benutzerkonto und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Unwirksamen Azure Active Directory Dienstpläne direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 107
- Unwirksamen Azure Active Directory Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 159
- Unwirksamen Azure Active Directory Dienstplan an Geschäftsrollen zuweisen auf Seite 161

- Unwirksamen Azure Active Directory Dienstplan in Systemrollen aufnehmen auf Seite 163
- Unwirksamen Azure Active Directory Dienstplan in den IT Shop aufnehmen auf Seite 164

# Unwirksamen Azure Active Directory Dienstplan in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

Mit dieser Aufgabe nehmen Sie einen unwirksamen Dienstplan in Systemrollen auf. Wenn Sie eine Systemrolle an Personen zuweisen, wird der unwirksame Dienstplan an alle Benutzerkonten vererbt, die diese Personen besitzen.

HINWEIS: Unwirksame Dienstpläne, bei denen die Option **Verwendung nur im IT Shop** aktiviert ist, können nur an Systemrollen zugewiesen werden, bei denen diese Option ebenfalls aktiviert ist. Weitere Informationen finden Sie im *One Identity Manager Administrationshandbuch für Systemrollen*.

***Um einen unwirksamen Dienstplan an Systemrollen zuzuweisen***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Systemrollen entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

## Verwandte Themen

- Unwirksamen Azure Active Directory Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 159
- Unwirksamen Azure Active Directory Dienstplan an Geschäftsrollen zuweisen auf Seite 161
- Azure Active Directory Benutzerkonten direkt an unwirksamen Azure Active Directory Dienstplan zuweisen auf Seite 162
- Unwirksamen Azure Active Directory Dienstplan in den IT Shop aufnehmen auf Seite 164

# Unwirksamen Azure Active Directory Dienstplan in den IT Shop aufnehmen

Mit der Zuweisung eines unwirksamen Dienstplans an ein IT Shop Regal kann dieser von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Der unwirksame Dienstplan muss mit der Option **IT Shop** gekennzeichnet sein.
- Dem unwirksamen Dienstplan muss eine Leistungsposition zugeordnet sein.
- Soll der unwirksame Dienstplan nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss der Dienstplan zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.

HINWEIS: Bei rollenbasierter Anmeldung können die IT Shop Administratoren unwirksame Dienstpläne an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt unwirksame Dienstpläne in den IT Shop aufzunehmen.

***Um einen unwirksamen Dienstplan in den IT Shop aufzunehmen***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Unwirksame Azure Active Directory Dienstpläne** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** den Dienstplan an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

***Um einen unwirksamen Dienstplan aus einzelnen Regalen des IT Shops zu entfernen***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Unwirksame Azure Active Directory Dienstpläne** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** den Dienstplan aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

***Um einen unwirksamen Dienstplan aus allen Regalen des IT Shops zu entfernen***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | Unwirksame Azure Active Directory Dienstpläne** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Der unwirksame Dienstplan wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen dieses unwirksamen Dienstplans abbestellt.

Ausführliche Informationen zur Bestellung von Unternehmensressourcen über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

### Verwandte Themen

- Unwirksamen Azure Active Directory Dienstplan an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 159
- Unwirksamen Azure Active Directory Dienstplan an Geschäftsrollen zuweisen auf Seite 161
- Azure Active Directory Benutzerkonten direkt an unwirksamen Azure Active Directory Dienstplan zuweisen auf Seite 162
- Unwirksamen Azure Active Directory Dienstplan in Systemrollen aufnehmen auf Seite 163

# Zusätzliche Aufgaben für die Verwaltung von unwirksamen Azure Active Directory Dienstplänen

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

# Überblick über unwirksamen Azure Active Directory Dienstpläne

***Um einen Überblick über einen unwirksamen Dienstpläne zu erhalten***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Überblick über den unwirksamen Azure Active Directory Dienstplan**.

# Wirksamkeit von Zuweisungen unwirksamer Dienstpläne

Das unter Wirksamkeit von Gruppenmitgliedschaften auf Seite 128 beschriebene Verhalten können Sie auch für unwirksame Dienstpläne einsetzen. Die Wirksamkeit der Zuweisungen wird in den Tabellen `AADUserHasDeniedService` und `AADBaseTreeHasDeniedService` über die Spalte `XIsInEffect` abgebildet.

## Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.
- Sich ausschließende unwirksamen Dienstpläne gehören zum selben Mandanten.

***Um Abonnements auszuschließen***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den unwirksamen Dienstplan.
3. Wählen Sie die Aufgabe **Unwirksame Dienstpläne ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die unwirksamen Dienstpläne zu, die sich mit dem gewählten Dienstplan ausschließen.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die unwirksamen Dienstpläne, die sich nicht länger ausschließen.
5. Speichern Sie die Änderungen.

# Vererbung von unwirksamen Azure Active Directory Dienstplänen anhand von Kategorien

Das unter Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 130 beschriebene Verhalten können Sie auch für unwirksame Dienstpläne einsetzen.

