One Identity Manager 9.2

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 - 06. Januar 2024, 01:55 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter One Identity Manager Dokumentation.

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 Identitäten eines Unternehmens mit den benötigten Benutzerkonten versorgt. Dabei können Sie unterschiedliche Mechanismen für die Verbindung der Identitäten mit ihren Benutzerkonten nutzen. Ebenso können Sie die Benutzerkonten getrennt von Identitäten 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.

HINWEIS: Voraussetzung für die Verwaltung einer Azure Active Directory-Umgebung im One Identity Manager ist die Installation des Azure Active Directory Moduls. Ausführliche Informationen zur Installation finden Sie im *One Identity Manager Installationshandbuch.*

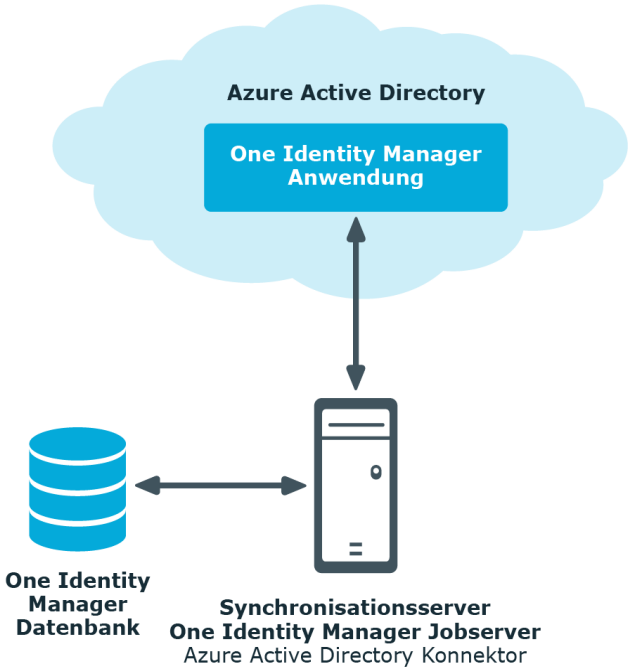
Architekturüberblick

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 Anwendung für den One Identity Manager, die im Azure Active Directory Mandanten integriert wird und mit den entsprechenden Zugriffsberechtigungen ausgestattet wird.

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

Benutzer	Aufgaben
	Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen. • Legen die Zielsystemverantwortlichen fest. • Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein. • Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen. • Berechtigen weitere Identitäten als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Azure Active Directory** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Identitäten anlegen, die nicht den Identitätstyp **Primäre Identität** haben. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Identitäten als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden

Benutzer	Aufgaben
	nicht in Anwendungsrollen aufgenommen. One Identity Manager Administratoren: • Erstellen bei Bedarf im Designer kundenspezifische Berechtigungsgruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Berechtigungsgruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
Administratoren für den IT Shop	Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • 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. Benutzer mit dieser Anwendungsrolle: • Entscheiden über Bestellungen. • Bearbeiten die Leistungspositionen und Servicekategorien, für die sie verantwortlich sind.
Administratoren für Organisationen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Organisationen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Abteilungen, Kostenstellen und Standorte zu.
Administratoren für Geschäftsrollen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Geschäftsrollen |**

Benutzer	Aufgaben
	Administratoren zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Geschäftsrollen zu.

Konfigurationsparameter für die Verwaltung von Azure Active Directory-Umgebungen

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 286.

Synchronisieren einer Azure Active Directory-Umgebung

HINWEIS: Die Synchronisation folgender nationaler Cloudbereitstellungen mit dem Azure Active Directory Konnektor wird nicht unterstützt.

- Microsoft Cloud for US Government (L5)
- Microsoft Cloud Germany
- Azure Active Directory und Office 365 betrieben von 21Vianet in China

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

Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und einem Azure Active Directory Mandanten sorgt der One Identity Manager Service.

Informieren Sie sich hier:

- wie Sie die Synchronisation einrichten, um initial Daten aus einem Azure Active Directory Mandanten in die One Identity Manager-Datenbank einzulesen,
- wie Sie eine Synchronisationskonfiguration anpassen, beispielsweise um verschiedene Azure Active Directory Mandanten mit ein und demselben Synchronisationsprojekt zu synchronisieren,
- wie Sie die Synchronisation starten und deaktivieren,
- wie Sie die Synchronisationsergebnisse auswerten.

TIPP: Bevor Sie die Synchronisation mit einem Azure Active Directory Mandanten einrichten, machen Sie sich mit dem Synchronization Editor vertraut. Ausführliche Informationen über dieses Werkzeug finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Einrichten der Initialsynchronisation mit einem Azure Active Directory Mandanten auf Seite 17

- Anpassen der Synchronisationskonfiguration für Azure Active Directory-Umgebungen auf Seite 36
- Ausführen einer Synchronisation auf Seite 54
- Aufgaben nach einer Synchronisation auf Seite 58
- Fehleranalyse auf Seite 62
- Verarbeitung von Azure Active Directory Systemobjekten auf Seite 293

Einrichten der Initialsynchronisation mit einem Azure Active Directory Mandanten

Der Synchronization Editor stellt eine Projektvorlage bereit, mit der die Synchronisation von Benutzerkonten und Berechtigungen der Azure Active Directory-Umgebung eingerichtet werden kann. Nutzen Sie diese Projektvorlage, um Synchronisationsprojekte zu erstellen, mit denen Sie Daten aus einem Azure Active Directory Mandanten in Ihre One Identity Manager-Datenbank einlesen. Zusätzlich werden die notwendigen Prozesse angelegt, über die Änderungen an Zielsystemobjekten aus der One Identity Manager-Datenbank in das Zielsystem provisioniert werden.

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

1. Stellen Sie sicher, dass der Azure Active Directory Mandant eine Lizenz mit dem Dienst **SharePoint Online** besitzt.

   HINWEIS: Ist keine solche Lizenz vorhanden, tritt beim Laden der Azure Active Directory Benutzerkonten ein Fehler auf. Weitere Informationen finden Sie unter Mögliche Fehler bei der Synchronisation eines Azure Active Directory Mandanten auf Seite 284.

2. Registrieren Sie für den One Identity Manager eine Anwendung in ihrem Azure Active Directory Mandanten.

   Abhängig davon, wie die Anwendung für den One Identity Manager im Azure Active Directory Mandanten registriert ist, wird entweder ein Benutzerkonto mit ausreichenden Berechtigungen oder der geheime Schlüssel benötigt.

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.

HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

- 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.

Detaillierte Informationen zum Thema

- Registrieren einer Unternehmensanwendung für den One Identity Manager im Azure Active Directory Mandanten auf Seite 18
- Benutzer und Berechtigungen für die Synchronisation mit dem Azure Active Directory auf Seite 22
- Einrichten des Azure Active Directory Synchronisationsservers auf Seite 24
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure Active Directory Mandanten auf Seite 28
- Synchronisationsprojekte für die Einladung von Gastbenutzern anpassen auf Seite 39
- Konfigurationsparameter für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 286
- Standardprojektvorlagen für Azure Active Directory auf Seite 290

Registrieren einer Unternehmensanwendung für den One Identity Manager im Azure Active Directory Mandanten

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

- Registrieren Sie die One Identity Manager-Anwendung im Microsoft Azure Portal (https://portal.azure.com/) oder im Azure Active Directory Admin Center (https://admin.microsoft.com/).

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

Ausführliche Informationen zum Registrieren einer Anwendung finden Sie unter https://docs.microsoft.com/azure/active-directory/develop/quickstart-register-app.

- Für die Authentifizierung an der Anwendung stehen zwei Wege zur Auswahl.
  - Authentifizierung im Kontext eines Verzeichnisbenutzers (delegierte Berechtigungen)

    Wenn Sie die Authentifizierung im Kontext eines Verzeichnisbenutzers nutzen, benötigen Sie bei der Einrichtung des Synchronisationsprojektes ein Benutzerkonto mit ausreichenden Berechtigungen.
  - Authentifizierung im Kontext einer Anwendung (Anwendungsberechtigungen)

    Wenn Sie die Authentifizierung im Kontext einer Anwendung nutzen, benötigen Sie bei der Einrichtung des Synchronisationsprojektes den Wert des geheimen Schlüssels. Der geheime Schlüssel wird bei der Registrierung der One Identity Manager-Anwendung des Azure Active Directory Mandanten erzeugt.

    HINWEIS: Der Schlüssel ist nur begrenzte Zeit gültig und muss nach Ablauf ausgetauscht werden.

Um die Authentifizierung im Kontext eines Verzeichnisbenutzers (delegierte Berechtigungen) zu konfigurieren

1. Im Microsoft Azure Portal wählen Sie unter **App-Registrierungen** Ihre Anwendung.
2. Legen Sie unter **Verwalten > Authentifizierung** folgende Einstellungen fest.
   a. Im Bereich **Plattformkonfiguration** klicken Sie **Plattform hinzufügen** und wählen Sie unter **Plattformen konfigurieren** die Kachel **Mobilgerät- und Desktopanwendungen**.
      i. Unter **Benutzerdefinierte Umleitungs-URIs** können Sie eine beliebige URI angeben.
      ii. Klicken Sie **Konfigurieren**.
   b. Im Bereich **Unterstützte Kontotypen** wählen Sie **Nur Konten in diesem Organisationsverzeichnis (einzelner Mandant)**.
   c. Im Bereich **Erweiterte Einstellungen** aktivieren Sie die Option **Öffentliche Clientflows zulassen**.
3. Legen Sie unter **Verwalten > API-Berechtigungen** die Berechtigungen fest.
   a. Im Bereich **Konfigurierte Berechtigungen** klicken Sie **Berechtigung hinzufügen**.
      i. Wählen Sie unter **API-Berechtigungen anfordern > Microsoft-APIs** die Kachel **Microsoft Graph**.
      ii. Wählen Sie **Delegierte Berechtigungen** und wählen Sie folgende Berechtigungen aus:

- **Directory.AccessAsUser.All** (Access directory as the signed in user)
- **Directory.ReadWrite.All** (Read and write directory data)
- **AuditLog.Read.All** (Read all login times)
- **User.ReadWrite.all** (Read and write all users' full profile)
- **Group.ReadWrite.all** (Read and write all groups)
- **openid** (Sign users in)

iii. Klicken Sie **Berechtigungen hinzufügen**.

b. Im Bereich **Konfigurierte Berechtigungen** klicken Sie **Administratorzustimmung für ... erteilen** und bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die konfigurierten Berechtigungen werden damit aktiv.

Um die Authentifizierung im Kontext einer Anwendung (Anwendungsberechtigungen) zu konfigurieren

1. Im Microsoft Azure Portal wählen Sie unter **App-Registrierungen** Ihre Anwendung.
2. Legen Sie unter **Verwalten > Authentifizierung** folgende Einstellungen fest.
   a. Im Bereich **Plattformkonfiguration** klicken Sie **Plattform hinzufügen** wählen Sie unter **Plattformen konfigurieren** die Kachel **Web**.
      i. Unter **Umleitungs-URIs** können Sie eine beliebige URI angeben.
      ii. Klicken Sie **Konfigurieren**.
   b. Im Bereich **Unterstützte Kontotypen** wählen Sie **Nur Konten in diesem Organisationsverzeichnis (einzelner Mandant)**.
   c. Im Bereich **Erweiterte Einstellungen** aktivieren Sie die Option **Öffentliche Clientflows zulassen**.
3. Legen Sie unter **Verwalten > API-Berechtigungen** die Berechtigungen fest.
   a. Im Bereich **Konfigurierte Berechtigungen** klicken Sie **Berechtigung hinzufügen**.
      i. Wählen Sie unter **API-Berechtigungen anfordern > Microsoft-APIs** die Kachel **Microsoft Graph**.
      ii. Wählen Sie **Anwendungsberechtigungen** und wählen Sie folgende Berechtigungen aus:
         - **Application.ReadWrite.All** (Read and write all applications)
         - **Directory.ReadWrite.All** (Read directory data)
         - **Group.ReadWrite.All** (Read and write all groups)
         - **Policy.Read.All** (Read your organization's policies)

- **RoleManagement.ReadWrite.Directory** (Read and write all directory RBAC settings)
- **User.ReadWrite.All** (Read and write all users' full profile)

iii. Klicken Sie **Berechtigungen hinzufügen**.

b. Im Bereich **Konfigurierte Berechtigungen** klicken Sie **Administratorzustimmung für ... erteilen** und bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die konfigurierten Berechtigungen werden damit aktiv.

4. Erzeugen Sie unter **Verwalten > Zertifikate & Geheimnisse** einen geheimen Schlüssel oder verwenden Sie ein Zertifikat.
   a. Verwendung eines geheimen Schlüssels:
      i. Im Bereich **Geheime Clientschlüssel** klicken Sie **Neuer geheimer Schlüssel**.
      ii. Erfassen Sie eine Beschreibung und die Gültigkeitsdauer für den geheimen Schlüssel.
      iii. Klicken Sie **Hinzufügen**.
      iv. Der geheime Schlüssel wird generiert und im Bereich **Geheime Clientschlüssel** angezeigt.
   b. Verwendung eines Verbindungszertifikats:
      i. Sie benötigen ein **X.509 Zertifikat** inklusive privaten Schlüssels als `*.CER` oder `*.PFX` - Datei.
      ii. Die Verwendung eines selbstsignierten Zertifikats ist möglich. Informationen zur Erstellung finden Sie unter **Erstellen Sie ein selbstsigniertes öffentliches Zertifikat zum Authentifizieren Ihrer Anwendung**.
      iii. Importieren Sie das Zertifikat (`*.PFX`) in den Zertifikatsspeicher des Jobservers und der administrativen Arbeitsstation, welche zur Einrichtung der Synchronisation verwendet wird.

      - ODER -

      Öffnen Sie die `*.CER` - Datei und kopieren sich den Wert "Thumbprint" aus den Eigenschaften. Dieser wird im Verbindungsdialog benötigt.
5. Zuweisen der Rolle Benutzeradministrator im **Azure Active Directory** Portal.
   a. Im Bereich **Rollen und Administratoren** wählen Sie die Rolle **Benutzeradministrator**.
   b. Wählen Sie unter **Zuweisung hinzufügen** die gewünschte Anwendung.
   c. Klicken Sie **Zuweisen.**

Verwandte Themen

- Benutzer und Berechtigungen für die Synchronisation mit dem Azure Active Directory auf Seite 22
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Azure Active Directory Mandanten auf Seite 28

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 Azure Active Directory oder Wert des geheimen Schlüssels	Abhängig davon, wie die One Identity Manager-Anwendung im Azure Active Directory Mandanten registriert ist, wird entweder ein Benutzerkonto mit ausreichenden Berechtigungen oder der geheime Schlüssel benötigt. • Wenn Sie die Authentifizierung im Kontext eines Verzeichnisbenutzers nutzen (delegierte Berechtigungen), benötigen Sie bei der Einrichtung des Synchronisationsprojektes ein Benutzerkonto, welches Mitglied in der Azure Active Directory Administratorrolle **Globaler Administrator** ist. Die Zuweisung der Azure Active Directory Administratorrolle an das Benutzerkonto nehmen Sie im Azure Active Directory Admin Center vor. Ausführliche Informationen zum Verwalten von Berechtigungen in Azure Active Directory finden Sie in der *Microsoft Dokumentation*. HINWEIS: Das Benutzerkonto für den Zugriff auf Azure Active Directory darf keine Multifaktor-Authentifizierung nutzen, damit automatisierte Anmeldungen in einem Benutzerkontext möglich sind. • Wenn Sie die Authentifizierung im Kontext einer Anwendung nutzen

Benutzer	Berechtigungen
	(Anwendungsberechtigungen), benötigen Sie bei der Einrichtung des Synchronisationsprojektes den Wert des geheimen Schlüssels. Der geheime Schlüssel, wird bei der Registrierung der One Identity Manager-Anwendung des Azure Active Directory Mandanten erzeugt. HINWEIS: Der Schlüssel ist nur begrenzte Zeit gültig und muss nach Ablauf ausgetauscht werden.
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Berechtigungen für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Berechtigungen für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%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.

Verwandte Themen

- Registrieren einer Unternehmensanwendung für den One Identity Manager im Azure Active Directory Mandanten auf Seite 18

Einrichten des Azure Active Directory Synchronisationsservers

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.

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Azure Active Directory Konnektor installiert werden.

Detaillierte Informationen zum Thema

- Systemanforderungen für den Azure Active Directory Synchronisationsserver auf Seite 24
- One Identity Manager Service mit Azure Active Directory Konnektor installieren auf Seite 25

Systemanforderungen für den Azure Active Directory Synchronisationsserver

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 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- Microsoft .NET Framework Version 4.8 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.

One Identity Manager Service mit Azure Active Directory Konnektor installieren

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Azure Active Directory Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

Tabelle 3: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	Azure Active Directory Konnektor
Maschinenrolle	Server | Job Server | Azure Active Directory

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 einen Jobserver einzurichten, führen Sie folgende Schritte aus.

1. Erstellen Sie einen Jobserver und installieren und konfigurieren Sie den One Identity Manager Service.

   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.
   - Installation der One Identity Manager Service-Komponenten entsprechend der Maschinenrollen.
   - Konfigurieren des One Identity Manager Service.
   - Starten des One Identity Manager Service.

   Mit dem Server Installer können Sie den One Identity Manager Service lokal oder remote installieren.

   Für die Remote-Installation des One Identity Manager Service stellen Sie eine administrative Arbeitstation bereit, auf der die One Identity Manager-Komponenten installiert sind. Für eine lokale Installation stellen Sie sicher, dass die One Identity Manager-Komponenten auf dem Server installiert sind. Ausführliche Informationen zur Installation der One Identity Manager-Komponenten finden Sie im *One Identity Manager Installationshandbuch*.

2. Wenn Sie mit einer verschlüsselten One Identity Manager-Datenbank arbeiten, geben Sie dem One Identity Manager Service den Datenbankschlüssel bekannt. Ausführliche Informationen zum Arbeiten mit einer verschlüsselten

One Identity Manager-Datenbank finden Sie im *One Identity Manager Installationshandbuch*.

3. 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 Erfassen der Verbindungsinformationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

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

1. Starten Sie das Programm Server Installer.

   HINWEIS: Für eine Remote-Installation starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation. Für eine lokale Installation starten Sie das Programm auf dem Server.

2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.

   Für die Verbindung zur Datenbank können Sie eine Verbindung über den Anwendungsserver oder die direkte Verbindung verwenden.

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 zu 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 Jobserver 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 in der Modulliste **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.
   d. Klicken Sie **OK**.

   Für eine Verbindung zum Anwendungsserver:

   a. Wählen Sie in der Modulliste den Eintrag **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen**.
   b. Wählen Sie **AppServerJobProvider** und klicken Sie **OK**.
   c. Wählen Sie in der Modulliste **Prozessabholung > AppServerJobProvider**.
   d. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
   e. Erfassen Sie die Adresse (URL) zum Anwendungsserver und klicken Sie **OK**.
   f. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
   g. Wählen Sie unter **Authentifizierungsverfahren** das Authentifizierungsmodul für die Anmeldung. 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*.
   h. Klicken Sie **OK**.
7. Zur Konfiguration der Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.

- **Computer**: Wählen Sie den Server über die Auswahlliste oder erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.

  Um die Installation lokal auszuführen, wählen Sie in der Auswahlliste den Eintrag **<lokale Installation>**.
- **Dienstkonto**: Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen.

Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.

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

    Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.
12. 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.

Verwandte Themen

- Benötigte Informationen für Synchronisationsprojekte mit Azure Active Directory Mandanten auf Seite 29
- Initiales Synchronisationsprojekt für einen Azure Active Directory Mandanten erstellen auf Seite 31
- Synchronisationsprojekte für die Einladung von Gastbenutzern anpassen auf Seite 39

Benötigte Informationen für Synchronisationsprojekte mit Azure Active Directory Mandanten

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

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Anwendungs-ID	Die Anwendungs-ID wird beim Registrieren der One Identity Manager-Anwendung im Azure Active Directory Mandanten erzeugt.
Anmeldedomäne	Azure Active Directory Name der Domäne zur Anmeldung am Azure Active Directory. Sie können die Basisdomäne oder eine verifizierte Domäne Ihres Azure Active Directory Mandanten verwenden.
Benutzerkonto und Kennwort zur Anmeldung oder Wert des geheimen Schlüssels	Abhängig davon, wie die One Identity Manager-Anwendung im Azure Active Directory Mandanten registriert ist, wird entweder ein Benutzerkonto mit ausreichenden Berechtigungen oder der geheime Schlüssel benötigt. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit dem Azure Active Directory auf Seite 22.
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. Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem

Angaben	Erläuterungen
	Azure Active Directory Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. • Serverfunktion: **Azure Active Directory Konnektor (via Microsoft Graph)** • Maschinenrolle: **Server | Job Server | Azure Active Directory**
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Name der Datenbank • SQL Server-Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das 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. Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen. Konfiguration des Remoteverbindungsservers: • One Identity Manager Service ist gestartet • **RemoteConnectPlugin** ist installiert • Azure Active Directory Konnektor ist installiert Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt.

Angaben	Erläuterungen
	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 das **RemoteConnectPlugin** zusätzlich installieren. Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Registrieren einer Unternehmensanwendung für den One Identity Manager im Azure Active Directory Mandanten auf Seite 18
- Einrichten des Azure Active Directory Synchronisationsservers auf Seite 24

Initiales Synchronisationsprojekt für einen Azure Active Directory Mandanten erstellen

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.

HINWEIS: Pro Zielsystem und genutzter Standardprojektvorlage kann genau ein Synchronisationsprojekt erstellt werden.

Um ein initiales Synchronisationsprojekt für einen Azure Active Directory Mandanten einzurichten

1. Starten Sie das Launchpad und 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 Startseite des Projektassistenten klicken Sie **Weiter**.
4. 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.
5. Auf der Seite **Azure Active Directory Mandant** erfassen Sie folgende Informationen:
    - **Bereitstellung**: Wählen Sie Ihre Cloudbereitstellung. Zur Auswahl stehen **Microsoft Graph global service** und **Microsoft Graph for US Government (L4)** .
    - **Anwendungs-ID**: Erfassen Sie die Anwendungs-ID. Die Anwendungs-ID wurde beim Registrieren der One Identity Manager-Anwendung im Azure Active Directory Mandanten erzeugt.
    - **Anmeldedomäne**: Erfassen Sie die Basisdomäne oder eine verifizierte Domäne Ihres Azure Active Directory Mandanten.
6. Auf der Seite **Authentifizierung** wählen Sie die Art der Anmeldung und erfassen die benötigten Anmeldeinformationen. Die benötigten Informationen sind abhängig davon, wie die One Identity Manager-Anwendung im Azure Active Directory Mandanten registriert ist.
    - Wenn Sie den One Identity Manager als Mobilgerät- und Desktopanwendung in Ihrem Azure Active Directory Mandanten registriert haben, wählen Sie die Option **Authentifizierung als Mobilgerät- und Desktopanwendung** und erfassen Sie das Benutzerkonto und das Kennwort des Benutzerkontos zur Anmeldung.
    - Wenn Sie den One Identity Manager als Webanwendung in Ihrem Azure Active Directory Mandanten integriert haben, wählen Sie die Option **Authentifizierung als Webanwendung** und erfassen Sie den Wert des geheimen Schlüssels.

      Der geheime Schlüssel wurde bei der Registrierung der One Identity Manager-Anwendung des Azure Active Directory Mandanten erzeugt.
7. Auf der letzten Seite des Systemverbindungsassistenten können Sie die Verbindungsdaten speichern.
    - Aktivieren Sie die Option **Verbindung lokal speichern**, um die Verbindungsdaten zu speichern. Diese können Sie bei der Einrichtung weiterer Synchronisationsprojekte nutzen.
    - Um den Systemverbindungsassistenten zu beenden und zum Projektassistenten zurückzukehren, klicken Sie **Fertig**.

8. 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.

9. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
10. Auf der Seite **Projektvorlage auswählen** wählen Sie die Projektvorlage **Azure Active Directory Synchronisation**.
11. 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.	Gibt an, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager-Datenbank eingerichtet werden soll. Der Synchronisationsworkflow zeigt folgende Besonderheiten: • Die Synchronisationsrichtung ist **In den One Identity Manager**. • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung **In den One Identity Manager** definiert.
Es sollen auch Änderungen im Zielsystem durchgeführt werden.	Gibt an, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll. Der Provisionierungsworkflow zeigt folgende Besonderheiten: • Die Synchronisationsrichtung ist **In das Zielsystem**. • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die

Option	Bedeutung
	Synchronisationsrichtung **In das Zielsystem** definiert. • Synchronisationsschritte werden nur für solche Schemaklassen erstellt, deren Schematypen schreibbar sind.

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

    Wenn der Synchronisationsserver noch nicht als Jobserver für dieses Zielsystem 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.

    > TIPP: Sie können auch einen vorhandenen Jobserver zusätzlich als Synchronisationsserver für dieses Zielsystem einsetzen.
    >
    > • Um einen Jobserver auszuwählen, klicken Sie .
    >
    > Diesem Jobserver wird die passende Serverfunktion automatisch zugewiesen.

    c. Klicken Sie **OK**.

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

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

13. 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**.
    - 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.

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

Verwandte Themen

- Benutzer und Berechtigungen für die Synchronisation mit dem Azure Active Directory auf Seite 22
- Benötigte Informationen für Synchronisationsprojekte mit Azure Active Directory Mandanten auf Seite 29
- Registrieren einer Unternehmensanwendung für den One Identity Manager im Azure Active Directory Mandanten auf Seite 18
- Einrichten des Azure Active Directory Synchronisationsservers auf Seite 24
- Synchronisationsprotokoll konfigurieren auf Seite 35
- Anpassen der Synchronisationskonfiguration für Azure Active Directory-Umgebungen auf Seite 36
- Ausführen einer Synchronisation auf Seite 54
- Aufgaben nach einer Synchronisation auf Seite 58
- Mögliche Fehler bei der Synchronisation eines Azure Active Directory Mandanten auf Seite 284
- Projektvorlage für Azure Active Directory Mandanten auf Seite 290
- Projektvorlage für Azure Active Directory B2C Mandanten auf Seite 291
- Einstellungen des Azure Active Directory Konnektors auf Seite 295

Synchronisationsprotokoll konfigurieren

Im Synchronisationsprotokoll werden alle Informationen, Hinweise, Warnungen und Fehler, die bei der Synchronisation auftreten, aufgezeichnet. Welche Informationen aufgezeichnet werden sollen, kann für jede Systemverbindung und für jeden Synchronisationsworkflow separat konfiguriert werden.

Um den Inhalt des Synchronisationsprotokolls für eine Systemverbindung zu konfigurieren

1. Um das Synchronisationsprotokoll für die Zielsystemverbindung zu konfigurieren, wählen Sie im Synchronization Editor die Kategorie **Konfiguration > Zielsystem**.

   - ODER -

   Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie im Synchronization Editor die Kategorie **Konfiguration > One Identity Manager Verbindung**.

2. Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren**.
3. Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.
4. Aktivieren Sie die zu protokollierenden Daten.

   HINWEIS: Einige Inhalte erzeugen besonders viele Protokolldaten. Das Synchronisationsprotokoll soll nur die für Fehleranalysen und weitere Auswertungen notwendigen Daten enthalten.
5. Klicken Sie **OK**.

Um den Inhalt des Synchronisationsprotokolls für einen Synchronisationsworkflow zu konfigurieren

1. Wählen Sie im Synchronization Editor die Kategorie **Workflows**.
2. Wählen Sie in der Navigationsansicht einen Workflow.
3. Wählen Sie den Bereich **Allgemein** und klicken Sie **Bearbeiten**.
4. Wählen Sie den Tabreiter **Synchronisationsprotokoll**.
5. Aktivieren Sie die zu protokollierenden Daten.

   HINWEIS: Einige Inhalte erzeugen besonders viele Protokolldaten. Das Synchronisationsprotokoll soll nur die für Fehleranalysen und weitere Auswertungen notwendigen Daten enthalten.
6. Klicken Sie **OK**.

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.

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 56

Anpassen der Synchronisationskonfiguration für Azure Active Directory-Umgebungen

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 primäres System 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 Mandanten eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an den Mandanten 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.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.

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 38
- Synchronisation verschiedener Azure Active Directory Mandanten konfigurieren auf Seite 38
- Synchronisationsprojekte für die Einladung von Gastbenutzern anpassen auf Seite 39
- Unterstützung von kundenspezifischen Azure Active Directory Schemaerweiterungen auf Seite 40
- Einstellungen der Systemverbindung zum Azure Active Directory Mandanten ändern auf Seite 41
- Schema aktualisieren auf Seite 44
- Provisionierung von Mitgliedschaften konfigurieren auf Seite 50
- Einzelobjektsynchronisation konfigurieren auf Seite 51
- Beschleunigung der Provisionierung und Einzelobjektsynchronisation auf Seite 52

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 primäres System 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 im Synchronization Editor das Synchronisationsprojekt.
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 38

Synchronisation verschiedener Azure Active Directory Mandanten konfigurieren

Wenn Sie ein Synchronisationsprojekt für die Synchronisation eines weiteren Azure Active Directory Mandanten anpassen möchten, stellen Sie sicher, dass Sie beim Registrieren der Anwendung im Azure Active Directory Mandanten, die gleiche Art der Authentifizierung an der Anwendung verwenden.

Abhängig davon, wie die Anwendung für den One Identity Manager im Azure Active Directory Mandanten registriert ist, wird entweder ein Benutzerkonto mit ausreichenden Berechtigungen oder der geheime Schlüssel benötigt. Weitere

Informationen finden Sie unter Registrieren einer Unternehmensanwendung für den One Identity Manager im Azure Active Directory Mandanten auf Seite 18.

Um ein Synchronisationsprojekt für die Synchronisation eines weiteren Azure Active Directory Mandanten anzupassen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. 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.
    - Geben Sie die Verbindungsparameter bekannt. Die Verbindungsparameter werden in einem spezialisierten Variablenset gespeichert.

    Es wird eine Startkonfiguration erstellt, die das neu angelegte Variablenset verwendet.
3. Passen Sie bei Bedarf weitere Komponenten der Synchronisationskonfiguration an.
4. Speichern Sie die Änderungen.
5. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- Synchronisation in den Azure Active Directory Mandanten konfigurieren auf Seite 38
- Registrieren einer Unternehmensanwendung für den One Identity Manager im Azure Active Directory Mandanten auf Seite 18

Synchronisationsprojekte für die Einladung von Gastbenutzern anpassen

Ausführliche Informationen zu Gastbenutzern im Azure Active Directory finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

Im One Identity Manager können Sie Benutzerkonto mit folgenden Benutzertypen einrichten:

- **Mitglied**: Normales Azure Active Directory Benutzerkonto.
- **Gast**: Benutzerkonto für Gastbenutzer. Für Gastbenutzer erzeugt der Azure Active Directory Konnektor ein Benutzerkonto und sorgt dafür, dass eine Einladung an die eingetragene E-Mail-Adresse verschickt wird.

Um die Einladung für Gastbenutzer zu verschicken, sind zusätzlich Anpassungen der Variablen im Synchronisationsprojekt erforderlich.

Variable	Beschreibung
GuestInviteSendMail	Gibt an, ob eine Einladung für Gastbenutzer verschickt werden soll. Standard: **True**
GuestInviteLanguage	Sprache, in der die Einladung an Gastbenutzer verschickt werden soll. Standard: **en-us**
GuestInviteCustomMessage	Persönliche Willkommensnachricht an den Gastbenutzer.
GuestInviteRedirectUrl	URL zur Umleitung von Gastbenutzern, nachdem sie die Einladung angenommen und sich angemeldet haben. Standard: **http://www.office.com**

Um eine Variable zu bearbeiten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Variablen**.
3. Wählen Sie die Variable und bearbeiten Sie deren Wert.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212
- Verbindungsparameter im Variablenset bearbeiten auf Seite 42

Unterstützung von kundenspezifischen Azure Active Directory Schemaerweiterungen

Für Azure Active Directory Anwendungen, die im Unternehmen registriert werden, können Schemaerweiterungen im Azure Active Directory angelegt werden. Schemaerweiterungen im Azure Active Directory haben die Form `extension_<appId>_<propertyName>`. Ausführliche Informationen zu Schemaerweiterungen über die Microsoft Graph API finden Sie unter https://docs.microsoft.com/en-us/graph/extensibility-overview.

Der Azure Active Directory Konnektor kann die Azure Active Directory Schemaerweiterungen lesen und schreiben.

Um Azure Active Directory Schemaerweiterungen im One Identity Manager abzubilden und zu synchronisieren

1. Erweitern Sie das One Identity Manager Schema um die kundenspezifischen Spalten. Nutzen Sie dazu das Programm Schema Extension.

   Ausführliche Informationen zur Erweiterung des One Identity Manager Schemas finden Sie im *One Identity Manager Konfigurationshandbuch*.

2. Aktualisieren Sie mit dem Synchronization Editor in ihrem Synchronisationsprojekt das Schema des Zielsystems und das Schema der One Identity Manager Verbindung.

   Ausführliche Informationen zum Aktualisieren eines Schemas im Synchronization Editor finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

3. Erweitern Sie im Synchronization Editor in ihrem Synchronisationsprojekt die Mappings um entsprechende Property-Mapping-Regeln für die Schemaerweiterungen.

   Ausführliche Informationen zum Bearbeiten von Property-Mapping-Regeln im Synchronization Editor finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Einstellungen der Systemverbindung zum Azure Active Directory Mandanten ändern

Beim Einrichten der initialen Synchronisation werden für die Eigenschaften der Systemverbindung Standardwerte gesetzt. Diese Standardwerte können angepasst werden. Dafür gibt es zwei Wege:

a. Legen Sie ein spezialisiertes Variablenset an und ändern Sie die Werte der betroffenen Variablen.

   Die Standardwerte bleiben im Standardvariablenset erhalten. Die Variablen können jederzeit auf die Standardwerte zurückgesetzt werden. (Empfohlenes Vorgehen)

b. Bearbeiten Sie die Zielsystemverbindung mit dem Systemverbindungsassistenten und ändern Sie die betroffenen Werte.

   Der Systemverbindungsassistent liefert zusätzliche Erläuterungen zu den Einstellungen. Die Standardwerte können nur unter bestimmten Voraussetzungen wiederhergestellt werden.

Detaillierte Informationen zum Thema

- Verbindungsparameter im Variablenset bearbeiten auf Seite 42
- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 43
- Synchronisationsprojekte für die Einladung von Gastbenutzern anpassen auf Seite 39
- Einstellungen des Azure Active Directory Konnektors auf Seite 295

Verbindungsparameter im Variablenset bearbeiten

Die Verbindungsparameter wurden beim Einrichten der Synchronisation als Variablen im Standardvariablenset gespeichert. Sie können die Werte dieser Variablen in einem spezialisierten Variablenset Ihren Erfordernissen anpassen und dieses Variablenset einer Startkonfiguration und einem Basisobjekt zuordnen. Damit haben Sie jederzeit die Möglichkeit, erneut die Standardwerte aus dem Standardvariablenset zu nutzen.

HINWEIS: Um die Datenkonsistenz in den angebundenen Zielsystemen zu bewahren, stellen Sie sicher, dass die Startkonfiguration für die Synchronisation und das Basisobjekt für die Provisionierung dasselbe Variablenset verwenden. Das gilt insbesondere, wenn ein Synchronisationsprojekt für die Synchronisation verschiedener Azure Active Directory Mandanten genutzt wird.

Um die Verbindungsparameter in einem spezialisierten Variablenset anzupassen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
3. Öffnen Sie die Ansicht **Verbindungsparameter**.

   Einige Verbindungsparameter können hier in Variablen umgewandelt werden. Für andere sind bereits Variablen angelegt.
4. Wählen Sie einen Parameter und klicken Sie **Umwandeln**.
5. Wählen Sie die Kategorie **Konfiguration > Variablen**.

   Im unteren Bereich der Dokumentenansicht werden alle spezialisierten Variablensets angezeigt.
6. Wählen Sie ein spezialisiertes Variablenset oder klicken Sie in der Symbolleiste der Variablensetansicht .
   - Um das Variablenset umzubenennen, markieren Sie das Variablenset und klicken Sie in der Symbolleiste der Variablensetansicht . Erfassen Sie einen Namen für das Variablenset.
7. Wählen Sie die zuvor angelegten Variablen und erfassen Sie neue Werte.
8. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
9. Wählen Sie eine Startkonfiguration und klicken Sie **Bearbeiten**.
10. Wählen Sie den Tabreiter **Allgemein**.
11. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
12. Wählen Sie die Kategorie **Konfiguration > Basisobjekte**.
13. Wählen Sie ein Basisobjekt und klicken Sie .

    - ODER -

    Klicken Sie , um ein neues Basisobjekt anzulegen.

14. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
15. Speichern Sie die Änderungen.

Ausführliche Informationen zur Anwendung von Variablen und Variablensets, zum Wiederherstellen der Standardwerte und zum Anlegen von Basisobjekten finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 43

Eigenschaften der Zielsystemverbindung bearbeiten

Die Verbindungsparameter können auch mit dem Systemverbindungsassistenten geändert werden. Wenn für die Einstellungen Variablen definiert sind, werden die Änderungen in das aktive Variablenset übernommen.

HINWEIS: Unter folgenden Umständen können die Standardwerte nicht wiederhergestellt werden:

- Die Verbindungsparameter sind nicht als Variablen hinterlegt.
- Das Standardvariablenset ist als aktives Variablenset ausgewählt.

In beiden Fällen überschreibt der Systemverbindungsassistent die Standardwerte. Sie können später nicht wiederhergestellt werden.

Um die Verbindungsparameter mit dem Systemverbindungsassistenten zu bearbeiten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie in der Symbolleiste das aktive Variablenset, das für die Verbindung zum Zielsystem verwendet werden soll.

   HINWEIS: Ist das Standardvariablenset ausgewählt, werden die Standardwerte überschrieben und können später nicht wiederhergestellt werden.
3. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.
4. Klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
5. Folgen Sie den Anweisungen des Systemverbindungsassistenten und ändern Sie die gewünschten Eigenschaften.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Verbindungsparameter im Variablenset bearbeiten auf Seite 42

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 im Synchronization Editor das Synchronisationsprojekt.
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 im Synchronization Editor das Synchronisationsprojekt.
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.

Beschleunigung der Synchronisation

Zur Beschleunigung der Azure Active Directory Synchronisation unterstützt der Azure Active Directory Konnektor das Verfahren der Delta-Synchronisation. Das Verfahren beruht auf der Delta-Abfrage-Funktion von Microsoft Graph. Es werden die Schematypen **User** (Benutzerkonto), **Group** (Gruppe) und **DirectoryRole** (Administratorrolle) unterstützt. Die Delta-Synchronisation ist standardmäßig nicht aktiviert, sondern muss kundenspezifisch eingerichtet werden.

Inbetriebnahme der Delta-Synchronisation

1. Einrichtung eines regulären Azure Active Directory Synchronisationsprojektes.
2. Ausführen einer initialen Synchronisation.
3. Anpassen des Konfigurationsparameters **TargetSystem | AzureAD | DeltaTokenDirectory**.

   Der Konfigurationsparameter enthält das Verzeichnis, in dem die Delta-Token-Dateien abgelegt werden. Passen Sie im Designer den Wert des Konfigurationsparameter an. Stellen Sie sicher, dass das Benutzerkonto des One Identity Manager Service Schreibrechte auf das Verzeichnis hat.
4. (Optional) Anpassen des Prozesses `AAD_Organization_DeltaSync`.

   Der Prozess besteht aus drei Prozessschritten. Jeder Prozessschritt behandelt einen der drei unterstützten Schematypen. Jeder Prozessschritt ist so konfiguriert, dass alle unterstützten Delta-Eigenschaften des jeweiligen Schematyps synchronisiert werden. Des Weiteren legt jeder dieser Prozessschritte eine eigene Delta-Token-Datei an. Die Reihenfolge der Prozessschritte wurde wie folgt festgelegt:

   - Synchronisieren der Benutzerkonten (Prozessschritt `Synchronize User`)
   - Synchronisieren der Gruppen (Prozessschritt `Synchronize Group`)
   - Synchronisieren der Administratorrollen (Prozessschritt `Synchronize DirectoryRole`)

   Stellen Sie bei kundenspezifischen Anpassungen sicher, dass der Prozess nur generiert wird, wenn kein gleichartiger Prozess in der Jobqueue vorhanden ist. Ebenso darf der Prozess nicht während einer regulären Synchronisation starten.
5. (Optional) Anpassen der Verarbeitungsskripte für die unterstützten Schematypen.

- Verarbeiten der Benutzerkonten (Skript `AAD_ProcessDeltaQueryUser`)
- Verarbeiten der Gruppen (Skript `AAD_ProcessDeltaQueryGroup`)
- Verarbeiten der Administratorrollen (Skript `AAD_ProcessDeltaQueryDirectoryRole`)

Das Skript `AAD_ProcessDeltaQueryGroup` wurde mit umfangreichen Kommentaren versehen, um eine Bearbeitung und kundenspezifische Weiterentwicklung zu vereinfachen.

6. Anpassen und Aktivieren des Zeitplanes **Azure Active Directory Delta-Synchronisation**.

   Der Zeitplan sorgt für die regelmäßige Ausführung der Delta-Synchronisation der Azure Active Directory Mandanten. Der Zeitplan ist im Standard auf ein Ausführungsintervall von **15** Minuten eingestellt. Passen Sie im Designer das Ausführungsintervall bei Bedarf an. Aktivieren Sie den Zeitplan.

Ablauf der Delta-Synchronisation

1. Für einen Schematyp (Benutzerkonto, Gruppe, Administratorrolle) wird eine initiale Abfrage ausgeführt. Die initiale Abfrage liefert die komplette Liste für den Schematyp, beispielsweise alle Benutzerkonten, mit den abgefragten Eigenschaften. Des Weiteren wird ein Statustoken zurück geliefert. Das Statustoken stellt den Datenzustand zum Zeitpunkt der Abfrage im Azure Active Directory dar.

   Das Statustoken und die abgefragten Eigenschaften werden in eine Delta-Token-Datei geschrieben. Im Standard erfolgt keine initiale Verarbeitung der Daten.

   Ablagestruktur der Delta-Token-Datei:

   ```
   <Verzeichnis laut Konfigurationsparameter TargetSystem | AzureAD | DeltaTokenDirectory>\<UID_AADOrganization>_<SchemaTyp>Query.token
   ```

   Beispiel:

   ```
   C:\Temp\OneIM\DeltaToken\2da43fd4-ce7b-48af-9a00-686e5e3fb8a5_UserQuery.token
   ```

2. Die weiteren Abfragen werden mit dem Statustoken der vorherigen Abfrage ausgeführt. Sie liefern zusätzlich zum neuen Statustoken nur die Objekte, die sich seit der letzten Abfrage geändert haben.
   - Es wird versucht neue Objekte anzulegen, falls alle Pflichteigenschaften abgefragt wurden.
   - Objekte, die im Zielsystem gelöscht wurden, werden generell als **Ausstehend** markiert.

   Objekte, bei denen ein Verarbeitungsfehler aufgetreten ist, werden in den Meldungen des Prozessschritts protokolliert.

   Das neue Statustoken wird in die Delta-Token-Datei geschrieben.

Einschränkungen

Hinsichtlich der Wiederholfestigkeit hat das Verfahren der Differenzabfragen gewisse Einschränkungen. Wurde ein Statustoken einmal verwendet, ist es im Zweifel ungültig und die Abfrage kann nicht erneut ausgeführt werden. Tritt bei der Verarbeitung der

Rückgabedaten ein Fehler auf, kann die entsprechende Änderung erst im nächsten regulären Synchronisationslauf eingelesen werden. Dies trifft beispielsweise auf gemeldete neue Mitgliedschaften einer Gruppe zu, wenn das Mitglied selbst noch nicht eingelesen wurde.

Ein weiterer Nachteil ist die Laufzeit der Initialabfrage und der initialen Verarbeitung der Daten. Von dieser Verarbeitung wird dringend abgeraten. Da die initiale Verarbeitung innerhalb der regulären Synchronisation erfolgen sollte, wird empfohlen in den Prozessschritten den Parameter `DoNotProcessOffset` auf den Wert **True** zu setzen (Standard).

Ebenfalls ist zu berücksichtigen, dass nicht alle Eigenschaften mittels Microsoft Graph API Delta-Abfrage abgefragt werden können.

Passen die Daten der Delta-Token-Datei nicht zu den Aufrufparametern einer Abfrage, wird die vorhandene Datei in `<alterName>.backup` umbenannt, um den Statustoken nicht zu verlieren und eine neue Datei angelegt. In diesem Fall wird eine neue Initialabfrage ausgeführt. Dies geschieht auch, wenn die Datei nicht vorhanden oder leer ist.

Unterstützte Schematypen

Die folgenden Tabellen enthalten die unterstützten Schematypen mit den unterstützen Eigenschaften. Sofern neue Objekte in die Datenbank importiert werden sollen, müssen die Pflichteigenschaften in der Delta-Synchronisation mit angefragt werden.

Tabelle 6: Unterstützte Eigenschaften für Benutzerkonten (Schematyp: User)

Eigenschaft	Pflicht	Anmerkungen
AccountEnabled		
AgeGroup		
BusinessPhones		
City		
CompanyName		
ConsentProvidedForMinor		
Country		
Department		
DisplayName	X	
ExternalUserState		
ExternalUserStateChangeDateTime		
GivenName		
ID	X	
JobTitle		

Eigenschaft	Pflicht	Anmerkungen
LastPasswordChangeDateTime		
LegalAgeGroupClassification		
Licenses		Bei Abfrage dieser Eigenschaft wird eine zusätzliche Abfrage nach den Status der Zuweisung (`LicenseAssignmentStates`) des Benutzerkontos ausgeführt. Die Laufzeit erhöht sich dadurch stark. Enthält eine Liste von Objekten mit den Eigenschaften `DisabledPlans`, `SkuId`, `AssignedByGroup`, `State` und `Error`.
Mail		
MailNickname		
Manager		
MobilePhone		
OfficeLocation		
OnPremisesDistinguishedName		
OnPremisesDomainName		
OnPremisesImmutableId		
OnPremisesLastSyncDateTime		
OnPremisesSamAccountName		
OnPremisesSecurityIdentifier		
OnPremisesSyncEnabled		
OnPremisesUserPrincipalName		
PostalCode		
PreferredLanguage		
ProxyAddresses		
State		
StreetAddress		
Surname		
UsageLocation		

Eigenschaft	Pflicht	Anmerkungen
UserDomain	x	
UserPrincipalName	x	
UserType	x	

Tabelle 7: Unterstützte Eigenschaften für Gruppen (Schematyp: Group)

Eigenschaft	Pflicht	Anmerkungen
Description		
DisplayName	x	
GroupTypes	x	
ID	x	
Licenses		Enthält eine Liste von Objekten mit den Eigenschaften `DisabledPlans` und `SkuId`.
Mail		
MailEnabled	x	
MailNickName	x	
Members		Die Eigenschaft ist nicht in einer initialer Abfrage verfügbar. Das Ergebnis enthält den Schematyp und die ID.
OnPremisesSecurityIdentifier		
OnPremisesSyncEnabled		
Owners		Die Eigenschaft ist nicht in einer initialer Abfrage verfügbar. Das Ergebnis enthält den Schematyp und die ID.
ProxyAddresses		
SecurityEnabled	x	

Tabelle 8: Unterstützte Eigenschaften für Administratorrollen (Schematyp: DirectoryRole)

Eigenschaft	Pflicht	Anmerkungen
Description		
DisplayName	x	
ID	x	
Members		Die Eigenschaft ist nicht in einer initialer Abfrage verfügbar. Das Ergebnis enthält den Schematyp und die ID.

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.
5. Klicken Sie **Merge-Modus**.

   HINWEIS:

   - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` hat.
   - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden.

     Beispiel: `AADUserInGroup` und `AADGroupInGroup`
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. Dabei werden nur die neu eingefügten und gelöschten Zuordnungen verarbeitet. 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 Symbol gekennzeichnet:  . Die originale Bedingung kann jederzeit wiederhergestellt werden.

Um die originale Bedingung 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.

HINWEIS: Um in der Bedingung den Bezug zu den eingefügten oder gelöschten Zuordnungen herzustellen, nutzen Sie den Tabellenalias `i`.

Beispiel für eine Bedingung an der Zuordnungstabelle `AADUserInGroup`:

```
exists (select top 1 1 from AADGroup g
     where g.UID_AADGroup = i.UID_AADGroup
     and <einschränkende Bedingung>)
```

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

Einzelobjektsynchronisation konfigurieren

Änderungen an einem einzelnen Objekt im Zielsystem können sofort in die One Identity Manager-Datenbank übertragen werden, ohne dass eine vollständige Synchronisation der Zielsystem-Umgebung gestartet werden muss. Die Einzelobjektsynchronisation kann nur für Objekte ausgeführt werden, die in der One Identity Manager-Datenbank bereits vorhanden sind. Es werden die Änderungen an den gemappten Objekteigenschaften übernommen. Gehört zu diesen Objekteigenschaften eine Mitgliederliste, werden auch die Einträge in der Zuordnungstabelle aktualisiert. Ist das Objekt im Zielsystem nicht mehr vorhanden, wird es in der One Identity Manager-Datenbank gelöscht.

Voraussetzungen

- Es gibt einen Synchronisationsschritt, der die Änderungen am geänderten Objekt in den One Identity Manager einlesen kann.
- Für die Tabelle, die das geänderte Objekt enthält, ist der Pfad zum Basisobjekt der Synchronisation festgelegt.

Für Synchronisationsprojekte, die mit der Standard-Projektvorlage erstellt wurden, ist die Einzelobjektsynchronisation vollständig konfiguriert. Wenn Sie kundenspezifische Tabellen in solch ein Synchronisationsprojekt einbeziehen möchten, müssen Sie die Einzelobjektsynchronisation für diese Tabellen konfigurieren. Ausführliche Informationen dazu finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Um den Pfad zum Basisobjekt der Synchronisation für eine kundenspezifische Tabelle festzulegen

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 kundenspezifische Tabelle zu, für die Sie die Einzelobjektsynchronisation nutzen möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifische Tabelle und erfassen Sie den **Pfad zum Basisobjekt**.

   Geben Sie den Pfad zum Basisobjekt in der ObjectWalker-Notation der VI.DB an.

   Beispiel: `FK(UID_AADOrganization).XObjectKey`
8. Speichern Sie die Änderungen.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 57
- Ausstehende Objekte nachbehandeln auf Seite 58

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.
    - Für Jobserver, die an der Lastverteilung teilnehmen, muss die Option **Keine Prozesszuteilung** deaktiviert sein.
    - 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

- Jobserver für Azure Active Directory-spezifische Prozessverarbeitung auf Seite 277

Ausführen einer Synchronisation

Synchronisationen werden über zeitgesteuerte Prozessaufträge gestartet. Im Synchronization Editor ist es auch möglich, eine Synchronisation manuell zu starten. Zuvor können Sie die Synchronisation simulieren, um das Ergebnis der Synchronisation abzuschätzen und Fehler in der Synchronisationskonfiguration aufzudecken. Wenn eine Synchronisation irregulär abgebrochen wurde, müssen Sie die Startinformation zurücksetzen, um die Synchronisation erneut starten zu können.

Wenn verschiedene Zielsysteme immer in einer vorher festgelegten Reihenfolge synchronisiert werden sollen, nutzen Sie Startfolgen, um die Synchronisation zu starten. In einer Startfolge können beliebige Startkonfigurationen aus verschiedenen Synchronisationsprojekten zusammengestellt und in eine Ausführungsreihenfolge gebracht werden. Ausführliche Informationen zu Startfolgen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Synchronisationen starten auf Seite 54
- Synchronisation deaktivieren auf Seite 55
- Synchronisationsergebnisse anzeigen auf Seite 56
- Einzelobjekte synchronisieren auf Seite 57
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 63

Synchronisationen starten

Beim Einrichten des initialen Synchronisationsprojekts über das Launchpad werden Standardzeitpläne für regelmäßige Synchronisationen erstellt und zugeordnet. Um regelmäßige Synchronisationen auszuführen, aktivieren Sie diese Zeitpläne.

Um regelmäßige Synchronisationen auszuführen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
3. Wählen Sie in der Dokumentenansicht eine Startkonfiguration aus und klicken Sie **Zeitplan bearbeiten**.
4. Bearbeiten Sie die Eigenschaften des Zeitplans.
5. Um den Zeitplan zu aktivieren, klicken Sie **Aktiviert**.
6. Klicken Sie **OK**.

Wenn kein Zeitplan aktiviert ist, können Sie die Synchronisation auch manuell starten.

Um die initiale Synchronisation manuell zu starten

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > Startkonfigurationen**.
3. Wählen Sie in der Dokumentenansicht eine Startkonfiguration und klicken Sie **Ausführen**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

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.

Synchronisation deaktivieren

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

Um regelmäßige Synchronisationen zu verhindern

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
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 im Synchronization Editor das Synchronisationsprojekt.
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 28
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 63

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 im Synchronization Editor das Synchronisationsprojekt.
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 im Synchronization Editor das Synchronisationsprojekt.
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.

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 35
- Fehleranalyse auf Seite 62

Einzelobjekte synchronisieren

Die Einzelobjektsynchronisation kann nur für Objekte ausgeführt werden, die in der One Identity Manager-Datenbank bereits vorhanden sind. Es werden die Änderungen an den gemappten Objekteigenschaften übernommen. Gehört zu diesen Objekteigenschaften eine Mitgliederliste, werden auch die Einträge in der Zuordnungstabelle aktualisiert.

HINWEIS: Ist das Objekt im Zielsystem nicht mehr vorhanden, wird es in der One Identity Manager-Datenbank gelöscht.

Um ein Einzelobjekt zu synchronisieren

1. Wählen Sie im Manager die Kategorie **Azure Active Directory**.
2. Wählen Sie in der Navigationsansicht den Objekttyp.
3. Wählen Sie in der Ergebnisliste das Objekt, das Sie synchronisieren möchten.
4. Wählen Sie die Aufgabe **Objekt synchronisieren**.

   Es wird ein Prozess zum Lesen dieses Objekts in die Jobqueue eingestellt.

Besonderheiten bei der Synchronisation von Mitgliederlisten

Wenn Sie Änderungen in der Mitgliederliste eines Objekts synchronisieren, führen Sie die Einzelobjektsynchronisation am Basisobjekt der Zuweisung aus. Die Basistabelle einer Zuordnung enthält eine Spalte `XDateSubItem` mit der Information über die letzte Änderung der Mitgliedschaften.

Beispiel:

Basisobjekt für die Zuweisung von Benutzerkonten an Gruppen ist die Gruppe.

Im Zielsystem wurde ein Benutzerkonto an eine Gruppe zugewiesen. Um diese Zuweisung zu synchronisieren, wählen Sie im Manager die Gruppe, der das Benutzerkonto zugewiesen wurde, und führen Sie die Einzelobjektsynchronisation aus. Dabei werden alle Mitgliedschaften für diese Gruppe synchronisiert.

Das Benutzerkonto muss in der One Identity Manager-Datenbank bereits als Objekt vorhanden sein, damit die Zuweisung angelegt werden kann.

HINWEIS: Um die Änderung der Zuweisung von Abonnements an Benutzerkonten einzulesen, führen Sie die Einzelobjektsynchronisation am Benutzerkonto aus.

Detaillierte Informationen zum Thema

- Einzelobjektsynchronisation konfigurieren auf Seite 51

Aufgaben nach einer Synchronisation

Nach der Synchronisation von Daten aus dem Zielsystem in die One Identity Manager-Datenbank können Nacharbeiten erforderlich sein. Prüfen Sie folgende Aufgaben:

- Ausstehende Objekte nachbehandeln auf Seite 58
- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 60
- Azure Active Directory Benutzerkonten über Kontendefinitionen verwalten auf Seite 61

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

   1. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.
   2. 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 9: 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. Indirekte Mitgliedschaften können nicht gelöscht werden.

Symbol	Methode	Beschreibung
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Es wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: • Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen. • Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.
	Zurücksetzen	Die Markierung **Ausstehend** wird für das Objekt entfernt.

TIPP: Wenn eine Methode wegen bestimmter Einschränkungen nicht ausgeführt werden kann, ist das jeweilige Symbol deaktiviert.

- Um Details zur Einschränkung anzuzeigen, klicken Sie in der Spalte **Einschränkungen** die Schaltfläche **Anzeigen**.

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 das Symbol .

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.

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

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.

Verwandte Themen

- Ausstehende Objekte nachbehandeln auf Seite 58

Azure Active Directory Benutzerkonten über Kontendefinitionen verwalten

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Identitäten erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für den Mandanten bekannt, werden die Benutzerkonten mit den Identitäten 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

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 67

Fehleranalyse

Bei der Analyse und Behebung von Synchronisationsfehlern unterstützt Sie der Synchronization Editor auf verschiedene Weise.

- Synchronisation simulieren

  Die Simulation ermöglicht es, das Ergebnis einer Synchronisation abzuschätzen. Dadurch können beispielsweise Fehler in der Synchronisationskonfiguration aufgedeckt werden.

- Synchronisation analysieren

  Für die Analyse von Problemen während der Synchronisation, beispielsweise unzureichender Performance, kann der Synchronisationsanalysebericht erzeugt werden.

- Meldungen protokollieren

  Der One Identity Manager bietet verschiedene Möglichkeiten zur Protokollierung von Meldungen. Dazu gehören das Synchronisationsprotokoll, die Protokolldatei des One Identity Manager Service, die Protokollierung von Meldungen mittels NLog und weitere.

- Startinformation zurücksetzen

  Wenn eine Synchronisation irregulär abgebrochen wurde, beispielsweise weil ein Server nicht erreichbar war, muss die Startinformation manuell zurückgesetzt werden. Erst danach kann die Synchronisation erneut gestartet werden.

Ausführliche Informationen zu diesen Themen finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 56

Datenfehler bei der Synchronisation ignorieren

Standardmäßig werden Objekte mit fehlerhaften Daten nicht synchronisiert. Diese Objekte können synchronisiert werden, sobald die fehlerhaften Daten korrigiert wurden. In einzelnen Situationen kann es notwendig sein, solche Objekte dennoch zu synchronisieren und nur die fehlerhaften Objekteigenschaften zu ignorieren. Dieses Verhalten kann für die Synchronisation in den One Identity Manager konfiguriert werden.

Um Datenfehler bei der Synchronisation in den One Identity Manager zu ignorieren

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Konfiguration > One Identity Manager Verbindung**.
3. In der Ansicht **Allgemein** klicken Sie **Verbindung bearbeiten**.

   Der Systemverbindungsassistent wird gestartet.
4. Auf der Seite **Weitere Einstellungen** aktivieren Sie **Versuche Datenfehler zu ignorieren**.

   Diese Option ist nur wirksam, wenn am Synchronisationsworkflow **Bei Fehler fortsetzen** eingestellt ist.

   Fehler in Standardspalten, wie Primärschlüssel oder UID-Spalten, und Pflichteingabespalten können nicht ignoriert werden.
5. Speichern Sie die Änderungen.

WICHTIG: Wenn die Option aktiviert ist, versucht der One Identity Manager Speicherfehler zu ignorieren, die auf Datenfehler in einer einzelnen Spalte zurückgeführt werden können. Dabei wird die Datenänderung an der betroffenen Spalte verworfen und das Objekt anschließend neu gespeichert. Das beeinträchtigt die Performance und führt zu Datenverlust.

Aktivieren Sie die Option nur im Ausnahmefall, wenn eine Korrektur der fehlerhaften Daten vor der Synchronisation nicht möglich ist.

Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus)

Wenn ein Zielsystemkonnektor das Zielsystem zeitweilig nicht erreichen kann, können Sie den Offline-Modus für dieses Zielsystem aktivieren. Damit können Sie verhindern, dass zielsystemspezifische Prozesse in der Jobqueue eingefroren werden und später manuell reaktiviert werden müssen.

Ob der Offline-Modus für eine Zielsystemverbindung grundsätzlich verfügbar ist, wird am Basisobjekt des jeweiligen Synchronisationsprojekts festgelegt. Sobald ein Zielsystem

tatsächlich nicht erreichbar ist, kann diese Zielsystemverbindungen über das Launchpad offline und anschließend wieder online geschaltet werden.

Im Offline-Modus werden alle dem Basisobjekt zugewiesenen Jobserver angehalten. Dazu gehören der Synchronisationsserver und alle an der Lastverteilung beteiligten Jobserver. Falls einer der Jobserver auch andere Aufgaben übernimmt, dann werden diese ebenfalls nicht verarbeitet.

Voraussetzungen

Der Offline-Modus kann nur unter bestimmten Voraussetzungen für ein Basisobjekt zugelassen werden.

- Der Synchronisationsserver wird für kein anderes Basisobjekt als Synchronisationsserver genutzt.
- Wenn dem Basisobjekt eine Serverfunktion zugewiesen ist, darf keiner der Jobserver mit dieser Serverfunktion eine andere Serverfunktion (beispielsweise Aktualisierungsserver) haben.
- Es muss ein dedizierter Synchronisationsserver eingerichtet sein, der ausschließlich die Jobqueue für dieses Basisobjekt verarbeitet. Gleiches gilt für alle Jobserver, die über die Serverfunktion ermittelt werden.

Um den Offline-Modus für ein Basisobjekt zuzulassen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Basisobjekte**.
3. Wählen Sie in der Dokumentenansicht das Basisobjekt und klicken Sie .
4. Aktivieren Sie **Offline-Modus verfügbar**.
5. Klicken Sie **OK**.
6. Speichern Sie die Änderungen.

WICHTIG: Um Dateninkonsistenzen zu vermeiden, sollten Offline-Phasen kurz gehalten werden.

Die Zahl der nachträglich zu verarbeitenden Prozesse ist abhängig vom Umfang der Änderungen in der One Identity Manager-Datenbank mit Auswirkungen auf das Zielsystem während der Offline-Phase. Um Datenkonsistenz zwischen One Identity Manager-Datenbank und Zielsystem herzustellen, müssen alle anstehenden Prozesse verarbeitet werden, bevor eine Synchronisation gestartet wird.

Nutzen Sie den Offline-Modus möglichst nur, um kurzzeitige Systemausfälle, beispielsweise Wartungsfenster, zu überbrücken.

Um ein Zielsystem als offline zu kennzeichnen

1. Starten Sie das Launchpad und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie **Verwalten > Systemüberwachung > Zielsysteme als offline kennzeichnen**.

3. Klicken Sie **Starten**.

   Der Dialog **Offline-Systeme verwalten** wird geöffnet. Im Bereich **Basisobjekte** werden die Basisobjekte aller Zielsystemverbindungen angezeigt, für die der Offline-Modus zugelassen ist.
4. Wählen Sie das Basisobjekt, dessen Zielsystemverbindung nicht verfügbar ist.
5. Klicken Sie **Offline schalten**.
6. Bestätigen Sie die Sicherheitsabfrage mit **OK**.

   Damit werden die dem Basisobjekt zugewiesenen Jobserver angehalten. Es werden keine Synchronisations- und Provisionierungsaufträge ausgeführt. In Job Queue Info wird angezeigt, wenn ein Jobserver offline geschaltet wurde und die entsprechenden Aufträge nicht verarbeitet werden.

Ausführliche Informationen zum Offline-Modus finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Verwandte Themen

- Synchronisation deaktivieren auf Seite 55

Managen von Azure Active Directory Benutzerkonten und Identitäten

Zentraler Bestandteil des One Identity Manager ist die Abbildung von Identitäten 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 Identitäten verbunden werden. Für jede Identität 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 Identitäten 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 Identität mit den benötigten Benutzerkonten an. Der One Identity Manager unterstützt die folgenden Vorgehensweisen, um Identitäten und ihre Benutzerkonten zu verknüpfen:

- Identitäten erhalten ihre Benutzerkonten automatisch über Kontendefinitionen.

  Hat eine Identität noch kein Benutzerkonto in einem Azure Active Directory Mandanten, wird durch die Zuweisung der Kontendefinition an eine Identität 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 Identitäten festlegen.
- Beim Einfügen eines Benutzerkontos wird automatisch eine vorhandene Identität zugeordnet oder im Bedarfsfall eine neue Identität erstellt. Dabei werden die Identitätenstammdaten 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 Identitätenzuordnung definieren Sie Kriterien, anhand derer die Identitäten ermittelt werden sollen.

- Identitäten und Benutzerkonten können manuell erfasst und einander zugeordnet werden.

Ausführliche Informationen zu den Grundlagen zur Behandlung und Administration von Identitäten und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 67
- Automatische Zuordnung von Identitäten zu Azure Active Directory Benutzerkonten auf Seite 92
- Unterstützte Typen von Benutzerkonten auf Seite 98
- Aktualisieren von Identitäten bei Änderung von Azure Active Directory Benutzerkonten auf Seite 105
- Löschverzögerung für Azure Active Directory Benutzerkonten festlegen auf Seite 106
- Azure Active Directory Benutzerkonten erstellen und bearbeiten auf Seite 210

Kontendefinitionen für Azure Active Directory Benutzerkonten

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

Aus den Identitätenstammdaten resultieren die Daten für das Benutzerkonto im jeweiligen Zielsystem. Die Identitäten müssen ein zentrales Benutzerkonto besitzen. Über die primäre Zuordnung der Identität 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 Identität 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.

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

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

Ausführliche Informationen zu den Grundlagen zu Kontendefinitionen, Automatisierungsgraden und zur Ermittlung der gültigen IT Betriebsdaten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- Erstellen von Kontendefinitionen
- Konfigurieren der Automatisierungsgrade
- Erstellen der Abbildungsvorschriften für die IT Betriebsdaten
- Erfassen der IT Betriebsdaten
- Zuweisen der Kontendefinitionen an Identitäten und Zielsysteme

Detaillierte Informationen zum Thema

Kontendefinitionen erstellen

Erstellen Sie eine oder mehrere Kontendefinitionen für das Zielsystem.

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten der Kontendefinition.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten einer Kontendefinition auf Seite 69
- Kontendefinitionen bearbeiten auf Seite 69
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 75

Kontendefinitionen bearbeiten

Sie können die Stammdaten der Kontendefinitionen bearbeiten.

Um eine Kontendefinition zu bearbeiten

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. Bearbeiten Sie die Stammdaten der Kontendefinition.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten einer Kontendefinition auf Seite 69
- Kontendefinitionen erstellen auf Seite 68
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 75

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 10: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet. Für Azure Active Directory Benutzerkonten wählen Sie **AADUser**.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte	Angabe der vorausgesetzten Kontendefinition. Definieren Sie

Eigenschaft	Beschreibung
Kontendefinition	Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch zugeordnet. Für einen Azure Active Directory Mandanten lassen Sie die Angabe leer. In Verbund-Umgebungen können Sie die Kontendefinition der Active Directory Domäne eintragen.
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 Identitäten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. 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	Gibt an, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Identitäten und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal 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 Identitäten	Gibt an, ob die Kontendefinition automatisch an alle internen Identitäten zugewiesen werden soll. Um die Kontendefinition automatisch an alle internen Identitäten zuzuweisen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Identitäten aktivieren**. Die Kontendefinition wird an jede Identität zugewiesen, die nicht als extern markiert ist. Sobald eine neue interne Identität erstellt wird, erhält diese Identität ebenfalls automatisch diese Kontendefinition.

Eigenschaft	Beschreibung
	Um die automatische Zuweisung der Kontendefinition von allen Identitäten zu entfernen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Identitäten deaktivieren**. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Identitäten zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) 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 Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) 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 Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei Sicherheitsgefährdung beibehalten	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) 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.

Eigenschaft	Beschreibung
Gruppen erbbar	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Identität erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität diese Gruppe nur, wenn die Option aktiviert ist.
Abonnements erbbar	Gibt an, ob das Benutzerkonto Azure Active Directory Abonnements über die Identität erben darf. Ist die Option aktiviert, werden Azure Active Directory Abonnements über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Azure Active Directory Abonnements zugewiesen haben, dann erbt das Benutzerkonto diese Azure Active Directory Abonnements. • Wenn eine Identität ein Azure Active Directory Abonnement im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität dieses Azure Active Directory Abonnement nur, wenn die Option aktiviert ist.
Administratorrollen erbbar	Gibt an, ob das Benutzerkonto Azure Active Directory Administratorrollen über die Identität erben darf. Ist die Option aktiviert, werden Administratorrollen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Administratorrollen zugewiesen haben, dann erbt das Benutzerkonto diese Administratorrollen. • Wenn eine Identität eine Administratorrolle im IT Shop bestellt hat und diese Bestellung genehmigt und

Eigenschaft	Beschreibung
	zugewiesen ist, dann erbt das Benutzerkonto der Identität diese Administratorrolle nur, wenn die Option aktiviert ist.
Unwirksame Dienstpläne erbbar	Gibt an, ob das Benutzerkonto unwirksame Azure Active Directory Dienstpläne über die Identität erben darf. Ist die Option aktiviert, werden unwirksame Dienstpläne über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung unwirksame Dienstpläne zugewiesen haben, dann erbt das Benutzerkonto diese unwirksamen Dienstpläne. • Wenn eine Identität einen unwirksamen Dienstplan im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität diesen unwirksamen Dienstplan nur, wenn die Option aktiviert ist.
Office 365 Gruppen erbbar	HINWEIS: Diese Eigenschaft ist nur verfügbar, wenn das Exchange Online Modul vorhanden ist. Gibt an, ob das Benutzerkonto Office 365 Gruppen über die verbundene Identität erben darf. Ist die Option aktiviert, werden Office 365 Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Office 365 Gruppen zugewiesen haben, dann erbt das Azure Active Directory Benutzerkonto diese Office 365 Gruppen. • Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Azure Active Directory Benutzerkonto der Identität diese Office 365 Gruppe nur, wenn die Option aktiviert ist. Ausführliche Informationen zu Office 365 Gruppen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*.