***Um die Vererbung über Kategorien zu nutzen***

- Definieren Sie am Mandanten die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den unwirksamen Dienstplänen über ihre Stammdaten zu.

### Verwandte Themen

- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 85
- Allgemeine Stammdaten eines Azure Active Directory Benutzerkontos auf Seite 98
- Stammdaten von unwirksamen Azure Active Directory Dienstplänen bearbeiten auf Seite 157

# Zusatzeigenschaften an einen unwirksamen Azure Active Directory Dienstplan zuweisen

Zusatzeigenschaften sind Meta-Objekte, für die es im One Identity Manager-Datenmodell keine direkte Abbildung gibt, wie beispielsweise Buchungskreise, Kostenrechnungskreise oder Kostenstellenbereiche.

***Um Zusatzeigenschaften für einen unwirksamen Dienstplan festzulegen***

1. Wählen Sie die Kategorie **Azure Active Directory | Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   TIPP: Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Zusatzeigenschaften entfernen.

   ***Um eine Zuweisung zu entfernen***

   - Wählen Sie die Zusatzeigenschaft und doppelklicken Sie ✓.
5. Speichern Sie die Änderungen.

Ausführliche Informationen zum Verwenden von Zusatzeigenschaften finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

# 9

# Berichte über Azure Active Directory Objekte

Der One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen Objekten der One Identity Manager-Datenbank aufbereitet sind. Für Azure Active Directory stehen folgende Berichte zur Verfügung.

HINWEIS: Abhängig von den vorhandenen Modulen können weitere Berichte zur Verfügung stehen.

**Tabelle 40: Berichte für das Zielsystem**

| Bericht | Beschreibung |
|---|---|
| Übersicht aller Zuweisungen | Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Mandanten mindestens ein Benutzerkonto besitzen. |
| Unverbundene Benutzerkonten anzeigen | Der Bericht zeigt alle Benutzerkonten des Mandanten, denen keine Person zugeordnet ist. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung. |
| Personen mit mehreren Benutzerkonten anzeigen | Der Bericht zeigt alle Personen, die mehrere Benutzerkonten im Mandanten besitzen. Der Bericht enthält eine Risikoeinschätzung. |
| Ungenutzte Benutzerkonten anzeigen | Der Bericht enthält alle Benutzerkonten des Mandanten, die in den letzten Monaten nicht verwendet wurden. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung. |
| Abweichende Systemberechtigungen anzeigen | Der Bericht enthält alle Gruppen des Mandanten, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager. |
| Benutzerkonten mit einer überdurchschnittlichen Anzahl an | Der Bericht enthält alle Benutzerkonten des Mandanten, die eine überdurchschnittliche Anzahl an Gruppenmitgliedschaften besitzen. |

| Bericht | Beschreibung |
| --- | --- |
| Systemberechtigungen anzeigen | |
| Azure Active Directory Benutzerkonten- und Gruppenverteilung | Der Bericht enthält eine Zusammenfassung zur Benutzerkonten- und Gruppenverteilung aller Mandanten. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**. |
| Datenqualität der Azure Active Directory Benutzerkonten | Der Bericht enthält verschiedenen Auswertungen zur Datenqualität der Benutzerkonten aller Mandanten. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**. |

# Übersicht aller Zuweisungen

Für einige Objekte, wie beispielsweise Berechtigungen, Complianceregeln oder Rollen wird der Bericht **Übersicht aller Zuweisungen** angezeigt. Der Bericht ermittelt alle Rollen, wie beispielsweise Abteilungen, Kostenstellen, Standorte, Geschäftsrollen und IT Shop Strukturen, in denen sich Personen befinden, die das gewählte Basisobjekt besitzen. Dabei werden sowohl direkte als auch indirekte Zuweisungen des Basisobjektes berücksichtigt.

## Beispiele

- Wird der Bericht für eine Ressource erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Ressource besitzen.
- Wird der Bericht für eine Gruppe oder andere Systemberechtigung erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Gruppe oder Systemberechtigung besitzen.
- Wird der Bericht für eine Complianceregel erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Complianceregel verletzen.
- Wird der Bericht für eine Abteilung erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Abteilung ebenfalls Mitglied sind.
- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Geschäftsrolle ebenfalls Mitglied sind.

***Um detaillierte Informationen über Zuweisungen anzuzeigen***

- Um den Bericht anzuzeigen, wählen Sie in der Navigation oder in der Ergebnisliste das Basisobjekt und wählen Sie den Bericht **Übersicht aller Zuweisungen**.
- Wählen Sie über die Schaltfläche **Verwendet von** in der Symbolleiste des Berichtes die Rollenklasse, für die Sie ermitteln möchten, ob es Rollen gibt, in denen sich Personen mit dem ausgewählten Basisobjekt befinden.

Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.

- Mit einem Maus-Doppelklick auf das Steuerelement einer Rolle zeigen Sie alle untergeordneten Rollen der ausgewählten Rolle an.
- Mit einem einfachen Mausklick auf die Schaltfläche im Steuerelement einer Rolle zeigen Sie alle Personen dieser Rolle an, die das Basisobjekt besitzen.
- Über den Pfeil rechts neben der Schaltfläche starten Sie einen Assistenten, mit dem Sie die Liste der angezeigten Personen zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Personen werden der Geschäftsrolle zugeordnet.