Automatisierungsgrade bearbeiten

One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- **Unmanaged**: Benutzerkonten mit dem Automatisierungsgrad **Unmanaged** erhalten eine Verbindung zur Identität, erben jedoch keine weiteren Eigenschaften. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Identität werden initial einige der Identitäteneigenschaften übernommen. Werden die Identitäteneigenschaften 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 Identität. Beim Erstellen eines neuen Benutzerkontos mit diesem Automatisierungsgrad und Zuordnen einer Identität werden initial die Identitäteneigenschaften übernommen. Werden die Identitäteneigenschaften 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 Identität 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 Identität deaktiviert, gelöscht oder als sicherheitsgefährdend eingestuft wird, können die Benutzerkonten der Identität gesperrt werden. Wird die Identität 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 Identität gesperrt sind und somit auch nicht in Gruppen Mitglied sein dürfen. Während dieser Zeit sollen keine Vererbungsvorgänge für diese Identitäten berechnet werden. Bestehende Gruppenmitgliedschaften werden dann gelöscht!

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

4. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten eines Automatisierungsgrades auf Seite 76
- Automatisierungsgrade erstellen auf Seite 75
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 75

Automatisierungsgrade erstellen

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade **Unmanaged** und **Full managed**. Abhängig von Ihren Anforderungen können Sie weitere Automatisierungsgrade definieren.

WICHTIG: Erweitern Sie im Designer die Bildungsregeln um die Vorgehensweise für die zusätzlichen Automatisierungsgrade. Ausführliche Informationen zu Bildungsregeln finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um einen Automatisierungsgrad zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten des Automatisierungsgrades.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten eines Automatisierungsgrades auf Seite 76
- Kontendefinitionen bearbeiten auf Seite 69
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 75

Automatisierungsgrade an Kontendefinitionen zuweisen

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

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.

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

   Um eine Zuweisung zu entfernen

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

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 11: Stammdaten eines Automatisierungsgrades

Eigenschaft	Beschreibung
Automatisierungsgrad	Bezeichnung des Automatisierungsgrades.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Betriebsdaten überschreibend	Gibt an, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: • **Niemals**: Die Daten werden nicht aktualisiert. (Standard) • **Immer**: Die Daten werden immer aktualisiert. • **Nur initial**: Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Identitäten ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Identitäten gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Identitäten ihre Gruppenmitgliedschaften behalten sollen.

Eigenschaft	Beschreibung
Benutzerkonten bei dauerhafter Deaktivierung sperren	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Identitäten gesperrt werden sollen.
Gruppen bei verzögertem Löschen beibehalten	Gibt an, ob die Benutzerkonten zum Löschen markierter Identitäten ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren	Gibt an, ob die Benutzerkonten zum Löschen markierter Identitäten gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Identitäten ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Identitäten gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Gibt an, 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 Identität 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 Identität im Zielsystem verwendet.

- Gruppen erbbar
- Administratorrollen erbbar
- Abonnements erbbar
- Unwirksame Dienstpläne erbbar
- Kennwort bei der nächsten Anmeldung ändern
- Identität
- Privilegiertes Benutzerkonto

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.**
4. Klicken Sie **Hinzufügen** und erfassen Sie folgende Informationen.
    - **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*.
    - **Quelle**: Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen:
        - Primäre Abteilung
        - Primärer Standort
        - Primäre Kostenstelle
        - Primäre Geschäftsrolle

          HINWEIS: Die Geschäftsrolle kann nur verwendet werden, wenn das Geschäftsrollenmodul vorhanden ist.
        - keine Angabe

          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 Identität, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
    - **Immer Standardwert verwenden**: Gibt an, 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**: Gibt an, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Identität - Erstellung neues Benutzerkontos mit Standardwerten** verwendet.

      Um die Mailvorlage zu ändern, passen Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | Accounts | MailTemplateDefaultValues** an.

      Um die Mailvorlage zu ändern, passen Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | ExchangeOnline | Accounts | MailTemplateDefaultValues** an.
5. Speichern Sie die Änderungen.

Verwandte Themen

- IT Betriebsdaten erfassen auf Seite 79

IT Betriebsdaten erfassen

Um für eine Identität 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 Identität wird 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 Identität der Abteilung A ein Standardbenutzerkonto im Mandanten A. Zusätzlich erhalten einige Identitäten 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.

- **Wirksam für**: Legen Sie den Anwendungsbereich der IT Betriebsdaten fest. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.

  Um den Anwendungsbereich festzulegen

  a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.

  b. Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder, für eine Kontendefinition, die Tabelle `TSBAccountDef`.

  c. Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition.

  d. Klicken Sie **OK**.

- **Spalte**: Wählen Sie die 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*.

- **Wert**: Erfassen Sie den konkreten Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 77

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 Identität zu einer primären Abteilung, Kostenstelle, zu einer primären 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. Es bedeuten:

   - **Alter Wert**: Wert der Objekteigenschaft vor der Änderung der IT Betriebsdaten.
   - **Neuer Wert**: Wert der Objekteigenschaft nach der Änderung der IT Betriebsdaten.
   - **Auswahl**: Gibt an, ob der neue Wert 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 Kontendefinitionen an Identitäten

Kontendefinitionen werden an die Identitäten des Unternehmens zugewiesen.

Das Standardverfahren für die Zuweisung von Kontendefinitionen an Identitäten ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Identitäten 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 Identitäten zugewiesen werden.

Kontendefinitionen können automatisch an alle Identitäten 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 Identitäten zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

In den Prozessen der One Identity Manager Standardinstallation wird zunächst überprüft, ob die Identität 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.

HINWEIS: Solange eine Kontendefinition für eine Identität wirksam ist, behält die Identität ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht. Benutzerkonten, die als **Ausstehend** markiert sind, werden nur gelöscht, wenn der Konfigurationsparameter **QER | Person | User | DeleteOptions | DeleteOutstanding** aktiviert ist.

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Identitäten

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

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

   - ODER -

   Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
   - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
   - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
3. Speichern Sie die Änderungen.

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

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 83
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 83
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 84

- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 85
- Kontendefinitionen an Systemrollen zuweisen auf Seite 86
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 87

Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Kontendefinition an Abteilungen, Kostenstellen oder Standorte zu, damit die Kontendefinitionen über diese Organisationen an Identitäten zugewiesen werden.

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

- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 83
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 84
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 85
- Kontendefinitionen an Systemrollen zuweisen auf Seite 86
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 87

Kontendefinitionen an Geschäftsrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

Weisen Sie die Kontendefinition an Geschäftsrollen zu, damit die Kontendefinitionen über diese Geschäftsrollen an Identitäten zugewiesen werden.

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. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie 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

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 83
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 84
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 85
- Kontendefinitionen an Systemrollen zuweisen auf Seite 86
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 87

Kontendefinitionen an alle Identitäten zuweisen

Über diese Aufgaben wird die Kontendefinition an alle internen Identitäten zugewiesen. Identitäten, die als externe Identitäten gekennzeichnet sind, erhalten die Kontendefinition nicht. Sobald eine neue interne Identität erstellt wird, erhält diese Identität ebenfalls automatisch diese Kontendefinition. Die Zuweisung wird durch den DBQueue Prozessor berechnet.

WICHTIG: Führen Sie die Aufgabe nur aus, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Identitäten sowie alle zukünftig neu hinzuzufügenden internen Identitäten ein Benutzerkonto in diesem Zielsystem erhalten sollen!

Um eine Kontendefinition an alle Identitäten 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. Wählen Sie die Aufgabe **Automatische Zuweisung zu Identitäten aktivieren**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Speichern Sie die Änderungen.

HINWEIS: Um die automatische Zuweisung der Kontendefinition von allen Identitäten zu entfernen, führen Sie die Aufgabe **Automatische Zuweisung zu Identitäten deaktivieren** aus. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Identitäten zugewiesen. Bestehende Zuweisungen bleiben jedoch erhalten.

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 83
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 83
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 85
- Kontendefinitionen an Systemrollen zuweisen auf Seite 86
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 87

Kontendefinitionen direkt an Identitäten zuweisen

Kontendefinitionen können direkt oder indirekt an Identitäten zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung des Identitäten und der Kontendefinitionen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Kontendefinitionen auch direkt an die Identitäten zuweisen.

Um eine Kontendefinition direkt an Identitäten 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 Identitäten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 83
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 83
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 84
- Kontendefinitionen an Systemrollen zuweisen auf Seite 86
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 87

Kontendefinitionen an Systemrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Systemrollenmodul vorhanden ist.

Mit dieser Aufgabe nehmen Sie eine Kontendefinition in Systemrollen auf.

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

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 83
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 83
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 84
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 85
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 87

Kontendefinitionen 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 Identitäten 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 (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
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 in den IT Shop aufzunehmen (bei nicht-rollenbasierter Anmeldung)

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 **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 (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
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 einzelnen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

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 **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 (bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
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.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

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 **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 69
- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 83
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 83
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 84
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 85
- Kontendefinitionen an Systemrollen zuweisen auf Seite 86

Kontendefinitionen an Azure Active Directory Mandanten zuweisen

Wenn Sie die automatische Zuordnung von Benutzerkonten und Identitäten 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 Identität 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 Azure Active Directory 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 Identitäten zu Azure Active Directory Benutzerkonten auf Seite 92

Kontendefinitionen löschen

Sie können Kontendefinitionen löschen, wenn diese keinem Zielsystem, keiner Identität, 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 Identitäten.
    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. Wählen Sie die Aufgabe **Automatische Zuweisung zu Identitäten deaktivieren**.
    e. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
    f. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Identitäten.
    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 Identitäten zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Identitäten.
    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**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
    e. 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 Web Designer Web Portal Anwenderhandbuch*.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei rollenbasierter Anmeldung)

a. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
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.

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen (bei nicht-rollenbasierter Anmeldung)

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 **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 Azure Active Directory 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.

Automatische Zuordnung von Identitäten zu Azure Active Directory Benutzerkonten

Beim Einfügen eines Benutzerkontos kann automatisch eine vorhandene Identität zugeordnet werden. Im Bedarfsfall kann eine Identität neu erstellt werden. Dabei werden die Identitätenstammdaten anhand vorhandener Benutzerstammdaten erzeugt. Dieser Mechanismus kann auf die Erstellung eines neuen Benutzerkontos durch manuelle Anlage oder Synchronisation folgen.

Für die automatische Identitätenzuordnung definieren Sie Kriterien für die Ermittlung der Identitäten. Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Identität 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 Identitäten 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 Identitäten zu Benutzerkonten bleiben bestehen.

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

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

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

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

  Beispiel:

  `ADMINISTRATOR|GUEST`

  TIPP: Den Wert des Konfigurationsparameters können Sie über den Dialog **Ausschlussliste für die automatische Identitätenzuordnung** bearbeiten.

  Um die Ausschlussliste für die automatische Identitätenzuordnung zu bearbeiten

  1. Bearbeiten Sie im Designer den Konfigurationsparameter **PersonExcludeList**.
  2. Klicken Sie **...** hinter dem Eingabefeld **Wert**.

     Der Dialog **Ausschlussliste für Azure Active Directory Benutzerkonten** wird geöffnet.
  3. Um einen neuen Eintrag einzufügen, klicken Sie **Neu**.

     Um einen Eintrag zu bearbeiten, wählen Sie den Eintrag und klicken Sie **Bearbeiten**.
  4. Erfassen Sie die Bezeichnung des Benutzerkontos, dem Identitäten nicht automatisch zugeordnet werden sollen.

     Jeder Eintrag in der Liste wird als Teil eines regulären Ausdrucks behandelt. Metazeichen für reguläre Ausdrücke können verwendet werden.
  5. Um einen Eintrag zu löschen, wählen Sie den Eintrag und klicken Sie **Löschen**.
  6. Klicken Sie **OK**.
- Legen Sie über den Konfigurationsparameter **TargetSystem | AzureAD | PersonAutoDisabledAccounts** fest, ob an deaktivierte Benutzerkonten automatisch Identitäten 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 Identitätenzuordnung am Mandanten.

HINWEIS:

Für die Synchronisation gilt:

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

Außerhalb der Synchronisation gilt:

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

HINWEIS:

Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Identitäten erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für den Mandanten bekannt, werden die Benutzerkonten mit den Identitäten 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.

Weitere Informationen finden Sie unter Azure Active Directory Benutzerkonten über Kontendefinitionen verwalten auf Seite 61.

Verwandte Themen

- Kontendefinitionen erstellen auf Seite 68
- Kontendefinitionen an Azure Active Directory Mandanten zuweisen auf Seite 89
- Automatisierungsgrade für Azure Active Directory Benutzerkonten ändern auf Seite 97
- Suchkriterien für die automatische Identitätenzuordnung bearbeiten auf Seite 94
- Identitäten suchen und direkt an Benutzerkonten zuordnen auf Seite 95

Suchkriterien für die automatische Identitätenzuordnung bearbeiten

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

Die Kriterien für die Identitätenzuordnung werden am Mandanten definiert. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Identität übereinstimmen müssen, damit die Identität 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 Identitätenzuordnung** (`AccountToPersonMatchingRule`) der Tabelle `AADOrganization` geschrieben.

Die Suchkriterien werden bei der automatischen Zuordnung von Identitäten zu Benutzerkonten ausgewertet. Darüber hinaus können Sie anhand der Suchkriterien eine

Vorschlagsliste für die Identitätenzuordnung an Benutzerkonten erzeugen und die Zuordnung direkt ausführen.

HINWEIS: Die Objektdefinitionen für Benutzerkonten, auf welche die Suchkriterien angewendet werden können, sind vordefiniert. Sollten Sie weitere Objektdefinitionen benötigen, um beispielsweise die Vorauswahl der Benutzerkonten weiter einzuschränken, erzeugen Sie im Designer die entsprechenden kundenspezifische Objektdefinitionen. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um Kriterien für die Identitätenzuordnung festzulegen

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

   Tabelle 12: Standardsuchkriterien für Benutzerkonten und Kontakte

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

5. Speichern Sie die Änderungen.

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

Verwandte Themen

- Automatische Zuordnung von Identitäten zu Azure Active Directory Benutzerkonten auf Seite 92
- Identitäten suchen und direkt an Benutzerkonten zuordnen auf Seite 95

Identitäten suchen und direkt an Benutzerkonten zuordnen

Anhand der Suchkriterien können Sie eine Vorschlagsliste für die Zuordnung von Identitäten an Benutzerkonten erzeugen und die Zuordnung direkt ausführen. Die Benutzerkonten sind dafür in verschiedenen Ansichten zusammengestellt.

- **Vorgeschlagene Zuordnungen**: Die Ansicht listet alle Benutzerkonten auf, denen der One Identity Manager eine Identität zuordnen kann. Dazu werden die Identitäten angezeigt, die durch die Suchkriterien ermittelt und zugeordnet werden können.
- **Zugeordnete Benutzerkonten**: Die Ansicht listet alle Benutzerkonten auf, denen eine Identität zugeordnet ist.
- **Ohne Identitätenzuordnung**: Die Ansicht listet alle Benutzerkonten auf, denen keine Identität zugeordnet ist und für die über die Suchkriterien keine passende Identität ermittelt werden kann.

HINWEIS: Um deaktivierte Benutzerkonten oder deaktivierte Identitäten in den Ansichten anzuzeigen, aktivieren Sie die Option **Auch gesperrte Benutzerkonten werden verbunden**.

Wenn Sie eine deaktivierte Identität an ein Benutzerkonto zuordnen, wird das Benutzerkonto, abhängig von der Konfiguration, unter Umständen gesperrt oder gelöscht.

Um Suchkriterien auf die Benutzerkonten anzuwenden

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten**.
2. Wählen Sie in der Ergebnisliste den Mandanten.
3. Wählen Sie die Aufgabe **Suchkriterien für die Identitätenzuordnung definieren**.
4. Im unteren Bereich des Formulars klicken Sie **Neu laden**.

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

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

Durch die Zuordnung von Identitäten an die Benutzerkonten entstehen verbundene Benutzerkonten (Zustand **Linked**). Um verwaltete Benutzerkonten zu erhalten (Zustand **Linked configured**), können Sie gleichzeitig eine Kontendefinition zuordnen.

Um Identitäten direkt an Benutzerkonten zuzuordnen

- Klicken Sie **Vorgeschlagene Zuordnungen**.
  1. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Identität zugeordnet werden soll. Eine Mehrfachauswahl ist möglich.
  2. (Optional) Wählen Sie im Auswahlfeld **Diese Kontendefinition zuweisen** eine Kontendefinition und im Auswahlfeld **Diesen Automatisierungsgrad zuweisen** einen Automatisierungsgrad.
  3. Klicken Sie **Ausgewählte zuweisen.**
  4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

     Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Identitäten zugeordnet. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

  - ODER -

- Klicken Sie **Ohne Identitätenzuordnung**.
    1. Klicken Sie **Identität auswählen** für das Benutzerkonto, dem eine Identität zugeordnet werden soll. Wählen Sie eine Identität aus der Auswahlliste.
    2. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Identitäten zugeordnet werden sollen. Eine Mehrfachauswahl ist möglich.
    3. (Optional) Wählen Sie im Auswahlfeld **Diese Kontendefinition zuweisen** eine Kontendefinition und im Auswahlfeld **Diesen Automatisierungsgrad zuweisen** einen Automatisierungsgrad.
    4. Klicken Sie **Ausgewählte zuweisen**.
    5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

       Den ausgewählten Benutzerkonten werden die Identitäten zugeordnet, die in der Spalte **Identität** angezeigt werden. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

Um Zuordnungen zu entfernen

- Klicken Sie **Zugeordnete Benutzerkonten**.
    1. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Zuordnungen zu Identitäten entfernt werden soll. Mehrfachauswahl ist möglich.
    2. Klicken Sie **Ausgewählte entfernen**.
    3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

       Von den ausgewählten Benutzerkonten werden die zugeordneten Identitäten entfernt.

Automatisierungsgrade für Azure Active Directory Benutzerkonten ändern

Wenn Sie Benutzerkonten über die automatische Identitätenzuordnung 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

- Azure Active Directory Benutzerkonten erstellen und bearbeiten auf Seite 210

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.

- Identitätstyp

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

  Tabelle 13: Identitätstypen von Benutzerkonten

Identitätstyp	Beschreibung	Wert der Spalte IdentityType
Primäre Identität	Standardbenutzerkonto einer Identität.	Primary
Organisatorische Identität	Sekundäres Benutzerkonto, welches für unterschiedliche Rollen im Unternehmen verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.	Organizational
Persönliche Administratoridentität	Benutzerkonto mit administrativen Berechtigungen, welches von einer Identität genutzt wird.	Admin
Zusatzidentität	Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken.	Sponsored
Gruppenidentität	Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Identitäten genutzt wird.	Shared
Dienstidentität	Dienstkonto.	Service

- Privilegiertes Benutzerkonto

  Privilegierte Benutzerkonten werden eingesetzt, um Identitäten 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 99
- Administrative Benutzerkonten auf Seite 100
- Administrative Benutzerkonten für eine Identität bereitstellen auf Seite 101
- Administrative Benutzerkonten für mehrere Identitäten bereitstellen auf Seite 102
- Privilegierte Benutzerkonten auf Seite 103

Standardbenutzerkonten

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

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

   - Verwenden Sie in den Abbildungsvorschriften für die Spalten `IsGroupAccount_Group`, `IsGroupAccount_SubSku`, `IsGroupAccount_DeniedService` und `IsGroupAccount_DirectoryRole` 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 Identitäten zu.

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

Verwandte Themen

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 67

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 Identität bereitstellen auf Seite 101
- Administrative Benutzerkonten für mehrere Identitäten bereitstellen auf Seite 102

Administrative Benutzerkonten für eine Identität bereitstellen

Mit dieser Aufgabe erstellen Sie ein administratives Benutzerkonto, das von einer Identität genutzt werden kann.

Voraussetzungen

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

Um ein administratives Benutzerkonto für eine Identität 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 Identität, 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 **Identität** die Identität, die dieses administrative Benutzerkonto nutzt.

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

Verwandte Themen

- Administrative Benutzerkonten für mehrere Identitäten bereitstellen auf Seite 102
- Ausführliche Informationen zur Abbildung von Identitätstypen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administrative Benutzerkonten für mehrere Identitäten bereitstellen

Mit dieser Aufgabe erstellen Sie ein administratives Benutzerkonto, das von mehreren Identitäten genutzt werden kann.

Voraussetzung

- Das Benutzerkonto muss als Gruppenidentität gekennzeichnet sein.
- Es muss eine Identität mit dem Typ **Gruppenidentität** vorhanden sein. Die Gruppenidentität muss einen Manager haben.
- Die Identitäten, die das Benutzerkonto nutzen dürfen, müssen als primäre Identitäten gekennzeichnet sein.

Um ein administratives Benutzerkonto für mehrere Identitäten 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 Identität.
    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** eine Identität mit dem Typ **Gruppenidentität**.

    TIPP: Als Zielsystemverantwortlicher können Sie über die Schaltfläche eine neue Gruppenidentität erstellen.
3. Weisen Sie dem Benutzerkonto die Identitäten 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 **Identitäten mit Nutzungsberechtigungen zuzuweisen**.
    d. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Identität und doppelklicken Sie ✓.

Verwandte Themen

- Administrative Benutzerkonten für eine Identität bereitstellen auf Seite 101
- Ausführliche Informationen zur Abbildung von Identitätstypen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Privilegierte Benutzerkonten

Privilegierte Benutzerkonten werden eingesetzt, um Identitäten 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 Identität 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 Identität 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 Abbildungsvorschriften für die Spalten `IsGroupAccount_Group`, `IsGroupAccount_SubSku` und `IsGroupAccount_DeniedService` 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 Identitäten zu, die mit privilegierten Benutzerkonten arbeiten sollen.

   Durch die Zuweisung der Kontendefinition an eine Identität 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. Passen Sie bei Bedarf den Zeitplan im Designer an.

Verwandte Themen

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 67

Aktualisieren von Identitäten bei Änderung von Azure Active Directory Benutzerkonten

Im One Identity Manager werden Änderungen der Identitäteneigenschaften an die verbundenen Benutzerkonten weitergereicht und anschließend in das Zielsystem provisioniert. Unter Umständen kann es notwendig sein, Änderungen von Benutzerkonten im Zielsystem auf die Identitäteneigenschaften im One Identity Manager weiterzureichen.

Beispiel:

Während des Testbetriebs werden die Benutzerkonten aus dem Zielsystem in den One Identity Manager nur eingelesen und Identitäten erzeugt. Die Verwaltung der Benutzerkonten (Erstellen, Ändern und Löschen) über den One Identity Manager soll erst zu einem späteren Zeitpunkt in Betrieb genommen werden. Während des Testbetriebs werden die Benutzerkonten weiterhin im Zielsystem geändert, was zu Abweichungen der Benutzerkonteneigenschaften und Identitäteneigenschaften führen kann. Aus diesem Grund sollen vorübergehend die durch eine erneute Synchronisation eingelesenen Änderungen von Benutzerkonten an die bereits erzeugten Identitäten publiziert werden. Damit führt die Inbetriebnahme der Benutzerkontenverwaltung über den One Identity Manager nicht zu Datenverlusten.

Um Identitäten bei Änderungen von Benutzerkonten zu aktualisieren

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | AzureAD | PersonUpdate**.

Während der Synchronisation werden die Änderungen der Benutzerkonten in den One Identity Manager eingelesen. Durch anschließende Skript- und Prozessverarbeitung werden diese Änderungen an die verbundenen Identitäten weitergereicht.

HINWEIS:

- Die Aktualisierung der Identitäten bei Änderungen von Benutzerkonten erfolgt nur für Benutzerkonten, die den Automatisierungsgrad **Unmanaged** besitzen und mit einer Identität verbunden sind.
- Es wird nur die Identität aktualisiert, die aus dem geänderten Benutzerkonto erzeugt wurde. Die Datenquelle, aus der eine Identität erzeugt wurde, wird über die Eigenschaft **Datenquelle Import** der Identität angezeigt. Sind der Identität weitere Benutzerkonten zugeordnet, dann führen Änderungen dieser Benutzerkonten nicht zur Aktualisierung der Identität.
- Bei Identitäten, bei denen die Eigenschaft **Datenquelle Import** noch nicht gesetzt ist, wird während der ersten Aktualisierung des verbundenen Benutzerkontos das

Zielsystem des Benutzerkontos als Datenquelle für den Import eingetragen.

Das Mapping von Benutzerkontoeigenschaften auf Identitäteneigenschaften erfolgt über das Skript `AAD_PersonUpdate_AADUser`. Um das Mapping einfacher anzupassen, ist das Skript als überschreibbar definiert.

Für unternehmensspezifische Anpassungen, erzeugen Sie eine Kopie des Skriptes und beginnen Sie den Skriptcode folgendermaßen:

```
Public Overrides Function AAD_PersonUpdate_AADUser (ByVal UID_Account As String,
oldUserPrincipalName As String, ProcID As String)
```

Damit wird das Skript neu definiert und überschreibt das originale Skript. Eine Anpassung der Prozesse ist in diesem Fall nicht erforderlich.

Löschverzögerung für Azure Active Directory Benutzerkonten festlegen

Über die Löschverzögerung legen Sie fest, wie lange die Benutzerkonten nach dem Auslösen des Löschens in der Datenbank verbleiben, bevor sie endgültig entfernt werden. Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Die Benutzerkonten werden zunächst deaktiviert oder gesperrt. 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.

Sie haben die folgenden Möglichkeiten die Löschverzögerung zu konfigurieren.

- Globale Löschverzögerung: Die Löschverzögerung gilt für die Benutzerkonten in allen Zielsystemen. Der Standardwert ist **30** Tage.

  Erfassen Sie eine abweichende Löschverzögerung im Designer für die Tabelle `AADUser` in der Eigenschaft **Löschverzögerungen [Tage]**.
- Objektspezifische Löschverzögerung: Die Löschverzögerung kann abhängig von bestimmten Eigenschaften der Benutzerkonten konfiguriert werden.

  Um eine objektspezifische Löschverzögerung zu nutzen, erstellen Sie im Designer für die Tabelle `AADUser` ein **Skript (Löschverzögerung)**.

  Beispiel:

  Die Löschverzögerung für privilegierte Benutzerkonten soll 10 Tage betragen. An der Tabelle wird folgendes **Skript (Löschverzögerung)** eingetragen.

```
If $IsPrivilegedAccount:Bool$ Then
     Value = 10
End If
```

Ausführliche Informationen zum Bearbeiten der Tabellendefinitionen und zum Konfigurieren der Löschverzögerung im Designer finden Sie im *One Identity Manager Konfigurationshandbuch*.

Managen von Mitgliedschaften in Azure Active Directory Gruppen

Azure Active Directory Benutzerkonten können in Azure Active Directory Gruppen zusammengefasst werden, mit denen der Zugriff auf Ressourcen geregelt werden kann.

Im One Identity Manager können Sie die Azure Active Directory Gruppen direkt an die Benutzerkonten zuweisen oder über Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen vererben. Des Weiteren können Benutzer die Gruppen über das Web Portal bestellen. Dazu werden die Gruppen im IT Shop bereitgestellt.

HINWEIS: Zuweisungen zu Azure Active Directory Gruppen, die mit dem lokalen Active Directory synchronisiert werden, sind im One Identity Manager nicht erlaubt. Diese Gruppen können nicht über das Web Portal bestellt werden. Sie können diese Gruppen nur in Ihrer lokalen Umgebung verwalten. Ausführliche Informationen finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

Detaillierte Informationen zum Thema

Zuweisen von Azure Active Directory Gruppen an Azure Active Directory Benutzerkonten

Azure Active Directory Gruppen können indirekt oder direkt an Azure Active Directory Benutzerkonten zugewiesen werden.

Bei der indirekten Zuweisung werden Identitäten und Azure Active Directory Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Azure Active Directory Gruppen berechnet, die einer Identität zugewiesen sind. Wenn Sie eine Identität in Rollen aufnehmen und die Identität ein Azure Active Directory Benutzerkonto besitzt, dann wird dieses Azure Active Directory Benutzerkonto in die Azure Active Directory Gruppen aufgenommen.

Des Weiteren können Azure Active Directory Gruppen im Web Portal bestellt werden. Dazu werden Identitäten als Kunden in einen Shop aufgenommen. Alle Azure Active Directory Gruppen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Azure Active Directory Gruppen werden nach erfolgreicher Genehmigung den Identitäten zugewiesen.

Über Systemrollen können Azure Active Directory Gruppen zusammengefasst und als Paket an Identitäten und Arbeitsplätze zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich Azure Active Directory Gruppen enthalten. Ebenso können Sie in einer Systemrolle beliebige Unternehmensressourcen zusammenfassen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Azure Active Directory Gruppen auch direkt an Azure Active Directory Benutzerkonten zuweisen.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

Thema	Handbuch
Grundlagen zur Zuweisung von Unternehmensressourcen und zur Vererbung von Unternehmensressourcen	*One Identity Manager Administrationshandbuch für das Identity Management Basismodul* *One Identity Manager Administrationshandbuch für Geschäftsrollen*
Zuweisung von Unternehmensressourcen über IT Shop-Bestellungen	*One Identity Manager Administrationshandbuch für IT Shop*
Systemrollen	*One Identity Manager Administrationshandbuch für Systemrollen*

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Gruppen an Azure Active Directory Benutzerkonten auf Seite 110
- Azure Active Directory Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Azure Active Directory Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Azure Active Directory Gruppen in Systemrollen aufnehmen auf Seite 114
- Azure Active Directory Gruppen in den IT Shop aufnehmen auf Seite 115
- Azure Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 117

- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Gruppen zuweisen auf Seite 119
- Azure Active Directory Gruppen direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 119

Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Gruppen an Azure Active Directory Benutzerkonten

Bei der indirekten Zuweisung werden Identitäten und Azure Active Directory Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet. Für die indirekte Zuweisung von Azure Active Directory Gruppen prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Identitäten und Azure Active Directory Gruppen erlaubt.

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

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

   1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

      - ODER -

      Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
   2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
      - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
      - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
   3. Speichern Sie die Änderungen.
2. Einstellungen für die Zuweisung von Azure Active Directory Gruppen an Azure Active Directory Benutzerkonten.
   - Das Azure Active Directory Benutzerkonto ist mit einer Identität verbunden.
   - Am Azure Active Directory Benutzerkonto ist die Option **Gruppen erbbar** aktiviert.

HINWEIS: Bei der Vererbung von Unternehmensressourcen über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen spielen unter Umständen weitere Konfigurationseinstellungen eine Rolle. So kann beispielsweise die Vererbung für eine Rolle

blockiert sein oder die Vererbung an Identitäten nicht erlaubt sein. Ausführliche Informationen über die Grundlagen zur Zuweisung von Unternehmensressourcen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Azure Active Directory Benutzerkonten erstellen und bearbeiten auf Seite 210
- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212

Azure Active Directory Gruppen 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 nicht-rollenbasierter Anmeldung oder 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

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Gruppen an Azure Active Directory Benutzerkonten auf Seite 110
- Azure Active Directory Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Azure Active Directory Gruppen in Systemrollen aufnehmen auf Seite 114
- Azure Active Directory Gruppen in den IT Shop aufnehmen auf Seite 115
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Gruppen zuweisen auf Seite 119
- Azure Active Directory Gruppen direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 119
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 12

Azure Active Directory Gruppen an Geschäftsrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

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. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie 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 nicht-rollenbasierter Anmeldung oder 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

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Gruppen an Azure Active Directory Benutzerkonten auf Seite 110
- Azure Active Directory Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Azure Active Directory Gruppen in Systemrollen aufnehmen auf Seite 114
- Azure Active Directory Gruppen in den IT Shop aufnehmen auf Seite 115
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Gruppen zuweisen auf Seite 119
- Azure Active Directory Gruppen direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 119
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 12

Azure Active Directory Gruppen in Systemrollen aufnehmen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Systemrollenmodul vorhanden ist.

Mit dieser Aufgabe nehmen Sie eine Gruppe in Systemrollen auf.

Wenn Sie eine Systemrolle an Identitäten zuweisen, wird die Gruppe an alle Azure Active Directory Benutzerkonten vererbt, die diese Identitäten 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

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Gruppen an Azure Active Directory Benutzerkonten auf Seite 110
- Azure Active Directory Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Azure Active Directory Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Azure Active Directory Gruppen in den IT Shop aufnehmen auf Seite 115
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Gruppen zuweisen auf Seite 119
- Azure Active Directory Gruppen direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 119

Azure Active Directory Gruppen 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 Identitäten 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. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppe an die IT Shop Regale zu.
6. 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. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
6. 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 für Azure Active Directory Gruppen auf Seite 234
- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Gruppen an Azure Active Directory Benutzerkonten auf Seite 110
- Azure Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 117
- Azure Active Directory Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Azure Active Directory Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Azure Active Directory Gruppen in Systemrollen aufnehmen auf Seite 114
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Gruppen zuweisen auf Seite 119
- Azure Active Directory Gruppen direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 119

Azure Active Directory Gruppen automatisch in den IT Shop aufnehmen

Mit den folgenden Schritten können Azure Active Directory Gruppen automatisch in den IT Shop aufgenommen werden. Die Synchronisation sorgt dafür, dass die Azure Active Directory Gruppen in den IT Shop aufgenommen werden. Bei Bedarf können Sie die Synchronisation im Synchronization Editor sofort starten. Azure Active Directory Gruppen, die im One Identity Manager neu erstellt werden, werden ebenfalls automatisch in den IT Shop aufgenommen.

Um Azure Active Directory Gruppen automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | AADGroup**.
2. Um einzelne Azure Active Directory Gruppen nicht automatisch in den IT Shop aufzunehmen, aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | AADGroup | ExcludeList**.

   Der Konfigurationsparameter enthält eine Auflistung aller Azure Active Directory Gruppen, die nicht automatisch zum IT Shop zugeordnet werden sollen. Bei Bedarf können Sie die Liste erweitern. Erfassen Sie dazu im Wert des Konfigurationsparameters die Namen der Gruppen. Die Namen werden in einer Pipe (|) getrennten Liste angegeben. Reguläre Ausdrücke werden unterstützt.
3. Kompilieren Sie die Datenbank.

Die Azure Active Directory Gruppen werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

Folgende Schritte werden bei der Aufnahme einer Azure Active Directory Gruppe in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für die Azure Active Directory Gruppe ermittelt.

   Für jede Azure Active Directory Gruppe wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Bezeichnung der Azure Active Directory Gruppe.

   - Für Azure Active Directory Gruppen mit Leistungsposition wird die Leistungsposition angepasst.
   - Azure Active Directory Gruppen ohne Leitungsposition erhalten eine neue Leistungsposition.
2. Die Leistungsposition wird entweder der Standard-Servicekategorie **Azure Active Directory Gruppen | Sicherheitsgruppen** oder der Standard-Servicekategorie **Azure Active Directory Gruppen | Verteilergruppen** zugeordnet.
3. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet.

Die Produkteigner können Bestellungen von Mitgliedschaften in diesen Azure Active Directory Gruppen genehmigen. Standardmäßig wird der Eigentümer einer Azure Active Directory Gruppe als Produkteigner ermittelt.

HINWEIS: Die Anwendungsrolle für Produkteigner muss der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** untergeordnet sein.

- Ist der Eigentümer der Azure Active Directory Gruppe bereits Mitglied einer Anwendungsrolle für Produkteigner, dann wird diese Anwendungsrolle der Leistungsposition zugewiesen. Alle Mitglieder dieser Anwendungsrolle werden dadurch Produkteigner der Azure Active Directory Gruppe.
- Ist der Eigentümer der Azure Active Directory Gruppe noch kein Mitglied einer Anwendungsrolle für Produkteigner, dann wird eine neue Anwendungsrolle erzeugt. Die Bezeichnung der Anwendungsrolle entspricht der Bezeichnung des Eigentümers.
  - Handelt es sich beim Eigentümer um ein Benutzerkonto, wird die Identität des Benutzerkontos in die Anwendungsrolle aufgenommen.
  - Handelt es sich um eine Gruppe von Eigentümern, werden die Identitäten aller Benutzerkonten dieser Gruppe in die Anwendungsrolle aufgenommen.

4. Die Azure Active Directory Gruppe wird mit der Option **IT Shop** gekennzeichnet und dem IT Shop Regal **Azure Active Directory Gruppen** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Kunden des Shops Mitgliedschaften in Azure Active Directory Gruppen über das Web Portal bestellen.

HINWEIS: Wenn eine Azure Active Directory Gruppe endgültig aus der One Identity Manager-Datenbank gelöscht wird, wird auch die zugehörige Leistungsposition gelöscht.

Ausführliche Informationen zur Konfiguration des IT Shops finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*. Ausführliche Informationen zum Bestellen von Zugriffsanforderungen im Web Portal finden Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

Verwandte Themen

- Azure Active Directory Gruppen in den IT Shop aufnehmen auf Seite 115
- Azure Active Directory Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Azure Active Directory Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Azure Active Directory Gruppen in Systemrollen aufnehmen auf Seite 114
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Gruppen zuweisen auf Seite 119
- Azure Active Directory Gruppen in Azure Active Directory Gruppen aufnehmen auf Seite 237

Azure Active Directory Benutzerkonten direkt an Azure Active Directory Gruppen zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppen direkt an Benutzerkonten zuweisen. Gruppen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

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

Um Benutzerkonten 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 **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 Azure Active Directory Benutzerkonten zuweisen auf Seite 119
- Azure Active Directory Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Azure Active Directory Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Azure Active Directory Gruppen in Systemrollen aufnehmen auf Seite 114
- Azure Active Directory Gruppen in den IT Shop aufnehmen auf Seite 115

Azure Active Directory Gruppen direkt an Azure Active Directory Benutzerkonten zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppen direkt an Benutzerkonten zuweisen. Gruppen, die mit der Option **Verwendung nur im IT Shop**

gekennzeichnet sind, können nicht direkt zugewiesen werden.

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 Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Azure Active Directory Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Azure Active Directory Gruppen in Systemrollen aufnehmen auf Seite 114
- Azure Active Directory Gruppen in den IT Shop aufnehmen auf Seite 115
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Gruppen zuweisen auf Seite 119

Wirksamkeit von Gruppenmitgliedschaften

Bei der Zuweisung von Gruppen an Benutzerkonten kann es vorkommen, dass eine Identität 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: 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 Identität sowohl Bestellungen auslösen als auch Rechnungen zur Zahlung anweisen kann. Das heißt, die Gruppen A und B schließen sich aus. Eine Identität, die Rechnungen prüft, darf ebenfalls keine Rechnungen zur Zahlung anweisen. Das heißt, die Gruppen B und C schließen sich aus.

Tabelle 14: Festlegen der ausgeschlossenen Gruppen (Tabelle AADGroupExclusion)

Wirksame Gruppe	Ausgeschlossene Gruppe
Gruppe A	
Gruppe B	Gruppe A
Gruppe C	Gruppe B

Tabelle 15: Wirksame Zuweisungen

Identität	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 Identität ist berechtigt Bestellungen auszulösen und Rechnungen zu prüfen. Soll das verhindert werden, definieren Sie einen weiteren Ausschluss für die Gruppe C.

Tabelle 16: Ausgeschlossene Gruppen und wirksame Zuweisungen

Identität	Mitglied in Rolle	Zugewiesene Gruppe	Ausgeschlossene Gruppe	Wirksame Gruppe
Jenny Basset	Marketing	Gruppe A		Gruppe C
	Kontrollgruppe	Gruppe C	Gruppe B Gruppe A	

Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.

  Aktivieren Sie im Designer den Konfigurationsparameter und kompilieren Sie die Datenbank.

  HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

- 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 Gruppen, Administratorrollen, Abonnements und unwirksamen Dienstpläne an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 63**.

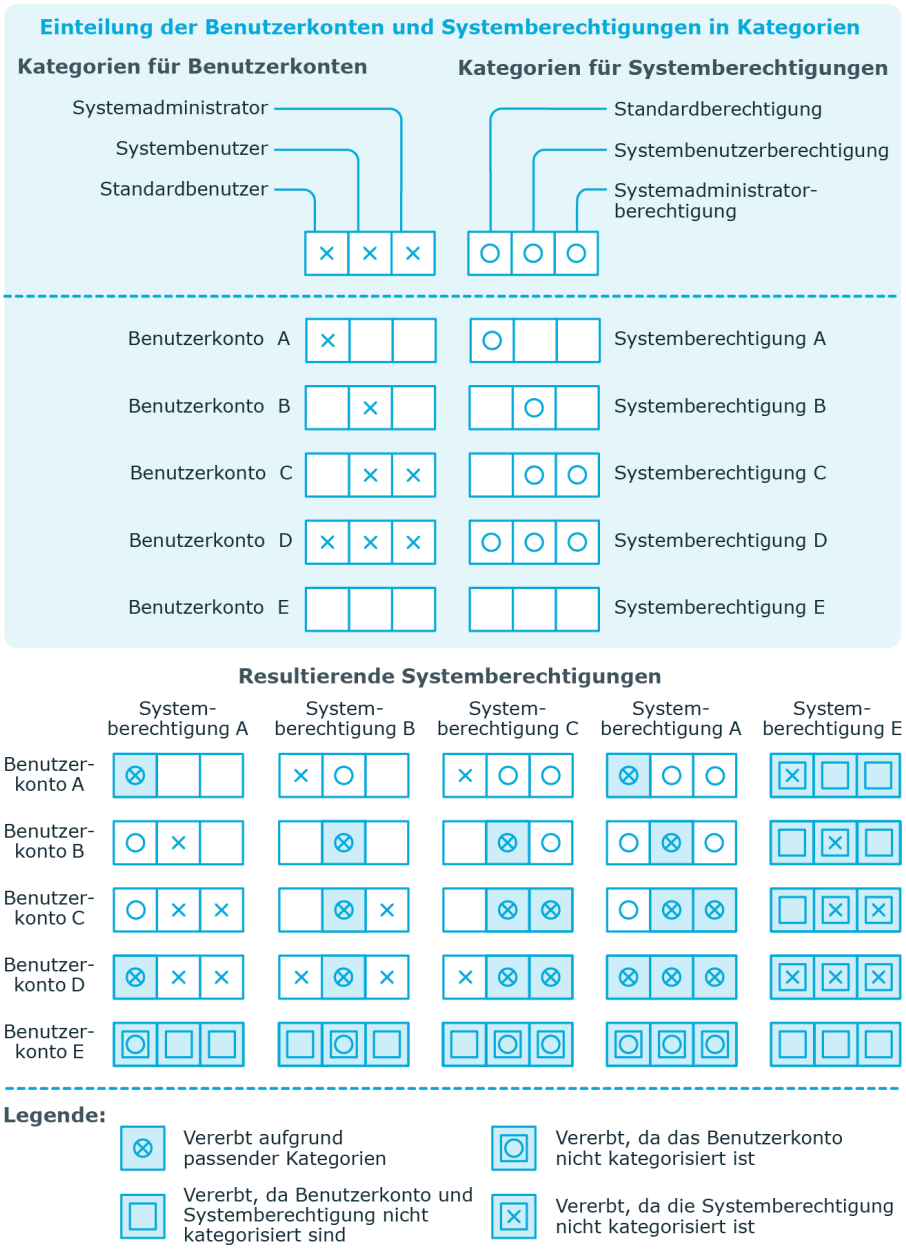
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist 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 17: 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

1. Definieren Sie im Manager am Azure Active Directory Mandanten die Kategorien.
2. Weisen Sie im Manager die Kategorien den Benutzerkonten über ihre Stammdaten zu.
3. Weisen Sie im Manager die Kategorien den Gruppen über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 203
- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212
- Allgemeine Stammdaten für Azure Active Directory Gruppen auf Seite 234
- Stammdaten von Azure Active Directory Abonnements bearbeiten auf Seite 248

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 Identitäten 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 Identitäten befinden, die diese Ressource besitzen.
- Wird der Bericht für eine Gruppe oder andere Systemberechtigung erstellt, werden alle Rollen ermittelt, in denen sich Identitäten befinden, die diese Gruppe oder Systemberechtigung besitzen.
- Wird der Bericht für eine Complianceregel erstellt, werden alle Rollen ermittelt, in denen sich Identitäten befinden, die diese Complianceregel verletzen.
- Wird der Bericht für eine Abteilung erstellt, werden alle Rollen ermittelt, in denen die Identitäten der gewählten Abteilung ebenfalls Mitglied sind.
- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Identitäten 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 Identitäten mit dem ausgewählten Basisobjekt befinden.

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Identitäten 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 Identitäten 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 Identitäten zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Identitäten werden der Geschäftsrolle zugeordnet.

Abbildung 3: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 18: 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.

5

Managen von Zuweisungen von Azure Active Directory Administratorrollen

Im One Identity Manager können Sie die Azure Active Directory Administratorrollen direkt an die Benutzerkonten zuweisen oder über Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen vererben. Des Weiteren können Benutzer die Administratorrollen über das Web Portal bestellen. Dazu werden die Administratorrollen im IT Shop bereitgestellt.

Detaillierte Informationen zum Thema

- Zuweisen von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten auf Seite 127
- Vererbung von Azure Active Directory Administratorrollen anhand von Kategorien auf Seite 136
- Übersicht aller Zuweisungen auf Seite 125

Zuweisen von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten

Azure Active Directory Administratorrollen können indirekt oder direkt an Azure Active Directory Benutzerkonten zugewiesen werden.

Bei der indirekten Zuweisung werden Identitäten und Azure Active Directory Administratorrollen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Azure Active Directory Administratorrollen berechnet, die einer Identität zugewiesen sind. Wenn Sie eine Identität in Rollen aufnehmen und die Identität ein Azure Active Directory Benutzerkonto besitzt, dann wird dieses

Azure Active Directory Benutzerkonto in die Azure Active Directory Administratorrollen aufgenommen.

Des Weiteren können Azure Active Directory Administratorrollen im Web Portal bestellt werden. Dazu werden Identitäten als Kunden in einen Shop aufgenommen. Alle Azure Active Directory Administratorrollen , die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Azure Active Directory Administratorrollen werden nach erfolgreicher Genehmigung den Identitäten zugewiesen.

Über Systemrollen können Azure Active Directory Administratorrollen zusammengefasst und als Paket an Identitäten zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich Azure Active Directory Administratorrollen enthalten. Ebenso können Sie in einer Systemrolle beliebige Unternehmensressourcen zusammenfassen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Azure Active Directory Administratorrollen auch direkt an Azure Active Directory Benutzerkonten zuweisen.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

Thema	Handbuch
Grundlagen zur Zuweisung von Unternehmensressourcen und zur Vererbung von Unternehmensressourcen	*One Identity Manager Administrationshandbuch für das Identity Management Basismodul* *One Identity Manager Administrationshandbuch für Geschäftsrollen*
Zuweisung von Unternehmensressourcen über IT Shop-Bestellungen	*One Identity Manager Administrationshandbuch für IT Shop*
Systemrollen	*One Identity Manager Administrationshandbuch für Systemrollen*

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten auf Seite 129
- Azure Active Directory Administratorrollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 130
- Azure Active Directory Administratorrollen an Geschäftsrollen zuweisen auf Seite 131
- Azure Active Directory Administratorrollen in Systemrollen aufnehmen auf Seite 132
- Azure Active Directory Administratorrollen in den IT Shop aufnehmen auf Seite 133
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Administratorrollen zuweisen auf Seite 135
- Azure Active Directory Administratorrollen direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 136

Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten

Bei der indirekten Zuweisung werden Identitäten und Azure Active Directory Administratorrollen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet. Für die indirekte Zuweisung von Azure Active Directory Administratorrollen prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Identitäten und Azure Active Directory Administratorrollen erlaubt.

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

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

   1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

      - ODER -

      Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
   2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
      - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
      - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
   3. Speichern Sie die Änderungen.
2. Einstellungen für die Zuweisung von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten.
   - Das Azure Active Directory Benutzerkonto ist mit einer Identität verbunden.
   - Am Azure Active Directory Benutzerkonto ist die Option **Administratorrollen erbbar** aktiviert.

HINWEIS: Bei der Vererbung von Unternehmensressourcen über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen spielen unter Umständen weitere Konfigurationseinstellungen eine Rolle. So kann beispielsweise die Vererbung für eine Rolle blockiert sein oder die Vererbung an Identitäten nicht erlaubt sein. Ausführliche Informationen über die Grundlagen zur Zuweisung von Unternehmensressourcen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Azure Active Directory Benutzerkonten erstellen und bearbeiten auf Seite 210
- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212

Azure Active Directory Administratorrollen 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 im Manager 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 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 Administratorrollen zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrollen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Administratorrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten auf Seite 129
- Azure Active Directory Administratorrollen an Geschäftsrollen zuweisen auf Seite 131
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Administratorrollen zuweisen auf Seite 135
- Azure Active Directory Administratorrollen in Systemrollen aufnehmen auf Seite 132
- Azure Active Directory Administratorrollen in den IT Shop aufnehmen auf Seite 133
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 12

Azure Active Directory Administratorrollen an Geschäftsrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

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 im Manager die Kategorie **Azure Active Directory > Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie 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 im Manager 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.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Administratorrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten auf Seite 129
- Azure Active Directory Administratorrollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 130
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Administratorrollen zuweisen auf Seite 135
- Azure Active Directory Administratorrollen in Systemrollen aufnehmen auf Seite 132
- Azure Active Directory Administratorrollen in den IT Shop aufnehmen auf Seite 133
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 12

Azure Active Directory Administratorrollen in Systemrollen aufnehmen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Systemrollenmodul vorhanden ist.

Mit dieser Aufgabe nehmen Sie eine Administratorrolle in Systemrollen auf. Wenn Sie eine Systemrolle an Identitäten zuweisen, wird die Administratorrolle an alle Azure Active Directory Benutzerkonten vererbt, die diese Identitäten 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 im Manager 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

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten auf Seite 129
- Azure Active Directory Administratorrollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 130
- Azure Active Directory Administratorrollen an Geschäftsrollen zuweisen auf Seite 131
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Administratorrollen zuweisen auf Seite 135
- Azure Active Directory Administratorrollen in den IT Shop aufnehmen auf Seite 133

Azure Active Directory Administratorrollen 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 Identitäten 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 im Manager die Kategorie **Azure Active Directory > Administratorrollen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager 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 im Manager die Kategorie **Azure Active Directory > Administratorrollen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager 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 im Manager die Kategorie **Azure Active Directory > Administratorrollen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager 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 242
- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten auf Seite 129
- Azure Active Directory Administratorrollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 130
- Azure Active Directory Administratorrollen an Geschäftsrollen zuweisen auf Seite 131
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Administratorrollen zuweisen auf Seite 135
- Azure Active Directory Administratorrollen in Systemrollen aufnehmen auf Seite 132

Azure Active Directory Benutzerkonten direkt an Azure Active Directory Administratorrollen zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Administratorrolle direkt an Benutzerkonten zuweisen. Administratorrollen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um eine Administratorrolle direkt an Benutzerkonten zuzuweisen

1. Wählen Sie im Manager 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 Azure Active Directory Benutzerkonten zuweisen auf Seite 136

- Azure Active Directory Administratorrollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 130
- Azure Active Directory Administratorrollen an Geschäftsrollen zuweisen auf Seite 131
- Azure Active Directory Administratorrollen in Systemrollen aufnehmen auf Seite 132
- Azure Active Directory Administratorrollen in den IT Shop aufnehmen auf Seite 133

Azure Active Directory Administratorrollen direkt an Azure Active Directory Benutzerkonten zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Administratorrollen direkt zuweisen. Administratorrollen, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um Administratorrollen 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 **Administratorrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Zuweisen von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten auf Seite 127

Vererbung von Azure Active Directory Administratorrollen anhand von Kategorien

Das unter Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 123 beschriebene Verhalten können Sie auch für Administratorrollen einsetzen.

Um die Vererbung über Kategorien zu nutzen

1. Definieren Sie im Manager am Azure Active Directory Mandanten die Kategorien.
2. Weisen Sie im Manager die Kategorien den Benutzerkonten über ihre Stammdaten zu.
3. Weisen Sie im Manager die Kategorien den Administratorrollen über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 203
- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212
- Stammdaten von Azure Active Directory Administratorrollen bearbeiten auf Seite 242

Managen von Zuweisungen von Azure Active Directory Abonnements und Azure Active Directory Dienstplänen

Um auf die Dienstpläne im Azure Active Directory zuzugreifen, benötigen die Benutzer ein Azure Active Directory Abonnement. Ein Azure Active Directory Abonnement definiert den Umfang der Dienstpläne, auf die ein Benutzer zugreifen darf. Die Nutzung einzelner Dienstpläne kann für Benutzer erlaubt oder nicht erlaubt werden.

Beispiel:

Das Azure Active Directory Abonnement A enthält den Dienstplan 1, den Dienstplan 2 und den Dienstplan 3.

- Das Abonnement A wird dem Benutzer zugewiesen.
- Der Dienstplan 2 wird für den Benutzer nicht erlaubt.

Damit kann der Benutzer die Dienstpläne 1 und 3 nutzen.

Azure Active Directory Abonnements können im Azure Active Directory an Benutzer und an Gruppen zugewiesen werden. Für die unterschiedlichen Zuweisungswege können Dienstpläne erlaubt oder nicht erlaubt werden. Der Benutzer erhält alle erlaubten Dienstpläne.

Beispiel:

Das Azure Active Directory Abonnement A enthält den Dienstplan 1, den Dienstplan 2 und den Dienstplan 3.

- Das Azure Active Directory Abonnement A wird dem Benutzer direkt zugewiesen.
- Der Dienstplan 2 wird für den Benutzer nicht erlaubt.

Das Azure Active Directory Abonnement B enthält den Dienstplan 4, den Dienstplan 5 und den Dienstplan 6.

- Das Azure Active Directory Abonnement B wird der Gruppe A zugewiesen.
- Der Dienstplan 6 wird für die Gruppe A nicht erlaubt.
- Der Benutzer ist in der Gruppe A.

Damit kann der Benutzer die Dienstpläne 1, 3, 4 und 5 nutzen.

Es ist möglich, dass ein Benutzer das gleiche Azure Active Directory Abonnement sowohl direkt als auch über eine oder mehrere Gruppen erhält. Ist ein Dienstplan über einen Zuweisungsweg erlaubt und über einen anderen Zuweisungsweg nicht erlaubt, dann erhält der Benutzer den Dienstplan.

Beispiel:

Das Azure Active Directory Abonnement A enthält den Dienstplan 1, den Dienstplan 2 und den Dienstplan 3.

- Das Azure Active Directory Abonnement A wird dem Benutzer direkt zugewiesen.
- Der Dienstplan 2 wird für den Benutzer nicht erlaubt.
- Das Azure Active Directory Abonnement A wird der Gruppe A zugewiesen.
- Alle Dienstpläne werden für die Gruppe A erlaubt.
- Der Benutzer ist in der Gruppe A.

Damit kann der Benutzer die Dienstpläne 1, 2 und 3 nutzen.

Im One Identity Manager werden die Azure Active Directory Abonnements und Dienstpläne und ihre Zuweisungen an Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen folgendermaßen abgebildet.

Tabelle 19: Abbildung der Azure Active Directory Abonnements und Dienstpläne im One Identity Manager Schema

Tabelle	Beschreibung
AADSubSku	Die Tabelle enthält alle Azure Active Directory Abonnements. Die Informationen zu Azure Active Directory Abonnements innerhalb eines Azure Active Directory Mandanten werden durch die Synchronisation in den One Identity Manager eingelesen. Neue Azure Active Directory Abonnements können Sie im One Identity Manager nicht erstellen.
AADServicePlan	Die Tabelle enthält die Dienstpläne. Die Informationen zu Dienstplänen innerhalb eines Azure Active Directory Mandanten werden durch die Synchronisation in den One Identity Manager eingelesen. Neue Dienstpläne können Sie im One Identity Manager nicht erstellen.
AADServicePlanInSubSku	Die Tabelle enthält die Zuweisungen von Dienstplänen zu Azure Active Directory Abonnements. Die Zuweisungen werden durch die Synchronisation in den One Identity Manager eingelesen. Die Zuweisungen können Sie im One Identity Manager nicht bearbeiten.
AADDeniedServicePlan	Die Tabelle enthält die Zuweisung der Dienstpläne zu Azure Active Directory Abonnements, um die nicht-erlaubten Dienstpläne abzubilden. Die Einträge werden nach der Synchronisation der Azure Active Directory Abonnements automatisch im One Identity Manager erzeugt. Nicht-erlaubte Dienstpläne werden im One Identity Manager als "unwirksame Dienstpläne" bezeichnet. Mit der Zuweisung eines unwirksamen Dienstplans an ein Azure Active Directory Benutzerkonto im One Identity Manager wird die Nutzung dieses Dienstplans im Azure Active Directory nicht erlaubt.
AADUserHasSubSku	Die Tabelle enthält die Zuweisungen der Azure Active Directory Abonnements zu den Azure Active Directory Benutzerkonten. Abgebildet werden die direkten Zuweisungen von Azure Active Directory Abonnements zu Azure Active Directory Benutzerkonten und die Zuweisungen, die ein Azure Active Directory Benutzerkonto über seine Azure Active Directory Gruppen erhält. Die Zuweisungen werden durch die Synchronisation eingelesen. Azure Active Directory Abonnements können Sie im

Tabelle	Beschreibung
	One Identity Manager an die Azure Active Directory Benutzerkonten zuweisen; entweder direkt, über IT Shop Bestellungen oder über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen. Die Zuweisungen über Azure Active Directory Gruppen können in One Identity Manager nicht bearbeitet werden. Die Azure Active Directory Gruppe, aus der eine Zuweisung resultiert, wird in der Spalte **Azure Active Directory Quellgruppe** (`AADUserHasSubSku.UID_AADGroupSource`) abgebildet. Ist die Spalte leer, handelt es sich um eine Zuweisung des Azure Active Directory Abonnements an das Azure Active Directory Benutzerkonto, die entweder direkt, über IT Shop Bestellungen oder über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen entstanden ist. Zuweisungen über Azure Active Directory Gruppen werden in der Spalte **Herkunft** mit dem Wert **Zuweisung durch Gruppe** (`AADUserHasSubSku.XOrigin=16`) gekennzeichnet. Die Tabelle enthält zusätzlich für jedes Azure Active Directory Benutzerkonto eine Liste der nicht erlaubten Dienstpläne seiner Azure Active Directory Abonnements (`AADUserHasSubSku.DenyList`).
AADUserHasDeniedService	Die Tabelle enthält die Zuweisungen der unwirksamen Dienstpläne zu den Azure Active Directory Benutzerkonten. Die Einträge werden aus der Liste der nicht erlaubten Dienstpläne (`AADUserHasSubSku.DenyList`) ermittelt. Unwirksame Dienstpläne können Sie im One Identity Manager an die Azure Active Directory Benutzerkonten zuweisen, entweder direkt, über IT Shop Bestellungen oder über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen. Mit der Zuweisung eines unwirksamen Dienstplans wird die Nutzung dieses Dienstplan im Azure Active Directory nicht erlaubt. HINWEIS: Ein unwirksamer Dienstplan, der an ein Benutzerkonto zugewiesen ist, kann effektiv erlaubt sein, wenn das Benutzerkonto diesen Dienstplan zusätzlich über eine Gruppe erhält und der Dienstplan für die Gruppe erlaubt ist. Die Zuweisung über Gruppen wird nicht in dieser Tabelle abgebildet.
AADUserHasServicePlan	Die Tabelle enthält die wirksamen Zuweisungen der

Tabelle	Beschreibung
	Dienstpläne für die Azure Active Directory Benutzerkonten. Die Zuweisungen werden im One Identity Manager berechnet aus den Einträgen aus den Tabellen `AADUserHasSubSku`, `AADUserHasDeniedService`, `AADGroupHasSubSku` und `AADGroupHasDeniedService`.
AADGroupHasSubSku	Die Tabelle enthält die Zuweisungen der Azure Active Directory Abonnements zu Azure Active Directory Gruppen. Die Tabelle enthält zusätzlich für jede Azure Active Directory Gruppe eine Liste der nicht erlaubten Dienstpläne ihrer Azure Active Directory Abonnements (`AADGroupHasSubSku.DenyList`). Die Zuweisungen werden durch die Synchronisation in den One Identity Manager eingelesen. Die Zuweisungen können Sie im One Identity Manager nicht bearbeiten.
AADGroupHasDeniedService	Die Tabelle enthält die Zuweisungen der unwirksamen Dienstpläne zu den Azure Active Directory Gruppen. Die Einträge werden aus der Liste der nicht erlaubten Dienstpläne (`AADGroupHasSubSku.DenyList`) berechnet. Die Zuweisungen können Sie im One Identity Manager nicht bearbeiten.

Detaillierte Informationen zum Thema

- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143
- Zuweisen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten auf Seite 145
- Vererbung von Azure Active Directory Abonnements anhand von Kategorien auf Seite 170
- Zuweisen von unwirksamen Azure Active Directory Dienstpläne an Azure Active Directory Benutzerkonten auf Seite 158
- Vererbung von unwirksamen Azure Active Directory Dienstplänen anhand von Kategorien auf Seite 171
- Übersicht aller Zuweisungen auf Seite 125

Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen

Ein Azure Active Directory Benutzerkonto kann Azure Active Directory Abonnements und Azure Active Directory Dienstpläne direkt oder über seine Azure Active Directory Gruppen erhalten.

HINWEIS: Es ist möglich, dass ein Azure Active Directory Benutzerkonto das gleiche Azure Active Directory Abonnement sowohl direkt als auch über eine oder mehrere Azure Active Directory Gruppen erhält. Ist ein Dienstplan über einen Zuweisungsweg erlaubt und über einen anderen Zuweisungsweg nicht erlaubt, dann erhält der Benutzer den Dienstplan.

Das bedeutet:

Ein unwirksamer Dienstplan, der an ein Benutzerkonto zugewiesen ist, kann effektiv erlaubt sein, wenn das Benutzerkonto diesen Dienstplan zusätzlich über eine Gruppe erhält und der Dienstplan für die Gruppe erlaubt ist.

Weitere Informationen finden Sie unter Managen von Zuweisungen von Azure Active Directory Abonnements und Azure Active Directory Dienstplänen auf Seite 138.

Um Informationen zu Azure Active Directory Abonnements und Dienstplänen für ein Benutzerkonto anzuzeigen

1. Wählen Sie im Manager 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**.

   Auf dem Überblicksformular werden folgende Informationen zu den Azure Active Directory Abonnements und Dienstplänen eines Benutzerkontos angezeigt.

   - **Azure Active Directory Abonnements (eigene)**: Azure Active Directory Abonnements, die dem Benutzerkonto zugewiesen sind; entweder direkt, über IT Shop Bestellungen oder über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen.
   - **Azure Active Directory Abonnements (geerbt)**: Azure Active Directory Abonnements, die das Benutzerkonto über seine Azure Active Directory Gruppen erhalten hat.

- **Wirksame Azure Active Directory Dienstpläne**: Azure Active Directory Dienstpläne, die für das Benutzerkonto erlaubt sind.
- **Unwirksame Azure Active Directory Dienstpläne aus eigenen Abonnements** : Unwirksame Azure Active Directory Dienstpläne, die dem Benutzerkonto zugewiesen sind; entweder direkt, über IT Shop Bestellungen oder über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen.

4. Wählen Sie den Bericht **Überblick über die Lizenz**.

   Der Bericht enthält eine Zusammenfassung der zugewiesenen und effektiv wirksamen Abonnements und Dienstpläne für ein Azure Active Directory Benutzerkonto.

Um Informationen zu Azure Active Directory Abonnements und Dienstplänen für eine Gruppe anzuzeigen

1. Wählen Sie im Manager 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**.

   Auf dem Überblicksformular werden folgende Informationen zu den Azure Active Directory Abonnements und Dienstplänen einer Gruppe angezeigt.

   - **Azure Active Directory Abonnements**: Azure Active Directory Abonnements, die der Azure Active Directory Gruppen zugewiesen sind.
   - **Wirksame Azure Active Directory Dienstpläne**: Azure Active Directory Dienstpläne, die für die Gruppe erlaubt sind.
   - **Unwirksame Azure Active Directory Dienstpläne**: Azure Active Directory Dienstpläne, die für die Gruppe nicht erlaubt sind.
   - **Azure Active Directory Benutzerkonten**: Azure Active Directory Benutzerkonten, die der Gruppe zugewiesen sind und somit die Abonnements und Dienstpläne erhalten.

Verwandte Themen

- Zuweisen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten auf Seite 145
- Zuweisen von unwirksamen Azure Active Directory Dienstpläne an Azure Active Directory Benutzerkonten auf Seite 158

Zuweisen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten

Azure Active Directory Abonnements können indirekt oder direkt an Azure Active Directory Benutzerkonten zugewiesen werden.

Bei der indirekten Zuweisung werden Identitäten und Azure Active Directory Abonnements in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Azure Active Directory Abonnements berechnet, die einer Identität zugewiesen sind. Besitzt die Identität ein Azure Active Directory Benutzerkonto, werden die Azure Active Directory Abonnements der Rollen an dieses Azure Active Directory Benutzerkonto vererbt.

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

TIPP: Damit eine Identität automatisiert ein Azure Active Directory Benutzerkonto und ein Azure Active Directory Abonnement erhält, können Sie die Kontendefinition zur Erstellung des Benutzerkontos und das zu verwendende Azure Active Directory Abonnement in einer Systemrolle zusammenfassen.

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

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Azure Active Directory Abonnements auch direkt an Azure Active Directory Benutzerkonten zuweisen.

HINWEIS: Ein Azure Active Directory Benutzerkonto kann Azure Active Directory Abonnements zusätzlich über seine Azure Active Directory Gruppen erhalten. Die Zuweisungen über Azure Active Directory Gruppen können in One Identity Manager nicht bearbeitet werden.

Die Tabelle `AADUserhasSubSku` enthält die Zuweisungen der Azure Active Directory Abonnements zu den Azure Active Directory Benutzerkonten mit ihrer Herkunft. Weitere Informationen finden Sie unter Managen von Zuweisungen von Azure Active Directory Abonnements und Azure Active Directory Dienstplänen auf Seite 138.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

Thema	Handbuch
Grundlagen zur Zuweisung von Unternehmensressourcen und zur Vererbung von Unternehmensressourcen	*One Identity Manager Administrationshandbuch für das Identity Management Basismodul* *One Identity Manager Administrationshandbuch für Geschäftsrollen*
Zuweisung von Unternehmensressourcen über IT Shop-Bestellungen	*One Identity Manager Administrationshandbuch für IT Shop*
Systemrollen	*One Identity Manager Administrationshandbuch für Systemrollen*

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten auf Seite 146
- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143
- Azure Active Directory Abonnements an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 148
- Azure Active Directory Abonnements an Geschäftsrollen zuweisen auf Seite 149
- Azure Active Directory Abonnements in Systemrollen aufnehmen auf Seite 150
- Azure Active Directory Abonnements in den IT Shop aufnehmen auf Seite 151
- Azure Active Directory Abonnements automatisch in den IT Shop aufnehmen auf Seite 153
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Abonnements zuweisen auf Seite 155
- Azure Active Directory Abonnements direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 157

Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten

Bei der indirekten Zuweisung werden Identitäten und Azure Active Directory Abonnements in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet. Für die indirekte Zuweisung von Azure Active Directory Abonnements prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Identitäten und Azure Active Directory Abonnements erlaubt.

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

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

   1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

      - ODER -

      Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
   2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
      - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
      - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
   3. Speichern Sie die Änderungen.
2. Einstellungen für die Zuweisung von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten.
   - Das Azure Active Directory Benutzerkonto ist mit einer Identität verbunden.
   - Am Azure Active Directory Benutzerkonto ist ein Standort eingetragen.
   - Am Azure Active Directory Benutzerkonto ist die Option **Abonnements erbbar** aktiviert.

HINWEIS: Bei der Vererbung von Unternehmensressourcen über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen spielen unter Umständen weitere Konfigurationseinstellungen eine Rolle. So kann beispielsweise die Vererbung für eine Rolle blockiert sein oder die Vererbung an Identitäten nicht erlaubt sein. Ausführliche Informationen über die Grundlagen zur Zuweisung von Unternehmensressourcen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Azure Active Directory Benutzerkonten erstellen und bearbeiten auf Seite 210
- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212

Azure Active Directory Abonnements an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Azure Active Directory Abonnements an Abteilungen, Kostenstellen oder Standorte zu, damit sie über diese Organisationen an Benutzerkonten zugewiesen wird.