**Abbildung 3: Symbolleiste des Berichts Übersicht aller Zuweisungen**


**Tabelle 41: Bedeutung der Symbole in der Symbolleiste des Berichts**

| Symbol | Bedeutung |
|---|---|
| | Anzeigen der Legende mit der Bedeutung der Steuerelemente des Berichts. |
| | Speichern der aktuellen Ansicht des Berichts als Bild. |
| | Auswählen der Rollenklasse, über die der Bericht erstellt werden soll. |
| | Anzeige aller Rollen oder Anzeige der betroffenen Rolle. |

# Anhang A

# Konfigurationsparameter für die Verwaltung einer Azure Active Directory-Umgebung

Mit der Installation des Moduls sind zusätzlich folgende Konfigurationsparameter im One Identity Manager verfügbar.

**Tabelle 42: Konfigurationsparameter**

| Konfigurationsparameter | Beschreibung |
|---|---|
| TargetSystem \| AzureAD | Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems Azure Active Directory. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. |
| TargetSystem \| AzureAD \| Accounts | Der Konfigurationsparameter erlaubt die Konfiguration der Angaben zu Benutzerkonten. |
| TargetSystem \| AzureAD \| Accounts \| InitialRandomPassword | Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind. |
| TargetSystem \| AzureAD \| Accounts \| InitialRandomPassword \| SendTo | Der Konfigurationsparameter enthält die Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Rolle, Verantwortlicher der Person oder XUserInserted). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter **TargetSystem \| AzureAD \| DefaultAddress** hinterlegte Adresse versandt. |
| TargetSystem \| AzureAD \| Accounts \| | Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den |

| Konfigurationsparameter | Beschreibung |
|---|---|
| InitialRandomPassword \| SendTo \| MailTemplateAccountName | Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet. |
| TargetSystem \| AzureAD \| Accounts \| InitialRandomPassword \| SendTo \| MailTemplatePassword | Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** verwendet. |
| TargetSystem \| AzureAD \| Accounts \| MailTemplateDefaultValues | Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto mit Standardwerten** verwendet. |
| TargetSystem \| AzureAD \| Accounts \| PrivilegedAccount | Der Konfigurationsparameter erlaubt die Konfiguration der Einstellungen für privilegierte Azure Active Directory Benutzerkonten. |
| TargetSystem \| AzureAD \| Accounts \| PrivilegedAccount \| AccountName_Postfix | Der Konfigurationsparameter enthält das Postfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten. |
| TargetSystem \| AzureAD \| Accounts \| PrivilegedAccount \| AccountName_Prefix | Der Konfigurationsparameter enthält das Präfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten. |
| TargetSystem \| AzureAD \| DefaultAddress | Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem. |
| TargetSystem \| AzureAD \| MaxFullsyncDuration | Der Konfigurationsparameter enthält die maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt. |
| TargetSystem \| AzureAD \| PersonAutoDefault | Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden. |

| Konfigurationsparameter | Beschreibung |
| --- | --- |
| TargetSystem \| AzureAD \| PersonAutoDisabledAccounts | Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition. |
| TargetSystem \| AzureAD \| PersonAutoFullSync | Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden. |
| TargetSystem \| AzureAD \| PersonExcludeList | Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (\|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird.<br>Beispiel:<br>`ADMINISTRATOR` |

# Anhang B

# Standardprojektvorlage für Azure Active Directory

Eine Standardprojektvorlage sorgt dafür, dass alle benötigten Informationen im One Identity Manager angelegt werden. Dazu gehören beispielsweise die Mappings, Workflows und das Basisobjekt der Synchronisation. Wenn Sie keine Standardprojektvorlage verwenden, müssen Sie das Basisobjekt der Synchronisation selbst im One Identity Manager bekannt geben.

Verwenden Sie eine Standardprojektvorlage für die initiale Einrichtung des Synchronisationsprojektes. Für kundenspezifische Implementierungen können Sie das Synchronisationsprojekt mit dem Synchronization Editor erweitern.

Die Vorlage verwendet Mappings für die folgenden Schematypen.

**Tabelle 43: Abbildung der Azure Active Directory Schematypen auf Tabellen im One Identity Manager Schema**

| Schematyp im Azure Active Directory | Tabelle im One Identity Manager Schema |
|---|---|
| DirectoryRole | AADDirectoryRole |
| Group | AADGroup |
| LicenseAssignments | AADUserHasSubSku |
| Organization | AADOrganization |
| ServicePlans | AADServicePlan |
| SubscribedSku | AADSubSku |
| User | AADUser |
| Verified Domain | AADVerifiedDomain |

# Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

## Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie https://www.oneidentity.com/company/contact-us.aspx.

## Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter https://support.oneidentity.com/ zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter www.YouTube.com/OneIdentity
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

# Index

## B



## E



## I



## J



## K

## L



## M



## O



## P



## S

## Z