Um ein Azure Active Directory Abonnement an Abteilungen, Kostenstellen oder Standorte zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Abonnements**.
2. Wählen Sie in der Ergebnisliste das Azure Active Directory 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 Azure Active Directory Abonnements 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 Abonnement zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** den Azure Active Directory Mandanten und weisen die Azure Active Directory Abonnements zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie das Azure Active Directory Abonnement und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten auf Seite 146
- Azure Active Directory Abonnements an Geschäftsrollen zuweisen auf Seite 149
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Abonnements zuweisen auf Seite 155
- Azure Active Directory Abonnements in Systemrollen aufnehmen auf Seite 150
- Azure Active Directory Abonnements in den IT Shop aufnehmen auf Seite 151
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 12

Azure Active Directory Abonnements an Geschäftsrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

Weisen Sie die Azure Active Directory Abonnements an Geschäftsrollen zu, damit die sie über diese Geschäftsrollen an Benutzerkonten zugewiesen wird.

Um ein Azure Active Directory Abonnement an Geschäftsrollen zuzuweisen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Abonnements**.
2. Wählen Sie in der Ergebnisliste das Azure Active Directory Abonnement.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie 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 Azure Active Directory Abonnements 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 Abonnements zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** den Azure Active Directory Mandanten und weisen die Azure Active Directory Abonnements zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie das Azure Active Directory Abonnement und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten auf Seite 146
- Azure Active Directory Abonnements an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 148
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Abonnements zuweisen auf Seite 155
- Azure Active Directory Abonnements in Systemrollen aufnehmen auf Seite 150
- Azure Active Directory Abonnements in den IT Shop aufnehmen auf Seite 151
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 12

Azure Active Directory Abonnements in Systemrollen aufnehmen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Systemrollenmodul vorhanden ist.

Mit dieser Aufgabe nehmen Sie ein Azure Active Directory Abonnement in Systemrollen auf. Wenn Sie eine Systemrolle an Identitäten zuweisen, wird das Azure Active Directory Abonnement an alle Azure Active Directory Benutzerkonten vererbt, die diese Identitäten besitzen.

HINWEIS: Azure Active Directory 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*.

TIPP: Damit eine Identität automatisiert ein Azure Active Directory Benutzerkonto und ein Azure Active Directory Abonnement erhält, können Sie die Kontendefinition zur Erstellung des Benutzerkontos und das zu verwendende Azure Active Directory Abonnement in einer Systemrolle zusammenfassen.

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

Um ein Azure Active Directory Abonnement an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Abonnements**.
2. Wählen Sie in der Ergebnisliste das Azure Active Directory 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

- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten auf Seite 146
- Azure Active Directory Abonnements an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 148
- Azure Active Directory Abonnements an Geschäftsrollen zuweisen auf Seite 149
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Abonnements zuweisen auf Seite 155
- Azure Active Directory Abonnements in den IT Shop aufnehmen auf Seite 151

Azure Active Directory Abonnements in den IT Shop aufnehmen

Mit der Zuweisung eines Azure Active Directory Abonnements an ein IT Shop Regal kann dieses von den Kunden des Shops bestellt werden. Für die Bestellbarkeit sind weitere Voraussetzungen zu gewährleisten.

- Das Azure Active Directory Abonnement muss mit der Option **IT Shop** gekennzeichnet sein.
- Dem Azure Active Directory Abonnement muss eine Leistungsposition zugeordnet sein.

- Soll das Azure Active Directory Abonnement nur über IT Shop-Bestellungen an Identitäten zugewiesen werden können, muss das Azure Active Directory 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 Azure Active Directory Abonnements an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Azure Active Directory Abonnements in den IT Shop aufzunehmen.

Um ein Azure Active Directory Abonnement in den IT Shop aufzunehmen

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

   - ODER -

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

Um ein Azure Active Directory Abonnement aus einzelnen Regalen des IT Shops zu entfernen

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

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Azure Active Directory Abonnements** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste das Azure Active Directory Abonnement.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** das Azure Active Directory Abonnement aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um ein Azure Active Directory Abonnement aus allen Regalen des IT Shops zu entfernen

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

   - ODER -

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

2. Wählen Sie in der Ergebnisliste das Azure Active Directory Abonnement.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

   Das Azure Active Directory Abonnement wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen dieses Azure Active Directory 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 248
- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten auf Seite 146
- Azure Active Directory Abonnements automatisch in den IT Shop aufnehmen auf Seite 153
- Azure Active Directory Abonnements an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 148
- Azure Active Directory Abonnements an Geschäftsrollen zuweisen auf Seite 149
- Azure Active Directory Abonnements in Systemrollen aufnehmen auf Seite 150
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Abonnements zuweisen auf Seite 155

Azure Active Directory Abonnements automatisch in den IT Shop aufnehmen

Mit den folgenden Schritten können Azure Active Directory Abonnements automatisch in den IT Shop aufgenommen werden. Die Synchronisation sorgt dafür, dass die Azure Active Directory Abonnements in den IT Shop aufgenommen werden. Bei Bedarf können Sie die Synchronisation im Synchronization Editor sofort starten.
Azure Active Directory Abonnements, die im One Identity Manager neu erstellt werden, werden ebenfalls automatisch in den IT Shop aufgenommen.

Um Azure Active Directory Abonnements automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | AADSubSku**.
2. Um einzelne Azure Active Directory Abonnements nicht automatisch in den IT Shop aufzunehmen, aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | AADSubSku | ExcludeList**.

   Der Konfigurationsparameter enthält eine Auflistung aller Azure Active Directory Abonnements, die nicht automatisch zum IT Shop zugeordnet werden sollen. Bei Bedarf können Sie die Liste erweitern. Erfassen Sie dazu im Wert des Konfigurationsparameters die Namen der Abonnements. Die Namen werden in einer Pipe (|) getrennten Liste angegeben. Reguläre Ausdrücke werden unterstützt.
3. Kompilieren Sie die Datenbank.

Die Azure Active Directory Abonnements werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

Folgende Schritte werden bei der Aufnahme eines Azure Active Directory Abonnements in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für das Azure Active Directory Abonnement ermittelt.

   Für jedes Azure Active Directory Abonnement wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Bezeichnung des Azure Active Directory Abonnements.

   - Für Azure Active Directory Abonnements mit Leistungsposition wird die Leistungsposition angepasst.
   - Azure Active Directory Abonnements ohne Leitungsposition erhalten eine neue Leistungsposition.
2. Die Leistungsposition wird der Standard-Servicekategorie **Azure Active Directory Abonnements** zugeordnet.
3. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet.

   Die Produkteigner können Bestellungen dieser Azure Active Directory Abonnements genehmigen. Standardmäßig wird der Eigentümer eines Azure Active Directory Abonnements als Produkteigner ermittelt.

   HINWEIS: Die Anwendungsrolle für Produkteigner muss der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** untergeordnet sein.

   - Ist der Eigentümer des Azure Active Directory Abonnements bereits Mitglied einer Anwendungsrolle für Produkteigner, dann wird diese Anwendungsrolle der Leistungsposition zugewiesen. Alle Mitglieder dieser Anwendungsrolle werden dadurch Produkteigner des Azure Active Directory Abonnements.
   - Ist der Eigentümer des Azure Active Directory Abonnements noch kein Mitglied einer Anwendungsrolle für Produkteigner, dann wird eine neue Anwendungsrolle erzeugt. Die Bezeichnung der Anwendungsrolle entspricht

der Bezeichnung des Eigentümers.

- Handelt es sich beim Eigentümer um ein Benutzerkonto, wird die Identität des Benutzerkontos in die Anwendungsrolle aufgenommen.
- Handelt es sich um eine Gruppe von Eigentümern, werden die Identitäten aller Benutzerkonten dieser Gruppe in die Anwendungsrolle aufgenommen.

4. Das Azure Active Directory Abonnement wird mit der Option **IT Shop** gekennzeichnet und dem IT Shop Regal **Azure Active Directory Abonnements** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Kunden des Shops das Azure Active Directory Abonnement über das Web Portal bestellen.

HINWEIS: Wenn ein Azure Active Directory Abonnement endgültig aus der One Identity Manager-Datenbank gelöscht wird, wird auch die zugehörige Leistungsposition gelöscht.

Ausführliche Informationen zur Konfiguration des IT Shops finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*. Ausführliche Informationen zum Bestellen von Zugriffsanforderungen im Web Portal finden Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

Verwandte Themen

- Azure Active Directory Abonnements in den IT Shop aufnehmen auf Seite 151
- Azure Active Directory Abonnements an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 148
- Azure Active Directory Abonnements an Geschäftsrollen zuweisen auf Seite 149
- Azure Active Directory Benutzerkonten direkt an Azure Active Directory Abonnements zuweisen auf Seite 155
- Azure Active Directory Abonnements in Systemrollen aufnehmen auf Seite 150

Azure Active Directory Benutzerkonten direkt an Azure Active Directory Abonnements zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Azure Active Directory Abonnements direkt zuweisen. Azure Active Directory Abonnements, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Besonderheiten auf dem Zuweisungsformular

Auf dem Formular werden die Zuweisungen der Azure Active Directory Abonnements zu den Azure Active Directory Benutzerkonten mit ihrer Herkunft angezeigt. Dabei bedeuten:

- **Azure Active Directory Quellgruppe**: Azure Active Directory Gruppe, aus der eine Zuweisung resultiert. Ist die Spalte leer, handelt es sich um eine Zuweisung des Azure Active Directory Abonnements an das Azure Active Directory Benutzerkonto, die entweder direkt, über IT Shop Bestellungen oder über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen entstanden ist.
- **Herkunft**: Art der Zuweisung. Zuweisungen über Azure Active Directory Gruppen werden mit dem Wert **Zuweisung durch Gruppe** (`AADUserHasSubSku.XOrigin=16`) gekennzeichnet.

HINWEIS: Zuweisungen, die aus einer Azure Active Directory Gruppe entstanden sind, können Sie nicht entfernen.

Um ein Azure Active Directory Abonnement direkt an Benutzerkonten zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Abonnements**.
2. Wählen Sie in der Ergebnisliste das Azure Active Directory Abonnement.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Klicken Sie **Hinzufügen** und wählen Sie in der Auswahlliste **Azure Active Directory Benutzerkonto** das Benutzerkonto.
5. Speichern Sie die Änderungen.

Um die direkte Zuweisung eines Azure Active Directory Abonnements zu entfernen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Abonnements**.
2. Wählen Sie in der Ergebnisliste das Azure Active Directory Abonnement.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Wählen Sie die Zuweisung und klicken Sie **Entfernen**.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143
- Azure Active Directory Abonnements direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 157
- Azure Active Directory Abonnements an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 148
- Azure Active Directory Abonnements an Geschäftsrollen zuweisen auf Seite 149
- Azure Active Directory Abonnements in Systemrollen aufnehmen auf Seite 150
- Azure Active Directory Abonnements in den IT Shop aufnehmen auf Seite 151

Azure Active Directory Abonnements direkt an Azure Active Directory Benutzerkonten zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Azure Active Directory Abonnements direkt zuweisen. Azure Active Directory Abonnements, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Besonderheiten auf dem Zuweisungsformular

Auf dem Formular werden die Zuweisungen der Azure Active Directory Abonnements zu den Azure Active Directory Benutzerkonten mit ihrer Herkunft angezeigt. Dabei bedeuten:

- **Azure Active Directory Quellgruppe**: Azure Active Directory Gruppe, aus der eine Zuweisung resultiert. Ist die Spalte leer, handelt es sich um eine Zuweisung des Azure Active Directory Abonnements an das Azure Active Directory Benutzerkonto, die entweder direkt, über IT Shop Bestellungen oder über Abteilungen, Kostenstellen, Standorte und Geschäftsrollen entstanden ist.
- **Herkunft**: Art der Zuweisung. Zuweisungen über Azure Active Directory Gruppen werden mit dem Wert **Zuweisung durch Gruppe** (`AADUserHasSubSku.XOrigin=16`) gekennzeichnet.

HINWEIS: Zuweisungen, die aus einer Azure Active Directory Gruppe entstanden sind, können Sie nicht entfernen.

Um Azure Active Directory Abonnements 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 **Abonnements direkt zuweisen**.
4. Klicken Sie **Hinzufügen** und wählen Sie in der Auswahlliste **Azure Active Directory Abonnement** das Azure Active Directory Abonnement.
5. Speichern Sie die Änderungen.

Um die direkte Zuweisung eines Azure Active Directory Abonnements zu entfernen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Abonnements direkt zuweisen**.
4. Wählen Sie die Zuweisung und klicken Sie **Entfernen**.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143
- Zuweisen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten auf Seite 145
- Azure Active Directory Abonnements an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 148
- Azure Active Directory Abonnements an Geschäftsrollen zuweisen auf Seite 149
- Azure Active Directory Abonnements in Systemrollen aufnehmen auf Seite 150
- Azure Active Directory Abonnements in den IT Shop aufnehmen auf Seite 151

Zuweisen von unwirksamen Azure Active Directory Dienstpläne an Azure Active Directory Benutzerkonten

Unwirksame Azure Active Directory Dienstpläne können indirekt oder direkt an Azure Active Directory Benutzerkonten zugewiesen werden.

Bei der indirekten Zuweisung werden Identitäten 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 Azure Active Directory Dienstpläne berechnet, die einer Identität zugewiesen sind. Besitzt die Identität ein Benutzerkonto im Azure Active Directory, werden die unwirksamen Dienstpläne der Rollen an dieses Benutzerkonto vererbt.

Des Weiteren können unwirksame Dienstpläne über IT Shop-Bestellungen an Identitäten zugewiesen werden. Damit unwirksame Dienstpläne über IT Shop-Bestellungen zugewiesen werden können, werden Identitäten 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 Identitäten zugewiesen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die unwirksamen Dienstpläne auch direkt an Azure Active Directory Benutzerkonten zuweisen.

HINWEIS: Es ist möglich, dass ein Azure Active Directory Benutzerkonto das gleiche Azure Active Directory Abonnement sowohl direkt als auch über eine oder mehrere Azure Active Directory Gruppen erhält. Ist ein Dienstplan über einen Zuweisungsweg erlaubt und über einen anderen Zuweisungsweg nicht erlaubt, dann erhält der Benutzer den Dienstplan.

Das bedeutet:

Ein unwirksamer Dienstplan, der an ein Benutzerkonto zugewiesen ist, kann effektiv erlaubt sein, wenn das Benutzerkonto diesen Dienstplan zusätzlich über eine Gruppe erhält und der Dienstplan für die Gruppe erlaubt ist.

Weitere Informationen finden Sie unter Managen von Zuweisungen von Azure Active Directory Abonnements und Azure Active Directory Dienstplänen auf Seite 138 und Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

Thema	Handbuch
Grundlagen zur Zuweisung von Unternehmensressourcen und zur Vererbung von Unternehmensressourcen	*One Identity Manager Administrationshandbuch für das Identity Management Basismodul* *One Identity Manager Administrationshandbuch für Geschäftsrollen*
Zuweisung von Unternehmensressourcen über IT Shop-Bestellungen	*One Identity Manager Administrationshandbuch für IT Shop*
Systemrollen	*One Identity Manager Administrationshandbuch für Systemrollen*

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von unwirksamen Azure Active Directory Dienstplänen an Azure Active Directory Benutzerkonten auf Seite 160
- Unwirksame Azure Active Directory Dienstpläne an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 161
- Unwirksame Azure Active Directory Dienstpläne an Geschäftsrollen zuweisen auf Seite 162
- Unwirksame Azure Active Directory Dienstpläne in Systemrollen aufnehmen auf Seite 163
- Unwirksame Azure Active Directory Dienstpläne in den IT Shop aufnehmen auf Seite 164
- Unwirksame Azure Active Directory Dienstpläne automatisch in den IT Shop aufnehmen auf Seite 166
- Azure Active Directory Benutzerkonten direkt an unwirksame Azure Active Directory Dienstpläne zuweisen auf Seite 168
- Unwirksame Azure Active Directory Dienstpläne direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 169

Voraussetzungen für indirekte Zuweisungen von unwirksamen Azure Active Directory Dienstplänen an Azure Active Directory Benutzerkonten

Bei der indirekten Zuweisung werden Identitäten und unwirksame Dienstpläne in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet. Für die indirekte Zuweisung von unwirksamen Azure Active Directory Dienstplänen prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Identitäten und unwirksamen Azure Active Directory Dienstpläne erlaubt.

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

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

   1. Wählen Sie im Manager in der Kategorie **Organisationen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.

      - ODER -

      Wählen Sie im Manager in der Kategorie **Geschäftsrollen > Basisdaten zur Konfiguration > Rollenklassen** die Rollenklasse.
   2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
      - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
      - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
   3. Speichern Sie die Änderungen.
2. Einstellungen für die Zuweisung von unwirksamen Azure Active Directory Dienstplänen an Azure Active Directory Benutzerkonten.
   - Das Azure Active Directory Benutzerkonto ist mit einer Identität verbunden.
   - Am Azure Active Directory Benutzerkonto ist die Option **Unwirksame Dienstpläne erbbar** aktiviert.

Verwandte Themen

- Azure Active Directory Benutzerkonten erstellen und bearbeiten auf Seite 210
- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212

Unwirksame Azure Active Directory Dienstpläne an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die unwirksamen Azure Active Directory 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 im Manager 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 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 **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

- Voraussetzungen für indirekte Zuweisungen von unwirksamen Azure Active Directory Dienstplänen an Azure Active Directory Benutzerkonten auf Seite 160
- Unwirksame Azure Active Directory Dienstpläne an Geschäftsrollen zuweisen auf Seite 162
- Azure Active Directory Benutzerkonten direkt an unwirksame Azure Active Directory Dienstpläne zuweisen auf Seite 168
- Unwirksame Azure Active Directory Dienstpläne in Systemrollen aufnehmen auf Seite 163
- Unwirksame Azure Active Directory Dienstpläne in den IT Shop aufnehmen auf Seite 164
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 12

Unwirksame Azure Active Directory Dienstpläne an Geschäftsrollen zuweisen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Geschäftsrollenmodul vorhanden ist.

Weisen Sie die unwirksamen Azure Active Directory 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 im Manager die Kategorie **Azure Active Directory > Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Dienstplan.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie 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 ✓.

1. Speichern Sie die Änderungen.

Um unwirksame Dienstpläne 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 **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

- Voraussetzungen für indirekte Zuweisungen von unwirksamen Azure Active Directory Dienstplänen an Azure Active Directory Benutzerkonten auf Seite 160
- Unwirksame Azure Active Directory Dienstpläne an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 161
- Azure Active Directory Benutzerkonten direkt an unwirksame Azure Active Directory Dienstpläne zuweisen auf Seite 168
- Unwirksame Azure Active Directory Dienstpläne in Systemrollen aufnehmen auf Seite 163
- Unwirksame Azure Active Directory Dienstpläne in den IT Shop aufnehmen auf Seite 164
- One Identity Manager Benutzer für die Verwaltung einer Azure Active Directory-Umgebung auf Seite 12

Unwirksame Azure Active Directory Dienstpläne in Systemrollen aufnehmen

HINWEIS: Diese Funktion steht zur Verfügung, wenn das Systemrollenmodul vorhanden ist.

Mit dieser Aufgabe nehmen Sie einen unwirksamen Azure Active Directory Dienstplan in Systemrollen auf. Wenn Sie eine Systemrolle an Identitäten zuweisen, wird der unwirksame Dienstplan an alle Azure Active Directory Benutzerkonten vererbt, die diese Identitäten besitzen.

HINWEIS: Unwirksame Azure Active Directory 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 im Manager 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

- Voraussetzungen für indirekte Zuweisungen von unwirksamen Azure Active Directory Dienstplänen an Azure Active Directory Benutzerkonten auf Seite 160
- Unwirksame Azure Active Directory Dienstpläne an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 161
- Unwirksame Azure Active Directory Dienstpläne an Geschäftsrollen zuweisen auf Seite 162
- Azure Active Directory Benutzerkonten direkt an unwirksame Azure Active Directory Dienstpläne zuweisen auf Seite 168
- Unwirksame Azure Active Directory Dienstpläne in den IT Shop aufnehmen auf Seite 164

Unwirksame Azure Active Directory Dienstpläne in den IT Shop aufnehmen

Mit der Zuweisung eines unwirksamen Azure Active Directory 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 Identitäten 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 im Manager die Kategorie **Azure Active Directory > Unwirksame Dienstpläne** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager 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 im Manager die Kategorie **Azure Active Directory > Unwirksame Dienstpläne** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager 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 im Manager die Kategorie **Azure Active Directory > Unwirksame Dienstpläne** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

Wählen Sie im Manager 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

- Voraussetzungen für indirekte Zuweisungen von unwirksamen Azure Active Directory Dienstplänen an Azure Active Directory Benutzerkonten auf Seite 160
- Unwirksame Azure Active Directory Dienstpläne automatisch in den IT Shop aufnehmen auf Seite 166
- Unwirksame Azure Active Directory Dienstpläne an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 161
- Unwirksame Azure Active Directory Dienstpläne an Geschäftsrollen zuweisen auf Seite 162
- Azure Active Directory Benutzerkonten direkt an unwirksame Azure Active Directory Dienstpläne zuweisen auf Seite 168
- Unwirksame Azure Active Directory Dienstpläne in Systemrollen aufnehmen auf Seite 163

Unwirksame Azure Active Directory Dienstpläne automatisch in den IT Shop aufnehmen

Mit den folgenden Schritten können unwirksame Azure Active Directory Dienstpläne automatisch in den IT Shop aufgenommen werden. Die Synchronisation sorgt dafür, dass die unwirksamen Dienstpläne in den IT Shop aufgenommen werden. Bei Bedarf können Sie die Synchronisation im Synchronization Editor sofort starten. Unwirksame Dienstpläne, die im One Identity Manager neu erstellt werden, werden ebenfalls automatisch in den IT Shop aufgenommen.

Um unwirksame Dienstpläne automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | AADDeniedServicePlan**.
2. Um einzelne unwirksame Dienstpläne nicht automatisch in den IT Shop aufzunehmen, aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | AADDeniedServicePlan | ExcludeList**.

   Der Konfigurationsparameter enthält eine Auflistung aller unwirksamen Dienstpläne, die nicht automatisch zum IT Shop zugeordnet werden sollen. Bei Bedarf können Sie die Liste erweitern. Erfassen Sie dazu im Wert des Konfigurationsparameters die Namen der Abonnements. Die Namen werden in einer Pipe (|) getrennten Liste angegeben. Reguläre Ausdrücke werden unterstützt.
3. Kompilieren Sie die Datenbank.

Die unwirksamen Dienstpläne werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

Folgende Schritte werden bei der Aufnahme eines unwirksamen Dienstplans in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für den unwirksamen Dienstplan ermittelt.

   Für jeden unwirksamen Dienstplan wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Bezeichnung des unwirksamen Dienstplans.

   - Für unwirksame Dienstpläne mit Leistungsposition wird die Leistungsposition angepasst.
   - Unwirksame Dienstpläne ohne Leitungsposition erhalten eine neue Leistungsposition.
2. Die Leistungsposition wird der Standard-Servicekategorie **Unwirksame Azure Active Directory Dienstpläne** zugeordnet.
3. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet.

   Die Produkteigner können Bestellungen dieser unwirksamen Dienstpläne genehmigen. Standardmäßig wird der Eigentümer eines unwirksamen Dienstplans als Produkteigner ermittelt.

   HINWEIS: Die Anwendungsrolle für Produkteigner muss der Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner** untergeordnet sein.

   - Ist der Eigentümer des unwirksamen Dienstplans bereits Mitglied einer Anwendungsrolle für Produkteigner, dann wird diese Anwendungsrolle der Leistungsposition zugewiesen. Alle Mitglieder dieser Anwendungsrolle werden dadurch Produkteigner des unwirksamen Dienstplans.
   - Ist der Eigentümer des unwirksamen Dienstplans noch kein Mitglied einer Anwendungsrolle für Produkteigner, dann wird eine neue Anwendungsrolle erzeugt. Die Bezeichnung der Anwendungsrolle entspricht der Bezeichnung des Eigentümers.

- Handelt es sich beim Eigentümer um ein Benutzerkonto, wird die Identität des Benutzerkontos in die Anwendungsrolle aufgenommen.
- Handelt es sich um eine Gruppe von Eigentümern, werden die Identitäten aller Benutzerkonten dieser Gruppe in die Anwendungsrolle aufgenommen.

4. Der unwirksame Dienstplan wird mit der Option **IT Shop** gekennzeichnet und dem IT Shop Regal **Unwirksame Azure Active Directory Dienstpläne** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Kunden des Shops den unwirksamen Dienstplan über das Web Portal bestellen.

HINWEIS: Wenn ein unwirksamer Dienstplan endgültig aus der One Identity Manager-Datenbank gelöscht wird, wird auch die zugehörige Leistungsposition gelöscht.

Ausführliche Informationen zur Konfiguration des IT Shops finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*. Ausführliche Informationen zum Bestellen von Zugriffsanforderungen im Web Portal finden Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

Verwandte Themen

- Unwirksame Azure Active Directory Dienstpläne in den IT Shop aufnehmen auf Seite 164
- Unwirksame Azure Active Directory Dienstpläne an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 161
- Unwirksame Azure Active Directory Dienstpläne an Geschäftsrollen zuweisen auf Seite 162
- Azure Active Directory Benutzerkonten direkt an unwirksame Azure Active Directory Dienstpläne zuweisen auf Seite 168
- Unwirksame Azure Active Directory Dienstpläne in Systemrollen aufnehmen auf Seite 163

Azure Active Directory Benutzerkonten direkt an unwirksame Azure Active Directory Dienstpläne zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die unwirksamen Dienstpläne direkt zuweisen. Unwirksame Dienstpläne, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um einen unwirksamen Dienstplan direkt an Benutzerkonten zuzuweisen

1. Wählen Sie im Manager 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

- Azure Active Directory Abonnements direkt an Azure Active Directory Benutzerkonten zuweisen auf Seite 157
- Unwirksame Azure Active Directory Dienstpläne an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 161
- Unwirksame Azure Active Directory Dienstpläne an Geschäftsrollen zuweisen auf Seite 162
- Unwirksame Azure Active Directory Dienstpläne in Systemrollen aufnehmen auf Seite 163
- Unwirksame Azure Active Directory Dienstpläne in den IT Shop aufnehmen auf Seite 164

Unwirksame Azure Active Directory Dienstpläne direkt an Azure Active Directory Benutzerkonten zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die unwirksamen Dienstpläne direkt zuweisen. Unwirksame Dienstpläne, die mit der Option **Verwendung nur im IT Shop** gekennzeichnet sind, können nicht direkt zugewiesen werden.

Um unwirksame Dienstpläne 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 **Unwirksame Dienstpläne zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die unwirksamen Dienstpläne zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den unwirksamen Dienstplan und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Zuweisen von unwirksamen Azure Active Directory Dienstpläne an Azure Active Directory Benutzerkonten auf Seite 158
- Unwirksame Azure Active Directory Dienstpläne an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 161
- Unwirksame Azure Active Directory Dienstpläne an Geschäftsrollen zuweisen auf Seite 162
- Unwirksame Azure Active Directory Dienstpläne in Systemrollen aufnehmen auf Seite 163
- Unwirksame Azure Active Directory Dienstpläne in den IT Shop aufnehmen auf Seite 164

Vererbung von Azure Active Directory Abonnements anhand von Kategorien

Das unter Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 123 beschriebene Verhalten können Sie auch für Azure Active Directory Abonnements einsetzen.

Um die Vererbung über Kategorien zu nutzen

1. Definieren Sie im Manager am Azure Active Directory Mandanten die Kategorien.
2. Weisen Sie im Manager die Kategorien den Benutzerkonten über ihre Stammdaten zu.
3. Weisen Sie im Manager die Kategorien den Azure Active Directory Abonnements über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 203
- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212
- Stammdaten von Azure Active Directory Abonnements bearbeiten auf Seite 248

Vererbung von unwirksamen Azure Active Directory Dienstplänen anhand von Kategorien

Das unter Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 123 beschriebene Verhalten können Sie auch für unwirksame Dienstpläne einsetzen.

Um die Vererbung über Kategorien zu nutzen

1. Definieren Sie im Manager am Azure Active Directory Mandanten die Kategorien.
2. Weisen Sie im Manager die Kategorien den Benutzerkonten über ihre Stammdaten zu.
3. Weisen Sie im Manager die Kategorien den unwirksamen Dienstplänen über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 203
- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212
- Stammdaten von unwirksamen Azure Active Directory Dienstplänen bearbeiten auf Seite 252

7

Bereitstellen von Anmeldeinformationen für Azure Active Directory Benutzerkonten

Wenn neue Benutzerkonten im One Identity Manager angelegt werden, werden sofort auch die zur Anmeldung am Zielsystem benötigten Kennwörter erstellt. Um das initiale Kennwort zu vergeben, stehen verschiedene Möglichkeiten zur Verfügung. Auf die Kennwörter werden vordefinierte Kennwortrichtlinien angewendet, die Sie bei Bedarf an Ihre Anforderungen anpassen können. Um die generierten Anmeldeinformationen an die Benutzer zu verteilen, können Sie E-Mail-Benachrichtigungen einrichten.

Detaillierte Informationen zum Thema

- Kennwortrichtlinien für Azure Active Directory Benutzerkonten auf Seite 172
- Initiales Kennwort für neue Azure Active Directory Benutzerkonten auf Seite 184
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 185

Kennwortrichtlinien für Azure Active Directory Benutzerkonten

Der One Identity Manager unterstützt Sie beim Erstellen von komplexen Kennwortrichtlinien beispielsweise für Systembenutzerkennwörter, das zentrale Kennwort von Identitäten 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 auf Seite 173
- Kennwortrichtlinien anwenden auf Seite 174
- Kennwortrichtlinien erstellen auf Seite 176
- Kennwortrichtlinien bearbeiten auf Seite 176
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 180
- Ausschlussliste für Kennwörter auf Seite 183
- Kennwörter prüfen auf Seite 184
- Generieren eines Kennwortes testen auf Seite 184

Vordefinierte Kennwortrichtlinien

Die vordefinierten 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 Identitäten, Benutzerkonten oder Systembenutzer ermittelt werden kann.

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Identitäten

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

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

Ausführliche Informationen zu Kennwortrichtlinien für Identitäten 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 9.2 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.
    - **Anwenden auf**: Anwendungsbereich der Kennwortrichtlinie.

      Um den Anwendungsbereich festzulegen

      1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.
      2. Wählen Sie unter **Tabelle** eine der folgenden Referenzen:
          - Die Tabelle, die die Basisobjekte der Synchronisation enthält.
          - Um die Kennwortrichtlinie abhängig von der Kontendefinition anzuwenden, wählen Sie die Tabelle **TSBAccountDef**.
          - Um die Kennwortrichtlinie abhängig vom Automatisierungsgrad anzuwenden, wählen Sie die Tabelle **TSBBehavoir**.
      3. Wählen Sie unter **Anwenden auf** die Tabelle, die die Basisobjekte enthält.
          - Wenn Sie die Tabelle mit den Basisobjekten der Synchronisation gewählt haben, dann wählen Sie das konkrete Zielsystem.
          - Wenn Sie die Tabelle **TSBAccountDef** gewählt haben, dann wählen Sie die konkrete Kontendefinition.
          - Wenn Sie die Tabelle **TSBBehavior** gewählt haben, dann wählen Sie den konkreten Automatisierungsgrad.
      4. 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 erstellen

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.

Um eine Kennwortrichtlinie zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular erfassen Sie die Stammdaten der Kennwortrichtlinie.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 177
- Richtlinieneinstellungen auf Seite 177
- Zeichenklassen für Kennwörter auf Seite 179
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 180
- Kennwortrichtlinien bearbeiten auf Seite 176

Kennwortrichtlinien bearbeiten

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

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.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Kennwortrichtlinie.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 177
- Richtlinieneinstellungen auf Seite 177
- Zeichenklassen für Kennwörter auf Seite 179
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 180
- Kennwortrichtlinien erstellen auf Seite 176

Allgemeine Stammdaten für Kennwortrichtlinien

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 20: 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. Die Option kann nicht geändert werden. HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Identitäten, Benutzerkonten oder Systembenutzer ermittelt werden kann.

Richtlinieneinstellungen

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

Tabelle 21: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wenn beim Erstellen eines Benutzerkontos kein Kennwort angegeben wird oder kein Zufallskennwort generiert wird, 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. Ist der Wert **0**, ist kein Kennwort erforderlich.
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. Die Anzahl der Fehlanmeldungen wird nur bei der Anmeldung am One Identity Manager berücksichtigt. Ist der Wert **0**, dann wird die Anzahl der Fehlanmeldungen nicht berücksichtigt. Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder identitätenbasierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen überschritten, kann sich die Identität oder der Systembenutzer nicht mehr am One Identity Manager anmelden. Kennwörter gesperrter Identitäten und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.
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. Ist der Wert **0**, dann läuft das Kennwort nicht ab.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert. Ist der Wert **0**, dann werden keine Kennwörter in der Kennwortchronik gespeichert.
Min. Kennwortstärke	Gibt an, 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**,

Eigenschaft	Bedeutung
	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	Gibt an, 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 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 22: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Erforderliche Anzahl von Zeichenklassen	Anzahl der Regeln für Zeichenklassen, die erfüllt sein müssen, damit ein Kennwort der Kennwortrichtlinie entspricht. Berücksichtigt werden die Regeln für **Min. Anzahl Buchstaben**, **Min. Anzahl Kleinbuchstaben**, **Min. Anzahl Großbuchstaben**, **Min. Anzahl Ziffern** und **Min. Anzahl Sonderzeichen**. Es bedeuten: • Wert **0**: Es müssen alle Zeichenklassenregeln erfüllt sein. • Wert **> 0**: Anzahl der Zeichenklassenregeln, die mindestens erfüllt sein müssen. Der Wert kann maximal der Anzahl der Regeln entsprechend, deren Wert **> 0** ist. HINWEIS: Die Prüfung erfolgt nicht für generierte Kennwörter.
Min. Anzahl Buchstaben	Gibt an, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss.
Min. Anzahl Kleinbuchstaben	Gibt an, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Großbuchstaben	Gibt an, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.

Eigenschaft	Bedeutung
Min. Anzahl Ziffern	Gibt an, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Gibt an, 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	Gibt an, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keinen Großbuch-staben erzeugen	Gibt an, ob ein generiertes Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Ziffern erzeugen	Gibt an, ob ein generiertes Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berück-sichtigt.
Keine Sonderzeichen erzeugen	Gibt an, 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 181
- Skript zum Generieren eines Kennwortes auf Seite 182

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: 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 182

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: 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 181

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 ein initiales Kennwort für neue Azure Active Directory Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung.

- Tragen Sie beim Erstellen des Benutzerkontos in den Stammdaten 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 Identität das initiale Kennwort per E-Mail versendet wird.

Verwandte Themen

- Kennwortrichtlinien für Azure Active Directory Benutzerkonten auf Seite 172
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 185

E-Mail-Benachrichtigungen über Anmeldeinformationen

Die Anmeldeinformationen für neue Benutzerkonten können per E-Mail an eine festgelegte Identität 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 Identitäten 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 Identitäten eine Sprache ermittelt werden kann. Nur so erhalten die Identitäten 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 Identität 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 **Identität - 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 **Identität - 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.

Azure Active Directory Rollenmanagement

Das Rollenmanagement beschreibt eine erweiterte Rollenverwaltungsfunktionalität der rollenbasierten Zugriffsteuerung in Microsoft 365. Diese ermöglicht dem Nutzer die Verwaltung von Rollen und deren Mitgliedern, als auch die Beschränkung von Rollenzuweisungen in Azure Active Directory Teilbereichen.

Verwandte Themen

- Azure Active Directory Rollenmanagement Mandanten
- Azure Active Directory Rollenzuweisungen hinzufügen
- Azure Active Directory Rollenberechtigungen hinzufügen
- Azure Active Directory Rollenzuweisungen für Bereiche zuweisen
- Azure Active Directory Rollenberechtigungen für Bereiche zuweisen
- Stammdaten von Azure Active Directory Rollen
- Managen von Azure Active Directory Rollenzuweisungen
- Managen von Azure Active Directory Rollenberechtigungen

Azure Active Directory Rollenmanagement Mandanten

Das Azure Active Directory Rollenmanagement stellt eine Auswahl von Rollenverwaltungsfunktionalitäten zur Verfügung. Der Umfang dieser Funktionen richtet sich nach der vom Nutzer ausgewählten Azure Active Directory Lizenzstufe, welche entsprechende Mandanten bereitstellen.

Azure AD "Free"

Diese Lizenz beinhaltet die Basisfunktionalitäten des Rollenmanagements. Integrierte Rollen können ohne Einschränkung verwendet werden. Diese Rollen besitzen vorgegebene

Rollendefinitionen. Das Hinzufügen und Entfernen einzelner Benutzer in integrierte Rollen ist innerhalb dieser Lizenz möglich. Gruppen können erstellt werden.

WICHTIG: Die Pflege von Verzeichnisrollen im One Identity Manager und die Verwendung benutzerdefinierter Rollen ist in den Basisfunktionalitäten nicht enthalten. Für diese Funktion wird die Azure AD P1-Lizenz oder P2-Lizenz benötigt.

WICHTIG: Verzeichnisrollen müssen über das Microsoft Azure Portal gepflegt werden.

WICHTIG: Diese Lizenz ermöglicht die Rollenzuweisung einzelner Benutzer. Die Zuweisung von Rollen an Gruppen ist nur innerhalb der Azure AD P1-Lizenz und P2-Lizenz möglich.

Azure AD Premium P1 - Rollenbasierte Zugriffssteuerung (RBAC)

Die rollenbasierte Zugriffssteuerung wird durch die Azure Active Directory Premium P1-Lizenz zur Verfügung gestellt. Sie beinhaltet neben den Basisfunktionen den Zugriff auf Rollendefinitionen und Rollenzuweisungen. Rollen können einer ganzen Gruppe zugewiesen werden. Dies ermöglicht übereinstimmende Rollenberechtigungen innerhalb einer Gruppe. Gruppen können erstellt werden.

Es gibt zwei verschiedene Arten von Teilbereichen, auf welche die rollenbasierte Zugriffssteuerung angewendet werden kann.

- Eingrenzung Verzeichnisobjekte: Rollenzuweisungen lassen sich auf bestimmte Objekte, beispielsweise eine registrierte Applikation oder einen Benutzer, innerhalb des Azure Active Directory Verzeichnisses begrenzen. Die Eingrenzung auf Elemente einer definierten administrativen Einheit ist ebenfalls möglich.
- Eingrenzung auf anwenderspezifische Elemente eines Dienstes: Benutzerdefinierte Rollen können synchronisiert aber nicht aus dem One Identity Manager angelegt werden.

WICHTIG: Diese Lizenz beinhaltet nicht die Funktionalitäten des Azure Active Directory Privileged Identity Management.

Azure AD Premium P2 - Privileged Identity Managemen (PIM)

Neben den bereits vorhandenen Einschränkungen der rollenbasierten Zugriffssteuerung, bietet diese Lizenz die zusätzliche Funktionalitäten zur Einschränkung und Steuerung von Rollenzuweisungen. Das Privileged Identity Management unterscheidet zwischen aktiven Rollenzuweisungen und Zuweisungsberechtigungen.

Rollenzuweisung: Einem Prinzipal wird eine Rolle zugewiesen.

Rollenberechtigung: Ein Prinzipal hat keine aktive Rollenzuweisung, kann bei Bedarf aber eine temporäre Rollenzuweisung aktivieren.

Eine Konfiguration von Rollenrichtlinien, wie beispielsweise zeitliche Begrenzungen, ist für beide Zuweisungsarten möglich. Weiterhin besteht die Möglichkeit, Attestierungen für Rollen zu erstellen.

HINWEIS: Die Erstellung von Rollenzuweisungen, für welche eine Multifaktor-Authentifizierung verpflichtend ist, ist nicht möglich.

HINWEIS: Aufgrund von Einschränkungen der Microsoft Graph API unterstützt das Rollenmanagement Feature im One Identity Manager im Modus "PIM" ausschließlich den globalen Verzeichnisbereich für aktive Rollenzuweisungen.

Detaillierte Informationen zum Thema

- Übersicht über die rollenbasierte Zugriffssteuerung in Azure Active Directory
- Grundlegendes zu Rollen in Azure Active Directory

Verwandte Themen

- Azure Active Directory Rollenmanagement
- Azure Active Directory Rollenberechtigungen hinzufügen
- Azure Active Directory Rollenzuweisungen für Bereiche zuweisen
- Azure Active Directory Rollenberechtigungen für Bereiche zuweisen

Aktivierung der Funktionen des Azure Active Directory Rollenmanagement

Mit Einführung des Rollenmanagements von Microsoft 365 werden erweitere Funktionalitäten für die Verwaltung von Rollen und deren Mitgliedern und die Beschränkung von Rollenzuweisungen in Azure Active Directory Teilbereichen des One Identity Manager, zur Verfügung gestellt.

Neue als auch bestehende Synchronisationsprojekte erhalten mit der Einführung des Azure Active Directory Rollenmanagements automatisch den Basis-Modus (gleichzusetzen mit der Azure AD Free Lizenz von Microsoft 365). Der Basis-Modus beinhaltet alle bisherigen Funktionen des One Identity Manager. Die neuen Funktionen des Rollenmanagements werden durch die Aktivierung des RBAC-Modus (Azure AD P1-Lizenz) und PIM-Modus (Azure AD P2-Lizenz) zugänglich. Diese Aktivierung ist notwendig für bereits bestehende Synchronisationsprojekte, sowie bei Neuanlage eines Synchronisationsprojektes.

HINWEIS: Alle bisherigen Funktionen des Azure Active Directory stehen weiterhin im Basis-Modus zur Verfügung. Die Aktivierung des RBAC-Modus oder PIM-Modus ist nur notwendig, sofern Sie die erweiterten Rollenverwaltungsfunktionen nutzen wollen.

Um die erweiterten Rollenverwaltungsfunktionen für RBAC zu aktivieren

1. Wählen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie **Workflows**.

3. Wählen Sie den Workflow **Initial Synchronization** und klicken Sie auf die Schaltfläche **Synchronisationsschritte aktivieren/deaktivieren**.
4. Deaktivieren Sie den Workflowschritt **DirectoryRole**.
5. Aktivieren Sie die folgenden Workflowschritte.
    a. **RBAC DirectoryRole**
    b. **RBAC DirectoryRole Assignments**
6. Speichern Sie die Änderungen.
7. Wählen Sie den Workflow **Provisioning** und klicken Sie auf die Schaltfläche **Synchronisationsschritte aktivieren/deaktivieren**.
8. Deaktivieren Sie den Workflowschritt **DirectoryRole**.
9. Aktivieren Sie den Workflowschritt **RBAC DirectoryRole Assignments**.
10. Speichern Sie die Änderungen.
11. Wählen Sie im Object Browser die Tabelle **AADOrganization**.
12. Setzen Sie den Wert **RoleBehavior** auf RBAC.
13. Speichern Sie die Änderungen.

Um die erweiterten Rollenverwaltungsfunktionen für PIM zu aktivieren

1. Wählen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie **Workflows**.
3. Wählen Sie den Workflow **Initial Synchronization** und klicken Sie auf die Schaltfläche **Synchronisationsschritte aktivieren/deaktivieren**.
4. Deaktivieren Sie den Workflowschritt **DirectoryRole**.
5. Aktivieren Sie die folgenden Workflowschritte.
    a. **RBAC DirectoryRole**
    b. **PIM DirectoryRole Assignments**
    c. **PIM DirectoryRole Eligibility**
    d. **PIM DirectoryRole Policies**
6. Speichern Sie die Änderungen.
7. Wählen Sie den Workflow **Provisioning** und klicken Sie auf die Schaltfläche **Synchronisationsschritte aktivieren/deaktivieren**.
8. Deaktivieren Sie den Workflowschritt **DirectoryRole**.
9. Aktivieren Sie die folgenden Workflowschritte.
    a. **PIM DirectoryRole Assignments**
    b. **PIM DirectoryRole Eligibility**
10. Speichern Sie die Änderungen.
11. Wählen Sie im Object Browser die Tabelle **AADOrganization**.

12. Setzen Sie den Wert **RoleBehavior** auf PIM.
13. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Übersicht über die rollenbasierte Zugriffssteuerung in Azure Active Directory
- Grundlegendes zu Rollen in Azure Active Directory

Verwandte Themen

- Azure Active Directory Rollenmanagement
- Azure Active Directory Rollenmanagement Mandanten
- Azure Active Directory Rollenzuweisungen für Bereiche zuweisen
- Azure Active Directory Rollenberechtigungen für Bereiche zuweisen

Stammdaten von Azure Active Directory Rollen

Zu einer Rolle erhalten Sie die folgenden allgemeinen Stammdaten.

Tabelle 23: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Anzeigename	Anzeigename zur Anzeige der Rolle in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Mandant	Azure Active Directory Mandant der Rolle.
Eigentümer (Anwendungsrolle)	Anwendungsrolle, deren Mitglieder die Rollenzuweisungen beziehungsweise Rollenberechtigungen entscheiden dürfen.
Provider	Schnittstelle, die für die Verwaltung der Rolle verantwortlich ist.
Version	Gibt die Version der Rollendefinition an.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Built-in	Gibt an, ob die Rollendefinition Teil der Azure Active Directory Grundeinstellungen oder eine benutzerdefinierte Definition ist.
Aktiviert	Gibt an, ob die Rolle für die Zuweisung freigegeben ist.

Verwandte Themen

- Azure Active Directory Rollenmanagement
- Azure Active Directory Rollenmanagement Mandanten
- Azure Active Directory Rollenzuweisungen für Bereiche zuweisen

Azure Active Directory Rollenzuweisungen hinzufügen

Durch das Rollenmanagement können Sie für Rollen zusätzliche Rollenzuweisungen in Azure Active Directory Teilbereichen vornehmen.

Um eine Rollenzuweisung an eine Rolle zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Rollen.**
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Hinzufügen oder Entfernen von Rollenzuweisungen**.
4. Klicken Sie **Hinzufügen** und erfassen Sie folgende Informationen.
    - **Prinzipal**: Der überstehende Prinzipal, dessen Zugriffe zugewiesen werden sollen, beispielsweise Gruppen oder einzelne Nutzer.
    - **App-Bereich**: Der Anwendungsbereich, für den der Prinzipal Zugriff erhalten soll.
      - ODER -
      Verzeichnisbereich: Der Verzeichnisbereich, für den der Prinzipal Zugriff erhalten soll.
    - Geben Sie an, ob es sich bei der Zuweisung um eine **Direkte Zuweisung** handelt.

      HINWEIS: Die Zuweisungsangaben **Indirekte Zuweisung** und **Zuweisungsbestellung** werden durch Prozesse gesetzt und sind nicht manuell setzbar.
    - **Bestellvorgang**: Verweis auf den Bestellvorgang, durch den die Zuweisung erfolgt ist.

      HINWEIS: Der Bestellvorgang wird durch Prozesse gesetzt und ist nicht manuell setzbar.

Verwandte Themen

- Azure Active Directory Rollenberechtigungen hinzufügen
- Managen von Azure Active Directory RollenzuweisungenManagen von Azure Active Directory Rollenzuweisungen
- Managen von Azure Active Directory Rollenberechtigungen

- Azure Active Directory Rollenzuweisungen für Bereiche zuweisen
- Azure Active Directory Rollenberechtigungen für Bereiche zuweisen

Azure Active Directory Rollenberechtigungen hinzufügen

Durch das Rollenmanagement können Sie Rollen zusätzliche Rollenberechtigungen in Azure Active Directory Teilbereichen zuweisen. Diese Rollenberechtigungen können bei Bedarf durch den zugewiesenen Prinzipal aktiviert werden.

Um eine Rollenberechtigung an eine Rolle zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Rollen.**
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Hinzufügen oder Entfernen von Rollenberechtigungen**.
4. Klicken Sie **Hinzufügen** und erfassen Sie folgende Informationen.
    - **Prinzipal**: Der überstehende Prinzipal, auf dessen Bereich ein Zugriff zugewiesen werden soll, beispielsweise Gruppen oder einzelne Nutzer.
    - **App-Bereich**: Der Anwendungsbereich, für den der Prinzipal Zugriff erhalten soll.
      - ODER -
      Verzeichnisbereich: Der Verzeichnisbereich, für den der Prinzipal Zugriff erhalten soll.
    - Geben Sie **Permanent** an, wenn es sich um eine dauerhafte Zuweisung handelt.
    - **Startzeit**: Der Zeitpunkt, ab dem die Rollenberechtigung zugewiesen wird.
    - **Schlusszeit**: Der Zeitpunkt, ab dem die Rollenberechtigung abgelaufen ist.

      HINWEIS: Durch die Auswahl von **Permanent** wird die Angabe **Schlusszeit** deaktiviert.
    - **Gültig von**: Der Zeitpunkt, ab dem die Gültigkeit der Rollenberechtigung beginnt.
    - **Gültig bis**: Der Zeitpunkt, ab dem die Gültigkeit der Rollenberechtigung ausläuft.
    - Geben Sie an, ob es sich bei der Zuweisung um eine **Direkte Zuweisung** handelt.

      HINWEIS: Die Zuweisungsangaben **Indirekte Zuweisung** und **Zuweisungsbestellung** werden durch Prozesse gesetzt und sind nicht manuell setzbar.

- **Bestellvorgang**: Verweis auf den Bestellvorgang, durch den die Zuweisung erfolgt ist.

Verwandte Themen

- Azure Active Directory Rollenzuweisungen hinzufügen
- Managen von Azure Active Directory RollenzuweisungenManagen von Azure Active Directory Rollenzuweisungen
- Managen von Azure Active Directory Rollenberechtigungen
- Azure Active Directory Rollenzuweisungen für Bereiche zuweisen
- Azure Active Directory Rollenberechtigungen für Bereiche zuweisen

Azure Active Directory Rollenzuweisungen für Bereiche zuweisen

Im Azure Active Directory können in bestimmten Teilbereichen aktive Rollenzuweisungen für Gruppen vergeben werden.

Um eine Systemrolle an einen Bereich zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Rollenzuweisungen für Bereiche.**
2. Wählen Sie in der Ergebnisliste die Rolle.
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.

Um eine Geschäftsrolle an einen Bereich zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Rollenzuweisungen für Bereiche.**
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie 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 eine Organisation an einen Bereich zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Rollenzuweisungen für Bereiche.**
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.

   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 ✓.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Azure Active Directory Rollenmanagement
- Azure Active Directory Rollenmanagement Mandanten
- Azure Active Directory Rollenzuweisungen hinzufügen
- Azure Active Directory Rollenberechtigungen hinzufügen
- Stammdaten von Azure Active Directory Rollen
- Azure Active Directory Rollenberechtigungen für Bereiche zuweisen

Azure Active Directory Rollenberechtigungen für Bereiche zuweisen

Im Azure Active Directory können in bestimmten Teilbereichen Rollenberechtigungen für Gruppen und Organisationen vergeben werden. Ein Prinzipal hat dadurch zwar keine aktive Rollenzuweisung, kann diese aber bei Bedarf jederzeit aktivieren.

Um eine Systemrolle an einen Bereich zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Rollenberechtigung für Bereiche.**
2. Wählen Sie in der Ergebnisliste die Rolle.
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.

Um eine Geschäftsrolle an einen Bereich zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Rollenberechtigung für Bereiche.**
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie 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 eine Organisation an einen Bereich zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Rollenberechtigung für Bereiche.**
2. Wählen Sie in der Ergebnisliste die Rolle.

3. Wählen Sie die Aufgabe **Organisationen zuweisen**.

   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 .

4. Speichern Sie die Änderungen.

Verwandte Themen

- Azure Active Directory Rollenmanagement
- Azure Active Directory Rollenmanagement Mandanten
- Stammdaten von Azure Active Directory Rollen
- Azure Active Directory Rollenzuweisungen für Bereiche zuweisen

Managen von Azure Active Directory Rollenzuweisungen

Um eine Rollenzuweisung zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Rollen.**
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Hinzufügen oder Entfernen von Rollenzuweisungen**.
4. Wählen Sie den Prinzipal aus der Ergebnisliste.
5. Bearbeiten Sie die gewünschten Informationen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Managen von Azure Active Directory Rollenberechtigungen
- Azure Active Directory Rollenzuweisungen hinzufügen
- Azure Active Directory Rollenberechtigungen hinzufügen

- Azure Active Directory Rollenzuweisungen für Bereiche zuweisen
- Azure Active Directory Rollenberechtigungen für Bereiche zuweisen

Managen von Azure Active Directory Rollenberechtigungen

Um eine Rollenzuweisung zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Rollen.**
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Hinzufügen oder Entfernen von Rollenberechtigungen**.
4. Wählen Sie den Prinzipal aus der Ergebnisliste.
5. Bearbeiten Sie die gewünschten Informationen.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Managen von Azure Active Directory Rollenzuweisungen
- Azure Active Directory Rollenzuweisungen hinzufügen
- Azure Active Directory Rollenberechtigungen hinzufügen
- Azure Active Directory Rollenzuweisungen für Bereiche zuweisen
- Azure Active Directory Rollenberechtigungen für Bereiche zuweisen

9

Abbildung von Azure Active Directory Objekten im One Identity Manager

Im One Identity Manager werden die Benutzerkonten, Gruppen, Administratorrollen, Abonnement, Dienstpläne, Anwendungen, Dienstprinzipale und App-Rollen eines Azure Active Directory Mandanten abgebildet. Diese Objekte werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können im Manager angezeigt oder bearbeitet werden.

Detaillierte Informationen zum Thema

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 200
- Azure Active Directory Domänen auf Seite 205
- Azure Active Directory Richtlinien zum Inaktivitätstimeout auf Seite 206
- Azure Active Directory Richtlinien zur Startbereichsermittlung auf Seite 206
- Azure Active Directory Richtlinien zur Token-Ausstellung auf Seite 207
- Azure Active Directory Richtlinien zur Token-Gültigkeitsdauer auf Seite 208

Azure Active Directory Mandant

Bei der erstmaligen Registrierung für einen Microsoft Cloud-Dienst stellen Sie Details zu Ihrer Organisation 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 Azure Active Directory Mandanten bearbeiten. Neue Azure Active Directory Mandanten können Sie im One Identity Manager nicht erstellen.

Um die Stammdaten eines Azure Active Directory Mandanten zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten**.
2. Wählen Sie in der Ergebnisliste den Azure Active Directory Mandanten.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

4. Bearbeiten Sie die Stammdaten für einen Azure Active Directory Mandanten.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Azure Active Directory Mandanten auf Seite 201
- Informationen zum lokalen Active Directory auf Seite 203
- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 203
- Einzelobjekte synchronisieren auf Seite 57

Allgemeine Stammdaten für Azure Active Directory Mandanten

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 24: Stammdaten eines Azure Active Directory Mandanten

Eigenschaft	Beschreibung
Anzeigename	Anzeigename des Azure Active Directory Mandanten.
Mandantentyp	Typ des Azure Active Directory Mandanten. Zulässige Werte sind: • **AAD**: Azure Active Directory Mandant • **AAD B2C**: Azure Active Directory B2C Mandanten Diese Eigenschaft wird durch die Synchronisation eingelesen und kann nicht bearbeitet werden.
Kontendefinition (initial)	Initiale Kontendefinition zur Erzeugung von Azure Active Directory Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diesen Azure Active Directory Mandanten die automatische Zuordnung von Identitäten zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet. Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Identität verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen des Azure Active Directory Mandanten festgelegt sind. Die

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>Zielsystemverantwortlichen bearbeiten nur die Objekte des Azure Active Directory Mandanten, dem sie zugeordnet sind. Jedem Azure Active Directory Mandanten können somit andere Zielsystemverantwortliche zugeordnet werden.

Wählen Sie die One Identity Manager Anwendungsrolle, deren Mitglieder verantwortlich für die Administration dieses Azure Active Directory Mandanten sind. Über die Schaltfläche  neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.</td></tr>
<tr><td>Standort</td><td>Standort des Azure Active Directory 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 Azure Active Directory Mandanten und dem One Identity Manager synchronisiert werden. Sobald Objekte für diesen Azure Active Directory Mandaten im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden.

Beim Erstellen eines Azure Active Directory Mandanten mit dem Synchronization Editor wird One Identity Manager verwendet.

Tabelle 25: Zulässige Werte
<table>
<tr><th>Wert</th><th>Synchronisation durch</th><th>Provisionierung 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 (Marketingbenachrichtigungen)</td><td>Liste von Empfängern von Marketingbenachrichtigungen.</td></tr>
</table>

Eigenschaft	Beschreibung
Empfänger (Technische Benachrichtigungen)	Liste von Empfängern von technischen Benachrichtigungen.
Empfänger (Sicherheitsbenachrichtigungen)	Liste von Empfängern von Sicherheitsbenachrichtigungen.
Telefonnummern (Sicherheitsbenachrichtigungen)	Telefonnummern für Sicherheitsbenachrichtigung.

Verwandte Themen

- Automatische Zuordnung von Identitäten zu Azure Active Directory Benutzerkonten auf Seite 92
- Zielsystemverantwortliche für Azure Active Directory auf Seite 275

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 26: Angaben zum lokalen Active Directory Benutzerkonto

Eigenschaft	Beschreibung
Synchronisation mit dem lokalen Active Directory aktiviert	Gibt an, 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 Gruppen, Administratorrollen, Abonnements und unwirksamen Dienstpläne an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 63**.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **Azure Active Directory > Mandanten** den Azure Active Directory 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 123
- Vererbung von Azure Active Directory Administratorrollen anhand von Kategorien auf Seite 136
- Vererbung von Azure Active Directory Abonnements anhand von Kategorien auf Seite 170
- Vererbung von unwirksamen Azure Active Directory Dienstplänen anhand von Kategorien auf Seite 171

Synchronisationsprojekt für einen Azure Active Directory Mandanten bearbeiten

Synchronisationsprojekte, in denen ein Azure Active Directory 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 im Manager die Kategorie **Azure Active Directory > Mandanten**.
2. Wählen Sie in der Ergebnisliste den Azure Active Directory Mandanten.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten**.

Verwandte Themen

- Anpassen der Synchronisationskonfiguration für Azure Active Directory-Umgebungen auf Seite 36

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 im Manager 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 27: Stammdaten einer Domäne

Eigenschaft	Beschreibung
Name der Domäne	Vollständiger Name der Domäne.
Mandant	Azure Active Directory Mandant, zu dem diese Domäne eingetragen ist.
Typ	Typ der Domäne.
Primäre Domäne	Gibt an, ob es sich um die primäre Domäne handelt, beispielsweise zum Erstellen neuer Azure Active Directory Benutzerkonten.
Initiale Domäne	Gibt an, 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.

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 57

Azure Active Directory Richtlinien zum Inaktivitätstimeout

Über Azure Active Directory Richtlinien zum Inaktivitätstimeout kann das Leerlauftimeout für Websitzungen für Anwendungen festgelegt werden. Ausführliche Informationen finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

Azure Active Directory Richtlinien zum Inaktivitätstimeout werden durch die Synchronisation in den One Identity Manager eingelesen und können nicht bearbeitet werden.

Um Informationen zu einer Azure Active Directory Richtlinie anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Ihr Mandant> > Richtlinien > Richtlinien zum Inaktivitätstimeout**.
2. Wählen Sie in der Ergebnisliste die Azure Active Directory Richtlinie.
3. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über die Richtlinie zum Inaktivitätstimeout**: Sie erhalten einen Überblick über die Azure Active Directory Richtlinie und ihre Abhängigkeiten.
    - **Stammdaten bearbeiten**: Es werden die Stammdaten für die Azure Active Directory Richtlinie angezeigt. Sie können die Stammdaten nicht bearbeiten.
        - **Anzeigename**: Anzeigename der Azure Active Directory Richtlinie.
        - **Beschreibung**: Beschreibung der Azure Active Directory Richtlinie.
        - **Definition**: Definition der Azure Active Directory Richtlinie im JSON Format.
        - **Mandant**: Azure Active Directory Mandant, zu dem die Richtlinie gehört.
        - **Standardrichtlinie**: Gibt an, ob es sich um die Standardrichtlinie des Azure Active Directory Mandanten handelt.

Azure Active Directory Richtlinien zur Startbereichsermittlung

Über Azure Active Directory Richtlinien zur Startbereichsermittlung kann die Anmeldung von Benutzern in Verbunddomänen beschleunigt werden. Um für eine Azure Active Directory Anwendung eine Azure Active Directory Richtlinie zur

Startbereichsermittlung zur Verfügung zu stellen, wird die Richtlinie an den Azure Active Directory Dienstprinzipal zugewiesen. Ausführliche Informationen finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

Azure Active Directory Richtlinien zur Startbereichsermittlung werden durch die Synchronisation in den One Identity Manager eingelesen und können nicht bearbeitet werden.

Um Informationen zu einer Azure Active Directory Richtlinie anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Ihr Mandant> > Richtlinien > Richtlinien zur Startbereichsermittlung**.
2. Wählen Sie in der Ergebnisliste die Azure Active Directory Richtlinie.
3. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über die Richtlinie zur Startbereichsermittlung**: Sie erhalten einen Überblick über die Azure Active Directory Richtlinie und ihre Abhängigkeiten.
    - **Stammdaten bearbeiten**: Es werden die Stammdaten für die Azure Active Directory Richtlinie angezeigt. Sie können die Stammdaten nicht bearbeiten.
        - **Anzeigename**: Anzeigename der Azure Active Directory Richtlinie.
        - **Beschreibung**: Beschreibung der Azure Active Directory Richtlinie.
        - **Definition**: Definition der Azure Active Directory Richtlinie im JSON Format.
        - **Mandant**: Azure Active Directory Mandant, zu dem die Richtlinie gehört.
        - **Standardrichtlinie**: Gibt an, ob es sich um die Standardrichtlinie des Azure Active Directory Mandanten handelt.

Verwandte Themen

- Stammdaten von Azure Active Directory Dienstprinzipalen anzeigen auf Seite 262

Azure Active Directory Richtlinien zur Token-Ausstellung

Über Azure Active Directory Richtlinien zur Token-Ausstellung können Eigenschaften von SAML-Token zur Anmeldung festgelegt werden. Um für eine Azure Active Directory Anwendung eine Azure Active Directory Richtlinie zur Token-Ausstellung zur Verfügung zu stellen, wird die Richtlinie an die Azure Active Directory Anwendung zugewiesen. Ausführliche Informationen finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

Azure Active Directory Richtlinien zur Token-Ausstellung werden durch die Synchronisation in den One Identity Manager eingelesen und können nicht bearbeitet werden.

Um Informationen zu einer Azure Active Directory Richtlinie anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Ihr Mandant> > Richtlinien > Richtlinien zur Token-Ausstellung**.
2. Wählen Sie in der Ergebnisliste die Azure Active Directory Richtlinie.
3. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über die Richtlinien zur Token-Ausstellung**: Sie erhalten einen Überblick über die Azure Active Directory Richtlinie und ihre Abhängigkeiten.
    - **Stammdaten bearbeiten**: Es werden die Stammdaten für die Azure Active Directory Richtlinie angezeigt. Sie können die Stammdaten nicht bearbeiten.
        - **Anzeigename**: Anzeigename der Azure Active Directory Richtlinie.
        - **Beschreibung**: Beschreibung der Azure Active Directory Richtlinie.
        - **Definition**: Definition der Azure Active Directory Richtlinie im JSON Format.
        - **Mandant**: Azure Active Directory Mandant, zu dem die Richtlinie gehört.
        - **Standardrichtlinie**: Gibt an, ob es sich um die Standardrichtlinie des Azure Active Directory Mandanten handelt.

Verwandte Themen

- Stammdaten von Azure Active Directory App-Registrierungen anzeigen auf Seite 257

Azure Active Directory Richtlinien zur Token-Gültigkeitsdauer

Über Azure Active Directory Richtlinien zur Token-Gültigkeitsdauer kann die Gültigkeit von Token für die Anmeldung festgelegt werden. Um für eine Azure Active Directory Anwendung eine Azure Active Directory Richtlinie zur Token-Gültigkeitsdauer zur Verfügung zu stellen, wird die Richtlinie an die Azure Active Directory Anwendung zugewiesen. Ausführliche Informationen finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

Azure Active Directory Richtlinien zur Token-Gültigkeitsdauer werden durch die Synchronisation in den One Identity Manager eingelesen und können nicht bearbeitet werden.

Um Informationen zu einer Azure Active Directory Richtlinie anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > <Ihr Mandant> > Richtlinien > Richtlinien zur Token-Gültigkeitsdauer**.
2. Wählen Sie in der Ergebnisliste die Azure Active Directory Richtlinie.
3. Wählen Sie eine der folgenden Aufgaben:

- **Überblick über die Richtlinien zur Token-Gültigkeitsdauer**: Sie erhalten einen Überblick über die Azure Active Directory Richtlinie und ihre Abhängigkeiten.
- **Stammdaten bearbeiten**: Es werden die Stammdaten für die Azure Active Directory Richtlinie angezeigt. Sie können die Stammdaten nicht bearbeiten.
    - **Anzeigename**: Anzeigename der Azure Active Directory Richtlinie.
    - **Beschreibung**: Beschreibung der Azure Active Directory Richtlinie.
    - **Definition**: Definition der Azure Active Directory Richtlinie im JSON Format.
    - **Mandant**: Azure Active Directory Mandant, zu dem die Richtlinie gehört.
    - **Standardrichtlinie**: Gibt an, ob es sich um die Standardrichtlinie des Azure Active Directory Mandanten handelt.

Verwandte Themen

- Stammdaten von Azure Active Directory App-Registrierungen anzeigen auf Seite 257

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 Azure Active Directory Benutzerkonten die nötigen Berechtigungen zum Zugriff auf die Ressourcen.

Verwandte Themen

- Managen von Azure Active Directory Benutzerkonten und Identitäten auf Seite 66
- Managen von Mitgliedschaften in Azure Active Directory Gruppen auf Seite 108
- Managen von Zuweisungen von Azure Active Directory Administratorrollen auf Seite 127
- Managen von Zuweisungen von Azure Active Directory Abonnements und Azure Active Directory Dienstplänen auf Seite 138
- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143
- Bereitstellen von Anmeldeinformationen für Azure Active Directory Benutzerkonten auf Seite 172
- Azure Active Directory Benutzerkonten erstellen und bearbeiten auf Seite 210

- Benutzeridentitäten für Azure Active Directory Benutzerkonten bereitstellen auf Seite 229
- Zusatzeigenschaften an Azure Active Directory Benutzerkonten zuweisen auf Seite 224
- Azure Active Directory Benutzerkonten deaktivieren auf Seite 225
- Azure Active Directory Benutzerkonten löschen und wiederherstellen auf Seite 226
- Überblick über Azure Active Directory Benutzerkonten anzeigen auf Seite 227
- Active Directory Benutzerkonten für Azure Active Directory Benutzerkonten anzeigen auf Seite 228
- Einzelobjekte synchronisieren auf Seite 57

Azure Active Directory Benutzerkonten erstellen und bearbeiten

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

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

HINWEIS: Sollen Identitäten ihre Benutzerkonten über Kontendefinitionen erhalten, müssen die Identitäten 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 Identität 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 Identität 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.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Benutzerkontos.
5. Speichern Sie die Änderungen.

Um ein Benutzerkonto für eine Identität manuell zuzuweisen

1. Wählen Sie im Manager die Kategorie **Identitäten > Identitäten**.
2. Wählen Sie in der Ergebnisliste die Identität.
3. Wählen Sie die Aufgabe **Azure Active Directory Benutzerkonten zuweisen**.
4. Weisen Sie ein Benutzerkonto zu.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212
- Kontaktdaten für Azure Active Directory Benutzerkonten auf Seite 220
- Informationen zum Nutzerprofil für Azure Active Directory Benutzerkonten auf Seite 221
- Organisatorische Informationen für Azure Active Directory Benutzerkonten auf Seite 221
- Informationen zum lokalen Active Directory Benutzerkonto auf Seite 222

Verwandte Themen

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 67
- Unterstützte Typen von Benutzerkonten auf Seite 98
- Bereitstellen von Anmeldeinformationen für Azure Active Directory Benutzerkonten auf Seite 172
- Managen von Azure Active Directory Benutzerkonten und Identitäten auf Seite 66
- Managen von Mitgliedschaften in Azure Active Directory Gruppen auf Seite 108
- Managen von Zuweisungen von Azure Active Directory Administratorrollen auf Seite 127
- Managen von Zuweisungen von Azure Active Directory Abonnements und Azure Active Directory Dienstplänen auf Seite 138

Allgemeine Stammdaten für Azure Active Directory Benutzerkonten

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 28: Allgemeine Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Identität	Identität, die das Benutzerkonto verwendet. • Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Identität bereits eingetragen. • Wenn Sie die automatische Identitätenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Identität gesucht und in das Benutzerkonto übernommen. • Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Identität aus der Auswahlliste wählen. In der Auswahlliste werden im Standard aktivierte und deaktivierte Identitäten angezeigt. Um deaktivierte Identitäten nicht in der Auswahlliste anzuzeigen, aktivieren Sie den Konfigurationsparameter **QER | Person| HideDeactivatedIdentities**. HINWEIS: Wenn Sie eine deaktivierte Identität an ein Benutzerkonto zuordnen, wird das Benutzerkonto, abhängig von der Konfiguration, unter Umständen gesperrt oder gelöscht. Für ein Benutzerkonto mit einer Identität vom Typ **Organisatorische Identität**, **Persönliche Administratoridentität**, **Zusatzidentität**, **Gruppenidentität** oder **Dienstidentität** können Sie eine neue Identität erstellen. Klicken Sie dafür neben dem Eingabefeld und erfassen Sie die erforderlichen Identitätenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp.
Keine Verbindung mit einer Identität erforderlich	Gibt an, ob dem Benutzerkonto absichtlich keine Identität zugeordnet ist. Die Option wird automatisch aktiviert, wenn ein Benutzerkonto in der Ausschlussliste für die automatische Identitätenzuordnung enthalten ist oder eine entsprechende Attestierung erfolgt ist. Sie können die Option manuell setzen. Aktivieren Sie die Option, falls das Benutzerkonto mit keiner Identität verbunden werden muss (beispielsweise, wenn mehrere Identitäten das Benutzerkonto verwenden).

Eigenschaft	Beschreibung
	Wenn durch die Attestierung diese Benutzerkonten genehmigt werden, werden diese Benutzerkonten künftig nicht mehr zur Attestierung vorgelegt. Im Web Portal können Benutzerkonten, die nicht mit einer Identität verbunden sind, nach verschiedenen Kriterien gefiltert werden.
Nicht mit einer Identität verbunden	Zeigt an, warum für das Benutzerkonto die Option **Keine Verbindung mit einer Identität erforderlich** aktiviert ist. Mögliche Werte sind: • **durch Administrator**: Die Option wurde manuell durch den Administrator aktiviert. • **durch Attestierung**: Das Benutzerkonto wurde attestiert. • **durch Ausschlusskriterium**: Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Identität verbunden. Das Benutzerkonto ist beispielsweise in der Ausschlussliste für die automatische Identitätenzuordnung enthalten (Konfigurationsparameter **PersonExcludeList**).
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. 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 Identität und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden. HINWEIS: Über die Aufgabe **Entferne Kontendefinition** am Benutzerkonto können Sie das Benutzerkonto wieder in den Zustand **Linked** zurücksetzen. Dabei wird die Kontendefinition vom Benutzerkonto und von der Identität entfernt. Das Benutzerkonto bleibt über diese Aufgabe erhalten, wird aber nicht mehr über die Kontendefinition verwaltet. Die Aufgabe entfernt nur Kontendefinitionen, die direkt zugewiesen sind (`XOrigin=1`).
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.

Eigenschaft	Beschreibung
Mandant	Azure Active Directory Mandant des Benutzerkontos.
Benutzertyp	Typ des Benutzerkontos. Abhängig vom Benutzertyp sind weitere Pflichtangaben erforderlich. Zulässig sind die Werte: • **Mitglied**: Normales Azure Active Directory Benutzerkonto. • **Gast**: Benutzerkonto für Gastbenutzer. Für Gastbenutzer erzeugt der Azure Active Directory Konnektor ein Benutzerkonto und sorgt dafür, dass eine Einladung an die eingetragene E-Mail-Adresse verschickt wird. Für Gastbenutzer sind zusätzliche Konfigurationen am Synchronisationsprojekt erforderlich. Weitere Informationen finden Sie unter Synchronisationsprojekte für die Einladung von Gastbenutzern anpassen auf Seite 39.
Erstellungstyp	Gibt an, durch welche Methode das Benutzerkonto erstellt wurde. Mögliche Werte sind: • **null**: Reguläres Schulkonto oder Arbeitskonto. • **Invitation**: Externes Benutzerkonto. • **LocalAccount**: Lokales Benutzerkonto für einen Azure Active Directory B2C Mandanten. • **EmailVerified**: Self-Service-Anmeldung durch einen internen Benutzer mit E-Mail-Verifizierung. • **SelfServiceSignUp**: Self-Service-Anmeldung durch einen externen Benutzer, der sich über einen Link anmeldet, der Teil eines Benutzerflusses ist.
Einladungsstatus	(Nur für Benutzertyp **Gast**) Zustimmungsstatus des eingeladenen Benutzers zur Einladung. Zulässige Werte sind: • **Annahme steht aus**: Die Zustimmung des Benutzers zur Einladung steht noch aus. • **Akzeptiert**: Die Einladung wurde vom Benutzer akzeptiert. • **Leer**: Gastbenutzer ohne Einladung.
Letzte Änderung	(Nur für Benutzertyp **Gast**) Zeitpunkt, an dem der Status der Einladung geändert wurde.
Domäne	Domäne des Benutzerkontos.
Standort	Standort, an dem das Benutzerkonto genutzt wird. Wenn Sie

Eigenschaft	Beschreibung
	im One Identity Manager Azure Active Directory Abonnements an Benutzerkonten zuweisen, wird der Standort benötigt.
Vorname	Vorname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Nachname	Nachname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Geburtstag	Geburtstag des Benutzers.
Altersgruppe	Altersgruppe des Benutzers. Zulässig sind die Werte **Minderjähriger**, **Teenager** und **Erwachsener**.
Einverständniserklärung für Minderjährige	Gibt an, ob die Einverständniserklärung für Minderjährige eingeholt wurde. Zulässig sind die Werte **Erteilt**, **Nicht erteilt** und **Nicht erforderlich**.
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.
Benutzeridentitäten	Sammlung von Identitäten, mit den sich ein Benutzer bei einem Benutzerkonto anmeldet. Weitere Informationen finden Sie unter Benutzeridentitäten für Azure Active Directory Benutzerkonten bereitstellen auf Seite 229.
Anzeigename	Anzeigename des Benutzerkontos.
Alias	E-Mail Alias für das Benutzerkonto.
E-Mail-Adresse	E-Mail-Adresse des Benutzers.
Bevorzugte Sprache	Bevorzugte Sprache des Benutzers, beispielsweise **en-US**.
Kennwort	Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Identität kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Identität finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*. Wenn Sie ein zufällig generiertes initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen.

Eigenschaft	Beschreibung
	Das Kennwort wird nach dem Publizieren in das Zielsystem aus der Datenbank gelöscht. 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	Gibt an, 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**.
Letzte Kennwortänderung	Datum der letzten Kennwortänderung. Das Datum wird aus der Azure Active Directory-Umgebung ausgelesen und kann nicht bearbeitet werden.
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 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.
Identitätstyp	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Identität. • **Organisatorische Identität**: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Identität genutzt wird. • **Zusatzidentität**: Benutzerkonto, das für einen

Eigenschaft	Beschreibung
	spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Identitäten genutzt wird. Weisen Sie alle Identitäten zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.
Privilegiertes Benutzerkonto	Gibt an, ob es sich um ein privilegiertes Benutzerkonto handelt.
Unwirksame Dienstpläne erbbar	Gibt an, ob das Benutzerkonto unwirksame Azure Active Directory Dienstpläne über die Identität erben darf. Ist die Option aktiviert, werden unwirksame Dienstpläne über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung unwirksame Dienstpläne zugewiesen haben, dann erbt das Benutzerkonto diese unwirksamen Dienstpläne. • Wenn eine Identität einen unwirksamen Dienstplan im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität diesen unwirksamen Dienstplan nur, wenn die Option aktiviert ist.
Abonnements erbbar	Gibt an, ob das Benutzerkonto Azure Active Directory Abonnements über die Identität erben darf. Ist die Option aktiviert, werden Azure Active Directory Abonnements über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Azure Active Directory Abonnements zugewiesen haben, dann erbt das Benutzerkonto diese Azure Active Directory Abonnements. • Wenn eine Identität ein Azure Active Directory Abonnement im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität dieses Azure Active Directory Abonnement nur, wenn die Option aktiviert ist.

Eigenschaft	Beschreibung
Administratorrollen erbbar	Gibt an, ob das Benutzerkonto Azure Active Directory Administratorrollen über die Identität erben darf. Ist die Option aktiviert, werden Administratorrollen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Administratorrollen zugewiesen haben, dann erbt das Benutzerkonto diese Administratorrollen. • Wenn eine Identität eine Administratorrolle im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität diese Administratorrolle nur, wenn die Option aktiviert ist.
Gruppen erbbar	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Identität erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität diese Gruppe nur, wenn die Option aktiviert ist.
Office 365 Gruppen erbbar	HINWEIS: Diese Eigenschaft ist nur verfügbar, wenn das Exchange Online Modul vorhanden ist. Gibt an, ob das Benutzerkonto Office 365 Gruppen über die verbundene Identität erben darf. Ist die Option aktiviert, werden Office 365 Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Office 365 Gruppen zugewiesen haben, dann erbt das Azure Active Directory Benutzerkonto diese Office 365 Gruppen.

Eigenschaft	Beschreibung
	• Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Azure Active Directory Benutzerkonto der Identität diese Office 365 Gruppe nur, wenn die Option aktiviert ist. Ausführliche Informationen zu Office 365 Gruppen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*.
Benutzerkonto ist deaktiviert	Gibt an, ob das Benutzerkonto deaktiviert ist. Wird ein Benutzerkonto vorübergehend nicht benötigt, können Sie das Benutzerkonto über die Option zeitweilig deaktivieren.
Ressourcenkonto	Gibt an, ob es sich bei dem Benutzerkonto um ein Ressourcenkonto handelt.

Verwandte Themen

- Benutzeridentitäten für Azure Active Directory Benutzerkonten bereitstellen auf Seite 229
- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 67
- Kennwortrichtlinien für Azure Active Directory Benutzerkonten auf Seite 172
- Azure Active Directory Benutzeridentitäten auf Seite 228
- Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 123
- Managen von Azure Active Directory Benutzerkonten und Identitäten auf Seite 66
- Unterstützte Typen von Benutzerkonten auf Seite 98
- Azure Active Directory Benutzerkonten deaktivieren auf Seite 225
- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Gruppen an Azure Active Directory Benutzerkonten auf Seite 110
- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Administratorrollen an Azure Active Directory Benutzerkonten auf Seite 129
- Voraussetzungen für indirekte Zuweisungen von Azure Active Directory Abonnements an Azure Active Directory Benutzerkonten auf Seite 146
- Voraussetzungen für indirekte Zuweisungen von unwirksamen Azure Active Directory Dienstplänen an Azure Active Directory Benutzerkonten auf Seite 160

Kontaktdaten für Azure Active Directory Benutzerkonten

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

Tabelle 29: 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 Identitäten 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.
Fax	Faxnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Weitere E-Mail-Adresse	E-Mail-Adressen des Benutzers.
Proxy Adressen	Weitere E-Mail-Adressen des Benutzers. Als Adresstyp können Sie zusätzlich zur Standardadressierung (SMTP, X400) weitere Mailkonnektoren (beispielsweise CCMail, MS) nutzen. Für die Erstellung weiterer Proxy Adressen ist die folgende Syntax einzuhalten: `Adresstyp: <E-Mail-Adresse>`

Informationen zum Nutzerprofil für Azure Active Directory Benutzerkonten

Auf dem Tabreiter **Nutzerprofil** werden folgende Informationen abgebildet.

Tabelle 30: Nutzerprofil

Eigenschaft	Beschreibung
Bevorzugter Name	Bevorzugter Name des Benutzers.
Gesetzliche Alters-gruppe	Wird verwendet von Enterprise-Anwendungen, um die gesetzliche Altersgruppe des Benutzers zu bestimmen. Diese Eigenschaft wird basierend auf den Eigenschaften **Altersgruppe** und **Einverständniserklärung für Minderjährige** berechnet.
VOIP-SIP-Adressen	Die VOIP-SIP-Adressen (Voice over IP; Session Initiation Protocol) der Chatnachricht für den Benutzer.
Persönliche Website	URL für die persönliche Webseite des Benutzers.
Über mich	Textfeld, in dem der Benutzer sich selbst beschreiben kann.
Verantwortlichkeiten	Aufzählung der Verantwortlichkeiten des Benutzers.
Schulen	Aufzählung der vom Benutzer besuchten Schulen.
Kompetenzen und Fachwissen	Aufzählung der Qualifikationen eines Benutzers.
Abgeschlossene Projekte	Aufzählung der erledigten Projekte eines Benutzers.
Interessen	Aufzählung der Interessen des Benutzers.

Organisatorische Informationen für Azure Active Directory Benutzerkonten

Auf dem Tabreiter **Organisatorisch** werden folgende organisatorische Stammdaten abgebildet.

Tabelle 31: Organisatorische Stammdaten

Eigenschaft	Beschreibung
Mitarbeiter-ID	ID des Benutzers in der Organisation. Haben Sie eine Konten-definition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.

Eigenschaft	Beschreibung
Anstellungstyp	Der Anstellungstyp des Benutzers, beispielsweise Mitarbeiter oder Lieferant.
Einstellungsdatum	(Geplantes) Datum, an dem der Benutzer in das Unternehmen eintritt.
Datum des Ausscheidens	(Geplantes) Datum, an dem der Benutzer aus dem Unternehmen ausscheidet.
Firma	Firma des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Abteilung	Abteilung des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Bereich	Bereich des Benutzers innerhalb der Abteilung.
Kostenstelle	Die dem Benutzer zugeteilte Kostenstelle.
Büro	Büro. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Berufsbezeichnung	Berufsbezeichnung. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Kontomanager	Verantwortlicher für das Benutzerkonto. ***Um einen Kontomanager festzulegen*** 1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, welche die Kontomanager abbildet. 3. Wählen Sie unter **Kontomanager** den Verantwortlichen. 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 32: Angaben zum lokalen Active Directory Benutzerkonto

Eigenschaft	Beschreibung
Synchronisation mit dem lokalen Active Directory aktiviert	Gibt an, 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	Bezeichner, mit dem die Beziehung zwischen Active Directory Benutzerkonto und Azure Active Directory Benutzerkonto aufrechterhalten wird. Der Bezeichner kann nicht geändert werden.
Definierter Name	Definierter Name des Active Directory Benutzerkontos.
Vollständiger Domänen-name	Vollständiger Domänenname der Active Directory Domäne des Benutzerkontos.
Anmeldename (pre Win2000)	Anmeldename des Active Directory Benutzerkontos für die Vorgängerversion von Active Directory.
Benutzeranmeldename (lokales Benutzerkonto)	Anmeldename des Active Directory Benutzerkontos.
Attributerweiterung 01 - Attributerweiterung 15	Zusätzliche unternehmensspezifische Informationen zum Active Directory Benutzerkonto.

Verwandte Themen

- Active Directory Benutzerkonten für Azure Active Directory Benutzerkonten anzeigen auf Seite 228
- Empfehlungen für Verbund-Umgebungen auf Seite 271

Auditdaten für Azure Active Directory Benutzerkonten

Auf dem Tabreiter **Audit** werden folgende Informationen abgebildet.

Tabelle 33: Audit

Eigenschaft	Beschreibung
Letzte nicht-interaktive Anmeldung	Zeitpunkt der letzten Anmeldung eines Benutzers im Verzeichnis mit einer nicht-interaktiven Authentifizierungsmethode.
ID der letzten nicht-interaktiven Anmeldung	ID der letzten nicht-interaktiven Anmeldung.
Letzte interaktive Anmeldung	Zeitpunkt der letzten Anmeldung eines Benutzers im Verzeichnis mit einer interaktiven Authentifizierungsmethode.
ID der letzten inter-aktiven Anmeldung	ID der letzten interaktiven Anmeldung.

Zusatzeigenschaften an Azure Active Directory Benutzerkonten zuweisen

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

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

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.

Azure Active Directory Benutzerkonten deaktivieren

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

Szenario: Die Benutzerkonten sind mit Identitäten verbunden und werden über Kontendefinitionen verwaltet.

Benutzerkonten, die über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Identität 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 Identitäten verbunden. Es sind keine Kontendefinitionen zugeordnet.

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

- Ist der Konfigurationsparameter aktiviert, werden die Benutzerkonten einer Identität deaktiviert, wenn die Identität zeitweilig oder dauerhaft deaktiviert wird.
- Ist der Konfigurationsparameter deaktiviert, haben die Eigenschaften der Identität 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: Die Benutzerkonten sind nicht mit Identitäten verbunden.

Um ein Benutzerkonto zu deaktivieren, das nicht mit einer Identität 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.

Ausführliche Informationen zum Deaktivieren und Löschen von Identitäten und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 67
- Automatisierungsgrade erstellen auf Seite 75
- Azure Active Directory Benutzerkonten löschen und wiederherstellen auf Seite 226

Azure Active Directory Benutzerkonten löschen und wiederherstellen

HINWEIS: Solange eine Kontendefinition für eine Identität wirksam ist, behält die Identität ihr daraus entstandenes Benutzerkonto. Wird die Zuweisung einer Kontendefinition entfernt, dann wird das Benutzerkonto, das aus dieser Kontendefinition entstanden ist, gelöscht. Benutzerkonten, die als **Ausstehend** markiert sind, werden nur gelöscht, wenn der Konfigurationsparameter **QER | Person | User | DeleteOptions | DeleteOutstanding** aktiviert ist.

Ein Benutzerkonto, das nicht über eine Kontendefinition entstanden ist, löschen Sie im Manager über die Ergebnisliste oder über die Menüleiste. Nach Bestätigung der Sicherheitsabfrage wird das Benutzerkonto im One Identity Manager zunächst zum Löschen markiert. Das Benutzerkonto wird im One Identity Manager gesperrt und je nach Einstellung der Löschverzögerung endgültig aus der One Identity Manager-Datenbank und aus dem Zielsystem gelöscht.

Ausführliche Informationen zum Deaktivieren und Löschen von Identitäten und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Um ein Benutzerkonto zu löschen, das nicht über eine Kontendefinition verwaltet wird

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

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

Verwandte Themen

- Azure Active Directory Benutzerkonten deaktivieren auf Seite 225
- Löschverzögerung für Azure Active Directory Benutzerkonten festlegen auf Seite 106

Überblick über Azure Active Directory Benutzerkonten anzeigen

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 im Manager 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

- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143

Active Directory Benutzerkonten für Azure Active Directory Benutzerkonten anzeigen

Das Active Directory Benutzerkonto zu einem Azure Active Directory Benutzerkonto wird auf dem Überblicksformular angezeigt.

Um das Active Directory Benutzerkonto für ein Azure Active Directory Benutzerkonto anzuzeigen

1. Wählen Sie im Manager 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**.

   Das Formularelement **Active Directory Benutzerkonto** zeigt das verbundene Benutzerkonto an.

Ausführliche Informationen zu Active Directory finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung*.

Verwandte Themen

- Informationen zum lokalen Active Directory Benutzerkonto auf Seite 222

Azure Active Directory Benutzeridentitäten

Für ein Benutzerkonto können mehrere Identitäten bereitgestellt werden, mit denen sich der Benutzer an diesem Benutzerkonto anmelden kann. Eine Identität kann beispielsweise von Microsoft, von Organisationen oder von Anbietern sozialer Identitäten wie Facebook oder Google bereitgestellt werden.

Verwandte Themen

- Benutzeridentitäten für Azure Active Directory Benutzerkonten bereitstellen auf Seite 229
- Benutzeridentitäten für Azure Active Directory Benutzerkonten anzeigen auf Seite 230
- Stammdaten von Azure Active Directory Benutzeridentitäten anzeigen auf Seite 230
- Überblick über Azure Active Directory Benutzeridentitäten anzeigen auf Seite 231

Benutzeridentitäten für Azure Active Directory Benutzerkonten bereitstellen

Azure Active Directory Benutzeridentitäten werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können weitere Benutzeridentitäten für ein Benutzerkonto erstellen oder Benutzeridentitäten löschen.

Um Benutzeridentitäten für ein Benutzerkonto zu erfassen

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. Klicken Sie neben der Eigenschaft **Benutzeridentitäten** auf  und erfassen Sie die Identitäten.

   Syntax:

   ```
   signInType=<type>;issuer=<your
   organization>.onmicrosoft.com;issuerAssignedId=<ID>
   ```

   Mit:

   - `signInType`: Anmeldetyp, beispielsweise **emailAddress** oder **userName** für lokale Benutzerkonten oder **federated** für Identitäten in sozialen Netzwerken.
   - `issuer`: Aussteller der Identität, beispielsweise `facebook.com`. Für lokale Benutzerkonten ist dies die Bezeichnung der Standarddomäne des Azure Active Directory B2C Mandanten, beispielsweise `<your organization>.onmicrosoft.com`.
   - `issuerAssignedId`: ID, mit der die Anmeldung erfolgt, abhängig vom Anmeldetyp. Wenn der Anmeldetyp **emailAddress** ist, muss die ID eine gültige E-Mail-Adresse sein. Wenn der Anmeldetyp **userName** ist, muss die ID ein gültiger lokalen Teil einer E-Mail Adresse sein. Beim Anmeldetyp **federated** wird ein eindeutige Bezeichner des Verbundkontos beim Aussteller erwartet.

   Beispiel:

   ```
   signInType=emailAddress;issuer=<your
   organization>.onmicrosoft.com;issuerAssignedId=Clara.Harris@<your domain>.com
   ```
5. Speichern Sie die Änderungen.

Um eine Benutzeridentität für ein Benutzerkonto zu löschen

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 in der Auswahlliste **Benutzeridentitäten** die Identität und klicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für Azure Active Directory Benutzerkonten auf Seite 212
- Benutzeridentitäten für Azure Active Directory Benutzerkonten anzeigen auf Seite 230
- Stammdaten von Azure Active Directory Benutzeridentitäten anzeigen auf Seite 230

Benutzeridentitäten für Azure Active Directory Benutzerkonten anzeigen

Die Benutzeridentitäten zu einem Azure Active Directory Benutzerkonto werden auf dem Überblicksformular des Benutzerkontos angezeigt.

Um einen Überblick über alle Benutzeridentitäten eines Benutzerkontos zu erhalten

1. Wählen Sie im Manager 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**.

   Das Formularelement **Azure Active Directory Benutzeridentitäten** zeigt die Benutzeridentitäten des Benutzerkontos.

Verwandte Themen

- Azure Active Directory Benutzeridentitäten auf Seite 228

Stammdaten von Azure Active Directory Benutzeridentitäten anzeigen

Die Stammdaten einer vorhandenen Benutzeridentität können Sie nicht bearbeiten. Sie können weitere Benutzeridentitäten erstellen oder Benutzeridentitäten löschen.

Um die Stammdaten einer Benutzeridentität anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Benutzerkonten > Benutzeridentitäten**.
2. Wählen Sie in der Ergebnisliste die Benutzeridentität.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Tabelle 34: Stammdaten einer Benutzeridentität

Eigenschaft	Beschreibung
Azure Active Directory Benutzerkonto	Bezeichnung des Azure Active Directory Benutzerkontos, welches die Identität verwendet.
Aussteller	Aussteller der Identität, beispielsweise `facebook.com`. Für lokale Benutzerkonten ist dies die Bezeichnung der Standarddomäne des Azure Active Directory B2C Mandanten, beispielsweise `<your organization>.onmicrosoft.com`.
Zugewiesene ID	ID, mit der die Anmeldung erfolgt, abhängig vom Anmeldetyp. Wenn der Anmeldetyp **emailAddress** ist, muss die ID eine gültige E-Mail-Adresse sein. Wenn der Anmeldetyp **userName** ist, muss die ID ein gültiger lokalen Teil einer E-Mail Adresse sein. Beim Anmeldetyp **federated** wird ein eindeutige Bezeichner des Verbundkontos beim Aussteller erwartet.
Anmeldetyp	Arten, wie sich eine Benutzer im Verzeichnis anmelden kann. Beispielsweise **emailAddress** oder **userName** für lokale Benutzerkonten oder **federated** für Identitäten in sozialen Netzwerken.

Verwandte Themen

- Benutzeridentitäten für Azure Active Directory Benutzerkonten bereitstellen auf Seite 229

Überblick über Azure Active Directory Benutzeridentitäten anzeigen

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

Um einen Überblick über eine Benutzeridentität zu erhalten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Benutzerkonten > Benutzeridentitäten**.
2. Wählen Sie in der Ergebnisliste die Benutzeridentität.

3. Wählen Sie die Aufgabe **Überblick über die Azure Active Directory Benutzeridentität**.

Verwandte Themen

- Benutzeridentitäten für Azure Active Directory Benutzerkonten anzeigen auf Seite 230

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.

Azure Active Directory 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.

HINWEIS: Zuweisungen zu Azure Active Directory Gruppen, die mit dem lokalen Active Directory synchronisiert werden, sind im One Identity Manager nicht erlaubt. Diese Gruppen können nicht über das Web Portal bestellt werden. Sie können diese Gruppen nur in Ihrer lokalen Umgebung verwalten. Ausführliche Informationen finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

Nachfolgend sind die im One Identity Manager unterstützten Gruppentypen aufgeführt.

Tabelle 35: 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. 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 nur erstellen, wenn das Exchange Online Modul vorhanden ist.

Gruppentyp	Beschreibung
	Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*.
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 Sicherheitsgruppe	E-Mail-aktivierte Sicherheitsgruppen sind Sicherheitsgruppen, die als Verteilergruppen eingesetzt werden. 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 nur erstellen, wenn das Exchange Online Modul vorhanden ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*.
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.

Verwandte Themen

- Managen von Mitgliedschaften in Azure Active Directory Gruppen auf Seite 108
- Stammdaten von Azure Active Directory Gruppen bearbeiten auf Seite 234
- Azure Active Directory Gruppen in Azure Active Directory Gruppen aufnehmen auf Seite 237
- Azure Active Directory Administratorrollen an Azure Active Directory Gruppen zuweisen auf Seite 238
- Eigentümer an Azure Active Directory Gruppen zuweisen auf Seite 239
- Zusatzeigenschaften an Azure Active Directory Gruppen zuweisen auf Seite 239
- Azure Active Directory Gruppen löschen auf Seite 240
- Überblick über Azure Active Directory Gruppen anzeigen auf Seite 240
- Active Directory Gruppen für Azure Active Directory Gruppen anzeigen auf Seite 241
- Einzelobjekte synchronisieren auf Seite 57

- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143

Stammdaten von Azure Active Directory Gruppen bearbeiten

Azure Active Directory Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können im One Identity Manager Sicherheitsgruppen erstellen. Verteilergruppen und dynamische Gruppen können Sie im One Identity Manager nicht erstellen.

E-Mail aktivierte Sicherheitsgruppen und Office 365 Gruppen können Sie im One Identity Manager nur erstellen, wenn das Exchange Online Modul vorhanden ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Exchange Online-Umgebung*

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.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Azure Active Directory Gruppen auf Seite 234
- Informationen zur lokalen Active Directory Gruppe auf Seite 237

Allgemeine Stammdaten für Azure Active Directory Gruppen

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 36: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Anzeigename	Name zur Anzeige der Gruppe in der Benutzeroberfläche der One Identity Manager-Werkzeuge.

Eigenschaft	Beschreibung
Mandant	Azure Active Directory 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. Für die Erstellung weiterer Proxy Adressen ist die folgende Syntax einzuhalten: `Adresstyp: neue E-Mail-Adresse`
Gruppentyp	Typ einer Gruppe. Für Sicherheitsgruppen und Verteilergruppen ist der Wert leer. Für Office 365 Gruppen ist der Wert **Unified** eingetragen. Für dynamische Gruppen ist der Wert **DynamicMembership** eingetragen.
Sicherheitsgruppe	Gibt an, 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	Gibt an, 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.

Zuweisbar an Administratorrollen	Gibt an, ob die Gruppe an Administratorrollen zugewiesen werden kann. Die Option kann nur beim Erstellen einer neuen Gruppe aktiviert werden.
	HINWEIS: Gruppen mit dieser Option können im Azure Active Directory nur erzeugt werden, wenn eine Azure Active Directory Premium Lizenz im Azure Active Directory Mandanten vorhanden ist. Anderenfalls kommt es zu einer Fehlermeldung:
	`Code: Authorization_RequestDenied`
	`Message: Only companies who have purchased AAD Premium may perform this operation.`

Mitgliedschaften nur lesbar	Gibt an, ob die Mitgliedschaften nur gelesen werden können, beispielsweise für dynamische Gruppen. Die Mitgliedschaften werden über das Zielsystem geregelt. Manuelle Änderungen der Mitgliedschaften im One Identity Manager sind nicht zulässig.
IT Shop	Gibt an, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal bestellt

Eigenschaft	Beschreibung
	und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Leistungsposition	Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. 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.
Mitgliedschaftsregel	Regel, nach der die Mitglieder der dynamischen Gruppe im Azure Active Directory ermittelt werden. Die Eigenschaft wird nur für Gruppen mit dem Gruppentyp **DynamicMembership** angezeigt.
Status der Mitgliedschaftsregel	Verarbeitungsstatus der Mitgliedschaftsregel für eine dynamische Gruppe. Die Eigenschaft wird nur für Gruppen mit dem Gruppentyp **DynamicMembership** angezeigt.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 123
- Azure Active Directory Administratorrollen an Azure Active Directory Gruppen zuweisen auf Seite 238
- Azure Active Directory Gruppen an Azure Active Directory Administratorrollen zuweisen auf Seite 243
- 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.

Zuweisungen zu Azure Active Directory Gruppen, die mit dem lokalen Active Directory synchronisiert werden, sind im One Identity Manager nicht erlaubt. Diese Gruppen können nicht über das Web Portal bestellt werden. Sie können diese Gruppen nur in Ihrer lokalen Umgebung verwalten. Ausführliche Informationen finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

Tabelle 37: Angaben zur lokalen Active Directory Gruppe

Eigenschaft	Beschreibung
Synchronisation mit dem lokalen Active Directory aktiviert	Gibt an, 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.

Verwandte Themen

- Active Directory Gruppen für Azure Active Directory Gruppen anzeigen auf Seite 241

Azure Active Directory Gruppen in Azure Active Directory Gruppen aufnehmen

Mit dieser Aufgabe nehmen Sie eine Gruppe in andere Gruppen auf. Damit können die Gruppen hierarchisch strukturiert werden.

Um Gruppen als Mitglieder 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. Wählen Sie den Tabreiter **Hat Mitglieder**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die untergeordneten 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 .

6. Speichern Sie die Änderungen.

Um eine Gruppe als Mitglied in andere Gruppen aufzunehmen

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. Wählen Sie den Tabreiter **Ist Mitglied in**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die übergeordneten 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 .

6. Speichern Sie die Änderungen.

Azure Active Directory Administratorrollen an Azure Active Directory Gruppen zuweisen

Diese Aufgabe ist nur für Gruppen verfügbar, für welche die Option **Zuweisbar an Administratorrollen** aktiviert ist.

Um Administratorrollen 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 **Administratorrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratorrollen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Administratorrolle und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für Azure Active Directory Gruppen auf Seite 234
- Azure Active Directory Gruppen an Azure Active Directory Administratorrollen zuweisen auf Seite 243

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 im Manager 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.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie den Eigentümer und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Zusatzeigenschaften an Azure Active Directory Gruppen zuweisen

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

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

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.

Azure Active Directory Gruppen löschen

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

Um eine Gruppe zu löschen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Überblick über Azure Active Directory Gruppen anzeigen

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 im Manager 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**.

Verwandte Themen

- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143

Active Directory Gruppen für Azure Active Directory Gruppen anzeigen

Die Active Directory Gruppe zu einer Azure Active Directory Gruppe wird auf dem Überblicksformular angezeigt.

Um die Active Directory Gruppe für eine Azure Active Directory Gruppe anzuzeigen

1. Wählen Sie im Manager 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**.

   Das Formularelement **Active Directory Gruppe** zeigt die verbundene Gruppe an.

Ausführliche Informationen zu Active Directory finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung*.

Verwandte Themen

- Informationen zur lokalen Active Directory Gruppe auf Seite 237

Azure Active Directory Administratorrollen

Mithilfe von Azure Active Directory 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.

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

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

Verwandte Themen

- Managen von Zuweisungen von Azure Active Directory Administratorrollen auf Seite 127

- Stammdaten von Azure Active Directory Administratorrollen bearbeiten auf Seite 242
- Azure Active Directory Gruppen an Azure Active Directory Administratorrollen zuweisen auf Seite 243
- Zusatzeigenschaften an Azure Active Directory Administratorrollen zuweisen auf Seite 244
- Überblick über Azure Active Directory Administratorrollen anzeigen auf Seite 245
- Einzelobjekte synchronisieren auf Seite 57

Stammdaten von Azure Active Directory Administratorrollen bearbeiten

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

Um die Stammdaten einer Azure Active Directory Administratorrolle zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für eine Administratorrolle.
5. Speichern Sie die Änderungen.

Tabelle 38: Stammdaten einer Azure Active Directory Administratorrolle

Eigenschaft	Beschreibung
Anzeigename	Anzeigename zur Anzeige der Administratorrolle in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Mandant	Azure Active Directory Mandant der Administratorrolle.
ID der Vorlage	ID der Administratorrollenvorlage auf der diese Administratorrolle basiert.
IT Shop	Gibt an, 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	Gibt an, ob die Administratorrolle ausschließlich über den IT Shop

Eigenschaft	Beschreibung
im 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	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 im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. 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 136
- 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 Gruppen an Azure Active Directory Administratorrollen zuweisen

Es können nur Gruppen zugewiesen werden, für welche die Option **Zuweisbar an Administratorrollen** aktiviert ist.

Um Gruppen an eine Administratorrolle zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Administratorrollen**.
2. Wählen Sie in der Ergebnisliste die Administratorrolle.

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

- Allgemeine Stammdaten für Azure Active Directory Gruppen auf Seite 234
- Azure Active Directory Administratorrollen an Azure Active Directory Gruppen zuweisen auf Seite 238

Zusatzeigenschaften an Azure Active Directory Administratorrollen zuweisen

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

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

Um Zusatzeigenschaften für eine Administratorrolle festzulegen

1. Wählen Sie im Manager 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.

Überblick über Azure Active Directory Administratorrollen anzeigen

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 im Manager 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**.

Azure Active Directory Verwaltungseinheiten

Azure Active Directory ermöglicht die Erstellung und Verwaltung von Verwaltungseinheiten. Durch Verwaltungseinheiten können Sie Rollenberechtigungen in den von Ihnen definierten Bereichen Ihrer Organisation steuern und einschränken. Mithilfe einer Verwaltungseinheit können Sie Geräte, Nutzer und Gruppen verwalten.

Weitere Informationen finden Sie unter Benutzerkonten erstellen und bearbeiten und Stammdaten von Azure Active Directory Gruppen bearbeiten.

Um eine Verwaltungseinheit zu erstellen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Verwaltungseinheiten**.
2. Klicken Sie in der Ergebnisliste  .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Verwaltungseinheit.
4. Speichern Sie die Änderungen.

Stammdaten von Verwaltungseinheiten bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Mandanten > Verwaltungseinheiten**.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Verwaltungseinheit.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von Verwaltungseinheiten bearbeiten
- Benutzerkonten an Verwaltungseinheiten zuweisen
- Gruppen an Verwaltungseinheiten zuweisen

Stammdaten von Verwaltungseinheiten bearbeiten

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 39: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Mandant	Azure Active Directory Mandant der Verwaltungseinheit.
Anzeigename	Anzeigename zur Anzeige der Verwaltungseinheit in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Sichtbarkeit	Legt fest, für welche Nutzer die Verwaltungseinheit sichtbar ist.

Verwandte Themen

- Azure Active Directory Verwaltungseinheiten
- Gruppen an Verwaltungseinheiten zuweisen
- Benutzerkonten an Verwaltungseinheiten zuweisen

Benutzerkonten an Verwaltungseinheiten zuweisen

Weisen Sie Benutzerkonten an Verwaltungseinheiten zu, um die Rollenberechtigungen dieser Benutzerkonten über die Verwaltungseinheit zu verwalten.

Um Benutzerkonten direkt an eine Verwaltungseinheit zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Verwaltungseinheiten**.
2. Wählen Sie in der Ergebnisliste die Verwaltungseinheit.
3. 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 .

4. Speichern Sie die Änderungen.

Verwandte Themen

- Azure Active Directory Verwaltungseinheiten
- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 67
- Gruppen an Verwaltungseinheiten zuweisen

Gruppen an Verwaltungseinheiten zuweisen

Weisen Sie Gruppen an Verwaltungseinheiten zu, um die Rollenberechtigungen dieser Gruppen über die Verwaltungseinheit zu verwalten.

Um Gruppen direkt an eine Verwaltungseinheit zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Verwaltungseinheiten.**
2. Wählen Sie in der Ergebnisliste die Verwaltungseinheit.
3. 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 .

4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Azure Active Directory Verwaltungseinheiten
- Azure Active Directory Gruppen
- Allgemeine Stammdaten für Azure Active Directory Gruppen auf Seite 234

Azure Active Directory Abonnements und Azure Active Directory Dienstpläne

Die Informationen zu Azure Active Directory Abonnements und Azure Active Directory Dienstplänen innerhalb eines Azure Active Directory Mandanten werden durch die Synchronisation in den One Identity Manager eingelesen. Neue Azure Active Directory Abonnements und Azure Active Directory Dienstpläne können Sie im One Identity Manager nicht erstellen. Sie können im One Identity Manager einzelne Stammdaten der Azure Active Directory Abonnements für die Bestellung im IT Shop und die Zuweisung an Benutzerkonten bearbeiten.

HINWEIS: Ein Azure Active Directory Benutzerkonto kann Azure Active Directory Abonnements zusätzlich über seine Azure Active Directory Gruppen erhalten. Die Zuweisungen über Azure Active Directory Gruppen können in One Identity Manager nicht bearbeitet werden.

Verwandte Themen

- Managen von Zuweisungen von Azure Active Directory Abonnements und Azure Active Directory Dienstplänen auf Seite 138
- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143
- Stammdaten von Azure Active Directory Abonnements bearbeiten auf Seite 248
- Zusatzeigenschaften an Azure Active Directory Abonnements zuweisen auf Seite 250
- Überblick über Azure Active Directory Abonnements und Dienstpläne anzeigen auf Seite 251
- Einzelobjekte synchronisieren auf Seite 57
- Unwirksame Azure Active Directory Dienstpläne auf Seite 251

Stammdaten von Azure Active Directory Abonnements bearbeiten

Um die Stammdaten eines Azure Active Directory Abonnements zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Abonnements**.
2. Wählen Sie in der Ergebnisliste das Azure Active Directory Abonnement.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Azure Active Directory Abonnements.
5. Speichern Sie die Änderungen.

Tabelle 40: Stammdaten eines Azure Active Directory Abonnements

Eigenschaft	Beschreibung
SKU Anzeigename	SKU Anzeigename des Azure Active Directory Abonnements, beispielsweise AAD_Premium oder RMSBASIC.
Mandant	Mandant, zu dem dieses Azure Active Directory Abonnement eingetragen ist.
Abonnementstatus	Angabe des Status des Azure Active Directory 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	Gibt an, ob das Azure Active Directory Abonnement über den IT Shop bestellbar ist. Das Azure Active Directory Abonnement kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Das Azure Active Directory Abonnement kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob das Azure Active Directory Abonnement ausschließlich über den IT Shop bestellbar ist. Das Azure Active Directory Abonnement kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung des Azure Active Directory Abonnements an hierarchische Rollen ist nicht zulässig.
Leistungsposition	Leistungsposition, um das Azure Active Directory Abonnement über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen des Azure Active Directory Abonnement an Azure Active Directory Benutzerkonten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen.*
Kategorie	Kategorien für die Vererbung von Azure Active Directory Abonnements. Azure Active Directory Abonnements können selektiv an Azure Active Directory Benutzerkonten vererbt werden. Dazu

Eigenschaft	Beschreibung
	werden die Azure Active Directory Abonnements und die Azure Active Directory Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie das Azure Active Directory Abonnement einer oder mehreren Kategorien zu.

Verwandte Themen

- Vererbung von Azure Active Directory Gruppen anhand von Kategorien auf Seite 123
- Ausführliche Informationen zur Vorbereitung der Abonnements für die Bestellung über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Zusatzeigenschaften an Azure Active Directory Abonnements zuweisen

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

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

Um Zusatzeigenschaften für ein Azure Active Directory Abonnement festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Abonnements**.
2. Wählen Sie in der Ergebnisliste das Azure Active Directory 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.

Überblick über Azure Active Directory Abonnements und Dienstpläne anzeigen

Über diese Aufgaben erhalten Sie einen Überblick über die wichtigsten Informationen zu einem Azure Active Directory Abonnements und einem Dienstplan.

Um einen Überblick über ein Azure Active Directory Abonnement zu erhalten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Abonnements**.
2. Wählen Sie in der Ergebnisliste das Azure Active Directory Abonnement.
3. Wählen Sie die Aufgabe **Überblick über das Azure Active Directory Abonnement**.

Um einen Überblick über einen Azure Active Directory Dienstplan zu erhalten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den Azure Active Directory Dienstplan.
3. Wählen Sie die Aufgabe **Überblick über den Azure Active Directory Dienstplan**.

Verwandte Themen

- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143

Unwirksame Azure Active Directory Dienstpläne

Um für die Benutzer die Nutzung einzelner Azure Active Directory Dienstpläne zu unterbinden, werden im One Identity Manager zusätzlich sogenannte "unwirksame Dienstpläne" abgebildet. Unwirksame Dienstpläne werden nach der Synchronisation der Azure Active Directory 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.

HINWEIS: Ein Azure Active Directory Benutzerkonto kann unwirksamen Dienstpläne zusätzlich über seine Azure Active Directory Gruppen erhalten. Die Zuweisungen über Azure Active Directory Gruppen können in One Identity Manager nicht bearbeitet werden.

Verwandte Themen

- Managen von Zuweisungen von Azure Active Directory Abonnements und Azure Active Directory Dienstplänen auf Seite 138

- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143
- Stammdaten von unwirksamen Azure Active Directory Dienstplänen bearbeiten auf Seite 252
- Zusatzeigenschaften an unwirksame Azure Active Directory Dienstpläne zuweisen auf Seite 253
- Überblick über unwirksame Azure Active Directory Dienstpläne anzeigen auf Seite 254
- Einzelobjekte synchronisieren auf Seite 57

Stammdaten von unwirksamen Azure Active Directory Dienstplänen bearbeiten

Um die Stammdaten eines unwirksamen Azure Active Directory Dienstplans zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den unwirksamen Dienstplan.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des unwirksamen Dienstplans.
5. Speichern Sie die Änderungen.

Tabelle 41: Stammdaten eines unwirksamen Dienstplans

Eigenschaft	Beschreibung
Abonnement	Bezeichnung des Azure Active Directory Abonnements.
Dienstplan	Bezeichnung des Azure Active Directory Dienstplans.
IT Shop	Gibt an, 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	Gibt an, 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

Eigenschaft	Beschreibung
	zulässig.
Leistungsposition	Leistungsposition, um den unwirksamen Dienstplan über den IT Shop zu bestellen.
Kategorie	Kategorien für die Vererbung von unwirksamen Dienstplänen. Unwirksame Dienstpläne können selektiv an Azure Active Directory Benutzerkonten vererbt werden. Dazu werden die unwirksamen Dienstpläne und die Azure Active Directory 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 123
- Ausführliche Informationen zur Vorbereitung der Dienstpläne für die Bestellung über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Zusatzeigenschaften an unwirksame Azure Active Directory Dienstpläne zuweisen

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

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

Um Zusatzeigenschaften für einen unwirksamen Azure Active Directory Dienstplan festzulegen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den unwirksamen 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.

Überblick über unwirksame Azure Active Directory Dienstpläne anzeigen

Über diese Aufgabe erhalten Sie einen Überblick über die wichtigsten Informationen zu einem unwirksamen Azure Active Directory Dienstplan.

Um einen Überblick über einen unwirksamen Azure Active Directory Dienstpläne zu erhalten

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Unwirksame Dienstpläne**.
2. Wählen Sie in der Ergebnisliste den unwirksamen Dienstplan.
3. Wählen Sie die Aufgabe **Überblick über den unwirksamen Azure Active Directory Dienstplan**.

Verwandte Themen

- Wirksame und unwirksame Azure Active Directory Dienstpläne für Azure Active Directory Benutzerkonten und Azure Active Directory Gruppen anzeigen auf Seite 143

Azure Active Directory App-Registierungen und Azure Active Directory Dienstprinzipale

Bei der Registrierung einer Anwendung in einem Azure Active Directory Mandanten wird ein dazugehöriger Azure Active Directory Dienstprinzipal erzeugt. Für App-Registrierungen sind sogenannte App-Rollen definiert. Über die App-Rollen können den Azure Active Directory Benutzern, Azure Active Directory Gruppen oder Azure Active Directory Dienstprinizipalen Berechtigungen oder Funktionen für die Anwendung zur Verfügung gestellt werden.

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

Die Informationen zu Azure Active Directory App-Registrierungen, Azure Active Directory Dienstprinzipalen und App-Rollen innerhalb eines Azure Active Directory Mandanten werden durch die Synchronisation in den One Identity Manager eingelesen.

Wird eine Azure Active Directory Anwendung in einem Azure Active Directory Mandanten genutzt, die in einem anderen Azure Active Directory Mandanten registriert ist, wird nur der Azure Active Directory Dienstprinzipal jedoch nicht die Azure Active Directory App-Registrierung in den One Identity Manager eingelesen.

Neue Azure Active Directory App-Registrierungen, Azure Active Directory Dienstprinzipale und App-Rollen können Sie im One Identity Manager nicht erstellen. Im One Identity Manager können Sie Eigentümer für App-Registrierungen und Dienstprinzipale festlegen und Zuweisungen zu den App-Rollen erstellen oder entfernen.

Detaillierte Informationen zum Thema

- Informationen über Azure Active Directory App-Registrierungen anzeigen auf Seite 255
- Eigentümer an Azure Active Directory App-Registrierungen zuweisen auf Seite 256
- Stammdaten von Azure Active Directory App-Registrierungen anzeigen auf Seite 257
- Informationen über Azure Active Directory Dienstprinzipale anzeigen auf Seite 258
- Eigentümer an Azure Active Directory Dienstprinzipale zuweisen auf Seite 259
- Autorisierungen für Azure Active Directory Dienstprinzipale bearbeiten auf Seite 260
- Azure Active Directory Dienstprinzipale für Unternehmensanwendungen anzeigen auf Seite 261
- Stammdaten von Azure Active Directory Dienstprinzipalen anzeigen auf Seite 262

Informationen über Azure Active Directory App-Registrierungen anzeigen

Die Informationen zu Azure Active Directory App-Registrierungen werden durch die Synchronisation in den One Identity Manager eingelesen. Für einen Azure Active Directory Mandanten werden alle Azure Active Directory App-Registrierungen mit ihren Azure Active Directory Dienstprinzipalen eingelesen, die in diesem Azure Active Directory Mandanten registriert sind.

Wird eine Azure Active Directory Anwendung in einem Azure Active Directory Mandanten genutzt, die in einem anderen Azure Active Directory Mandanten registriert ist, wird nur der Azure Active Directory Dienstprinzipal jedoch nicht die Azure Active Directory App-Registrierung in den One Identity Manager eingelesen.

Neue Azure Active Directory App-Registrierungen können Sie im One Identity Manager nicht erstellen.

Um Informationen zu einer Azure Active Directory App-Registrierung anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > App-Registrierungen**.

2. Wählen Sie in der Ergebnisliste die Azure Active Directory App-Registrierung.
3. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über die Azure Active Directory App-Registrierung**: Sie erhalten einen Überblick über die Azure Active Directory App-Registrierung und ihre Abhängigkeiten.
    - **Stammdaten bearbeiten**: Es werden die Stammdaten für die Azure Active Directory App-Registrierung angezeigt.
    - **Eigentümer zuweisen**: Es werden die Eigentümer der Azure Active Directory App-Registrierung angezeigt. Sie können Eigentümer zu einer App-Registrierung zuweisen oder von einer App-Registrierung entfernen.

Verwandte Themen

- Eigentümer an Azure Active Directory App-Registrierungen zuweisen auf Seite 256
- Stammdaten von Azure Active Directory App-Registrierungen anzeigen auf Seite 257
- Informationen über Azure Active Directory Dienstprinzipale anzeigen auf Seite 258
- Azure Active Directory Dienstprinzipale für Unternehmensanwendungen anzeigen auf Seite 261

Eigentümer an Azure Active Directory App-Registrierungen zuweisen

Über diese Aufgabe können Sie Eigentümer zu einer Azure Active Directory App-Registrierung zuweisen oder von einer Azure Active Directory App-Registrierung entfernen. Eigentümer einer Azure Active Directory App-Registrierung können die App-Registrierungen im Azure Active Directory anzeigen und bearbeiten.

Um Eigentümer an eine Azure Active Directory App-Registrierung zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > App-Registrierungen**.
2. Wählen Sie in der Ergebnisliste die Azure Active Directory App-Registrierung.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie in der Auswahlliste **Tabelle** den Eintrag **Azure Active Directory Benutzerkonten (AADUser)**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Eigentümer zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie den Eigentümer und doppelklicken Sie .

6. Speichern Sie die Änderungen.

Stammdaten von Azure Active Directory App-Registrierungen anzeigen

Die Informationen zu Azure Active Directory App-Registrierungen werden durch die Synchronisation in den One Identity Manager eingelesen. Die Stammdaten einer Azure Active Directory App-Registrierung können Sie nicht bearbeiten.

Um die Stammdaten einer Azure Active Directory App-Registrierung anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > App-Registrierungen**.
2. Wählen Sie in der Ergebnisliste die Azure Active Directory App-Registrierung.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Tabelle 42: Stammdaten einer Azure Active Directory App-Registrierung

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der Anwendung.
Domäne des Herausgebers	Bezeichnung der verifizierten Domäne des Herausgebers der Anwendung.
Datum der Registrierung	Datum und Zeit der Registrierung der Anwendung.
Gruppenansprüche	Gruppenansprüche, die die Anwendung erwartet. Gruppentypen, die in Zugriffs-, ID- und SAML-Token eingeschlossen werden. Zulässige Werte sind: • **Keine**: Keine Gruppentypen • **Alle**: Alle Gruppentypen. • **Sicherheitsgruppen**: Sicherheitsgruppen, in denen der Benutzer Mitglied ist. • **Anwendungsgruppen**: Anwendungsgruppen, in denen der Benutzer Mitglied ist. • **Verzeichnisrollen**: Verzeichnisrollen, die dem Benutzer zugewiesen sind.
URL des Logos	Link zum Anwendungslogo.

Eigenschaft	Beschreibung
Marketing URL	Link zur Marketingseite der Anwendung.
URL der Datenschutzerklärung	Link zur Datenschutzerklärung der Anwendung.
Service URL	Link zur Supportseite der Anwendung.
URL zu den Vertragsbedingungen	Link zu den Vertragsbedingungen der Anwendung.
Fallback öffentlicher Client	Gibt an, ob der Fallback-Anwendungstyp ein öffentlicher Client ist, zum Beispiel eine installierte Anwendung, die auf einem mobilen Gerät läuft. Ist die Option deaktiviert, bedeutet dies, dass der Fallback-Anwendungstyp ein vertraulicher Client ist, wie zum Beispiel eine Webanwendung (Standard).
Unterstützte Benutzerkonten	Gibt an, welche Microsoft Benutzerkonten für die aktuelle Anwendung unterstützt werden. Zulässige Werte sind: • Nur Konten in diesem Organisationsverzeichnis • Konten in einem beliebigen Organisationsverzeichnis • Konten in einem beliebigen Organisationsverzeichnis und persönliche Microsoft Konten • Nur persönliche Microsoft Konten
Richtlinie zur Token-Ausstellung	Bezeichnung der Richtlinie für die Ausstellung von Token.
Richtlinie zur Token-Gültigkeitsdauer	Bezeichnung der Richtlinie für die Gültigkeitsdauer von Token.
Schlagworte	Benutzerdefinierte Zeichenfolgen, die zur Kategorisierung und Identifizierung der Anwendung verwendet werden können.

Verwandte Themen

- Azure Active Directory Richtlinien zur Token-Ausstellung auf Seite 207
- Azure Active Directory Richtlinien zur Token-Gültigkeitsdauer auf Seite 208

Informationen über Azure Active Directory Dienstprinzipale anzeigen

Bei der Registrierung einer Anwendung in einem Azure Active Directory Mandanten im Microsoft Azure Management Portal wird ein dazugehöriger Azure Active Directory Dienstprinzipal erzeugt.

Die Informationen zu Azure Active Directory Dienstprinzipalen werden durch die Synchronisation in den One Identity Manager eingelesen. Neue Azure Active Directory Dienstprinzipale können Sie im One Identity Manager nicht erstellen.

Wird eine Azure Active Directory Anwendung in einem Azure Active Directory Mandanten genutzt, die in einem anderen Azure Active Directory Mandanten registriert ist, wird nur der Azure Active Directory Dienstprinzipal jedoch nicht die Azure Active Directory App-Registrierung in den One Identity Manager eingelesen.

Um Informationen zu einem Azure Active Directory Dienstprinzipal anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Dienstprinzipale**.
2. Wählen Sie in der Ergebnisliste den Azure Active Directory Dienstprinizipal.
3. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über den Azure Active Directory Dienstprinizipal**: Sie erhalten einen Überblick über den Azure Active Directory Dienstprinizipal und seine Abhängigkeiten.
    - **Stammdaten bearbeiten**: Es werden die Stammdaten für den Azure Active Directory Dienstprinizipal angezeigt.
    - **Eigentümer zuweisen**: Es werden die Eigentümer des Azure Active Directory Dienstprinizipals angezeigt. Sie können Eigentümer zu einem Dienstprinizipal zuweisen oder von einem Dienstprinizipal entfernen.
    - **Autorisierungen zuweisen**: Es werden die Benutzerkonten, Gruppen und Dienstprinizipale mit ihren zugewiesenen App-Rollen angezeigt. Sie können weitere Autorisierungen erstellen oder Autorisierungen entfernen.

Verwandte Themen

- Eigentümer an Azure Active Directory Dienstprinzipale zuweisen auf Seite 259
- Autorisierungen für Azure Active Directory Dienstprinzipale bearbeiten auf Seite 260
- Stammdaten von Azure Active Directory Dienstprinzipalen anzeigen auf Seite 262
- Informationen über Azure Active Directory App-Registrierungen anzeigen auf Seite 255
- Azure Active Directory Dienstprinzipale für Unternehmensanwendungen anzeigen auf Seite 261

Eigentümer an Azure Active Directory Dienstprinzipale zuweisen

Über diese Aufgabe können Sie Eigentümer zu einem Azure Active Directory Dienstprinzipal zuweisen oder von einem Dienstprinzipal entfernen.

Um Eigentümer an eine Azure Active Directory Anwendung zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Dienstprinzipale**.
2. Wählen Sie in der Ergebnisliste den Azure Active Directory Dienstprinizipal.
3. Wählen Sie die Aufgabe **Eigentümer zuweisen**.
4. Wählen Sie in der Auswahlliste **Tabelle** einen der folgenden Einträge:
    - **Azure Active Directory Benutzerkonten (AADUser)**
    - **Azure Active Directory Dienstprinzipal (AADServicePrincipal)**
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Eigentümer zu.

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

    Um eine Zuweisung zu entfernen

    - Wählen Sie den Eigentümer und doppelklicken Sie .
6. Speichern Sie die Änderungen.

Autorisierungen für Azure Active Directory Dienstprinzipale bearbeiten

Für App-Registierungen sind sogenannte App-Rollen definiert. Über die App-Rollen können den Azure Active Directory Benutzern, Azure Active Directory Gruppen oder Azure Active Directory Dienstprinizipalen Berechtigungen oder Funktionen für die Anwendung zur Verfügung gestellt werden.

App-Rollen und ihre Zuweisungen werden durch die Synchronisation in den One Identity Manager eingelesen. Neue App-Rollen können Sie im One Identity Manager nicht erstellen. Sie können im One Identity Manager Autorisierungen für die Dienstprinzipale und somit für ihre App-Registierungen erstellen oder entfernen.

Um Autorisierungen an einen Azure Active Directory Dienstprinzipal zuzuweisen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Dienstprinzipale**.
2. Wählen Sie in der Ergebnisliste den Azure Active Directory Dienstprinizipal.
3. Wählen Sie die Aufgabe **Autorisierungen zuweisen**.
4. Klicken Sie im Bereich **Zuweisungen** die Schaltfläche **Hinzufügen** und erfassen Sie folgende Daten.
    - **Autorisiert für**: Legen Sie das Benutzerkonto, die Gruppe oder den Dienstprinzipal für die Autorisierung fest.

a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.

b. Wählen Sie unter **Tabelle** eine der folgenden Tabellen:

- Um ein Benutzerkonto zu berechtigen, wählen Sie **AADUser**.
- Um eine Gruppe zu berechtigen, wählen Sie **AADGroup**.
- Um ein Dienstprinzipal zu berechtigen, wählen Sie **AADServicePrincipal**.

c. Wählen Sie unter **Autorisiert für** das Benutzerkonto, die Gruppe oder den Dienstprinzipal.

d. Klicken Sie **OK**.

- **App-Rolle**: Wählen Sie die App-Rolle für die Autorisierung.

  HINWEIS: Ist für einen Dienstprinzipal keine App-Rolle definiert, lassen Sie die Auswahl leer um das Benutzerkonto, die Gruppe oder den Dienstprinizipal zu autorisieren.

5. Speichern Sie die Änderungen.

Um Autorisierungen von einem Azure Active Directory Dienstprinzipal zu entfernen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Dienstprinzipale**.
2. Wählen Sie in der Ergebnisliste den Azure Active Directory Dienstprinizipal.
3. Wählen Sie die Aufgabe **Autorisierungen zuweisen**.
4. Wählen Sie im Bereich **Zuweisungen** die Autorisierung, die Sie entfernen möchten.
5. Klicken Sie die Schaltfläche **Entfernen**.
6. Speichern Sie die Änderungen.

Azure Active Directory Dienstprinzipale für Unternehmensanwendungen anzeigen

Mit dieser Aufgabe können Sie die Dienstprinzipale anzeigen, die Unternehmensanwendungen repräsentieren.

Um Unternehmensanwendungen anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Dienstprinzipale**.
2. Wählen Sie einen der folgenden Einträge:
   - **Nach Typ > Anwendungen > Unternehmensanwendungen**.
   - **Nach Typ > Legacy > Unternehmensanwendungen**.
3. Wählen Sie in der Ergebnisliste den Azure Active Directory Dienstprinizipal.

4. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über den Azure Active Directory Dienstprinizipal**: Sie erhalten einen Überblick über den Azure Active Directory Dienstprinizipal und seine Abhängigkeiten.
    - **Stammdaten bearbeiten**: Es werden die Stammdaten für den Azure Active Directory Dienstprinizipal angezeigt.
    - **Eigentümer zuweisen**: Es werden die Eigentümer des Azure Active Directory Dienstprinizipals angezeigt. Sie können Eigentümer zu einem Dienstprinizipal zuweisen oder von einem Dienstprinizipal entfernen.
    - **Autorisierungen zuweisen**: Es werden die Benutzerkonten, Gruppen und Dienstprinizipale mit ihren zugewiesenen App-Rollen angezeigt. Sie können weitere Autorisierungen erstellen oder Autorisierungen entfernen.

Verwandte Themen

- Stammdaten von Azure Active Directory Dienstprinzipalen anzeigen auf Seite 262
- Eigentümer an Azure Active Directory Dienstprinzipale zuweisen auf Seite 259
- Autorisierungen für Azure Active Directory Dienstprinzipale bearbeiten auf Seite 260
- Informationen über Azure Active Directory Dienstprinzipale anzeigen auf Seite 258

Stammdaten von Azure Active Directory Dienstprinzipalen anzeigen

Die Informationen zu Azure Active Directory Dienstprinzipalen werden durch die Synchronisation in den One Identity Manager eingelesen. Die Stammdaten eines Azure Active Directory Dienstprinzipals können Sie nicht bearbeiten.

Um die Stammdaten eines Azure Active Directory Dienstprinzipals anzuzeigen

1. Wählen Sie im Manager die Kategorie **Azure Active Directory > Dienstprinzipale**
2. Wählen Sie in der Ergebnisliste den Azure Active Directory Dienstprinzipal.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Tabelle 43: Stammdaten eines Azure Active Directory Dienstprinzipals

Eigenschaft	Beschreibung
Anzeigename	Anzeigename des Dienstprinzipals.
Alternative Bezeich-nungen	Alternative Bezeichnung. Diese werden zum Abrufen von Dienstprinzipalen per Abonnement, zur Identifizierung von Ressourcengruppen und vollständigen Ressourcen-IDs für verwaltete Identitäten verwendet.

Eigenschaft	Beschreibung
Webseite	Startseite der Azure Active Directory Anwendung.
Aktiviert	Gibt an, ob der Dienstprinzipal aktiviert ist.
Anzeigename der Anwendung	Anzeigename der zugehörigen Azure Active Directory Anwendung.
App-Rollenzuweisung erforderlich	Gibt an, ob Benutzern oder anderen Dienstprinzipalen eine App-Rollenzuweisung für diesen Dienstprinzipal erteilt werden muss, bevor Benutzer sich anmelden oder Anwendungen Token erhalten können.
URL des Logos	Link zum Anwendungslogo.
Marketing URL	Link zur Marketingseite der Anwendung.
URL der Datenschutzerklärung	Link zur Datenschutzerklärung der Anwendung.
Service URL	Link zur Supportseite der Anwendung.
URL zu den Vertragsbedingungen	Link zu den Vertragsbedingungen der Anwendung.
Anmelde-URL	URL, unter der der Identitätsanbieter den Benutzer zur Authentifizierung zu Azure Active Directory umleitet.
Abmelde-URL	URL, die vom Autorisierungsdienst von Microsoft verwendet wird, um einen Benutzer mithilfe von OpenID Connect front-channel, OpenID Connect back-channel oder SAML-Abmeldeprotokollen abzumelden.
E-Mail-Adressen für Benachrichtigungen	Liste der E-Mail-Adressen an, an die Azure Active Directory eine Benachrichtigung sendet, wenn sich das aktive Zertifikat dem Ablaufdatum nähert.
Bevorzugter Single Sign-On Modus	Modus für das Single Sign-On, der für diese Azure Active Directory Anwendung konfiguriert ist.
Antwort-URLs	URLs, an die Benutzertoken zur Anmeldung bei der verknüpften Anwendung gesendet werden, oder die Umleitungs-URIs, an die die OAuth 2.0-Autorisierungscodes und Zugriffstoken für die verknüpfte Anwendung gesendet werden.
Namen des Dienstprinzipals	Liste der URIs, die die zugehörige Azure Active Directory Anwendung innerhalb ihres Azure Active Directory Mandanten oder innerhalb einer verifizierten benutzerdefinierten Domäne identifizieren, wenn es sich um eine Azure Active Directory Anwendung für mehrere Azure Active Directory Mandanten handelt.

Eigenschaft	Beschreibung
Typ des Dienstprinzipals	Typ des Dienstprinzipal beispielsweise eine Anwendung oder eine verwaltete Identität. Der Typ wird intern von Azure Active Directory festgelegt.
Schlüssel-ID zur Verschlüsselung	ID des öffentlichen Schlüssels zur Anmeldung über Zertifikate.
Richtlinie zur Startbereichsermittlung	Bezeichnung der Richtlinie zur Startbereichsermittlung.
Datum der Löschung	Zeitpunkt, an dem der Dienstprinzipal gelöscht wurde.
Schlagworte	Benutzerdefinierte Zeichenfolgen, die zur Kategorisierung und Identifizierung der Anwendung verwendet werden können.

Verwandte Themen

- Azure Active Directory Richtlinien zur Startbereichsermittlung auf Seite 206

Berichte über Azure Active Directory Objekte

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 44: Berichte zur Datenqualität eines Zielsystems

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Herkunft)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die Herkunft der zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Historie)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto einschließlich eines historischen Verlaufs.

Bericht	Bereitgestellt für	Beschreibung
		Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Überblick über die Lizenz	Benutzerkonto	Der Bericht enthält eine Zusammenfassung der zugewiesenen und effektiven Abonnements und Dienstpläne für ein Benutzerkonto.
Überblick über die Lizenz	Abonnement	Der Bericht zeigt einen Überblick über die Lizenz eines Abonnements. Es wird angezeigt, an welche Gruppen und Benutzerkonten das Abonnement zugewiesen ist und welche Dienstpläne für die Gruppen und die Benutzerkonten effektiv wirken.
Übersicht aller Zuweisungen	Gruppe Abonnement Administratorrolle	Der Bericht ermittelt alle Rollen, in denen sich Identitäten befinden, welche die ausgewählte Systemberechtigung besitzen.
Übersicht anzeigen	Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre Zuweisungen.
Übersicht anzeigen (inklusive Herkunft)	Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Abweichende Systemberechtigungen anzeigen	Mandant	Der Bericht enthält alle Systemberechtigungen, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über

Bericht	Bereitgestellt für	Beschreibung
		den One Identity Manager.
Benutzerkonten anzeigen (inklusive Historie)	Mandant	Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten mit einer überdurch-schnittliche Anzahl an Systemberechtigungen anzeigen	Mandant	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
Identitäten mit mehreren Benut-zerkonten anzeigen	Mandant	Der Bericht zeigt alle Identitäten, die mehrere Benutzerkonten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Systemberechtigungen anzeigen (inklusive Historie)	Mandant	Der Bericht zeigt die Systemberechtigungen mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Mandant	Der Bericht ermittelt alle Rollen, in denen sich Identitäten befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.
Ungenutzte Benut-zerkonten anzeigen	Mandant	Der Bericht enthält alle Benutzerkonten, die in den letzten Monaten nicht verwendet wurden.
Unverbundene Benut-zerkonten anzeigen	Mandant	Der Bericht zeigt alle Benutzerkonten, denen keine Identität zugeordnet ist.

Tabelle 45: Zusätzliche Berichte für das Zielsystem

Bericht	Beschreibung
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**.

10

Behandeln von Azure Active Directory Objekten im Web Portal

Der One Identity Manager bietet seinen Benutzern die Möglichkeit, verschiedene Aufgaben unkompliziert über ein Web Portal zu erledigen.

- Managen von Benutzerkonten und Identitäten

  Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann die Kontendefinition von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Identität, beispielsweise einen Manager, wird das Benutzerkonto angelegt.

- Managen von Zuweisungen von Gruppen, Administratorrollen, Abonnements und unwirksamen Dienstplänen

  Mit der Zuweisung von Gruppen, Administratorrollen, Abonnements und unwirksamen Dienstplänen an ein IT Shop Regal können diese Produkte von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Identität wird die Gruppe, die Administratorrolle, das Abonnement oder der unwirksame Dienstplan zugewiesen.

  Im IT Shop sind die Regale **Identity & Access Lifecycle > Azure Active Directory Gruppen**, **Identity & Access Lifecycle > Azure Active Directory Abonnements** und **Identity & Access Lifecycle > Unwirksame Azure Active Directory Dienstpläne** vorhanden.

  Manager und Administratoren von Organisationen können im Web Portal Gruppen, Administratorrollen, Abonnements und unwirksame Dienstpläne an die Abteilungen, Kostenstellen oder Standorte zuweisen, für die sie verantwortlich sind. Die Gruppen, Administratorrollen, Abonnements und unwirksamen Dienstpläne werden an alle Identitäten vererbt, die Mitglied dieser Abteilungen, Kostenstellen oder Standorte sind.

  Wenn das Geschäftsrollenmodul vorhanden ist, können Manager und Administratoren von Geschäftsrollen im Web Portal Gruppen, Administratorrollen,

Abonnements und unwirksame Dienstpläne an die Geschäftsrollen zuweisen, für die sie verantwortlich sind. Die Gruppen, Administratorrollen, Abonnements und unwirksame Dienstpläne werden an alle Identitäten vererbt, die Mitglied dieser Geschäftsrollen sind.

Wenn das Systemrollenmodul vorhanden ist, können Verantwortliche von Systemrollen im Web Portal Gruppen, Administratorrollen, Abonnements und unwirksame Dienstpläne an die Systemrollen zuweisen. Die Gruppen, Administratorrollen, Abonnements und unwirksamen Dienstpläne werden an alle Identitäten vererbt, denen diese Systemrollen zugewiesen sind.

- Attestierung

  Wenn das Modul Attestierung vorhanden ist, kann die Richtigkeit der Eigenschaften von Zielsystemobjekten und von Berechtigungszuweisungen regelmäßig oder auf Anfrage bescheinigt werden. Dafür werden im Manager Attestierungsrichtlinien konfiguriert. Die Attestierer nutzen das Web Portal, um Attestierungsvorgänge zu entscheiden.

- Governance Administration

  Wenn das Modul Complianceregeln vorhanden ist, können Regeln definiert werden, die unzulässige Berechtigungszuweisungen identifizieren und deren Risiken bewerten. Die Regeln werden regelmäßig und bei Änderungen an den Objekten im One Identity Manager überprüft. Complianceregeln werden im Manager definiert. Verantwortliche nutzen das Web Portal, um Regelverletzungen zu überprüfen, aufzulösen und Ausnahmegenehmigungen zu erteilen.

  Wenn das Modul Unternehmensrichtlinien vorhanden ist, können Unternehmensrichtlinien für die im One Identity Manager abgebildeten Zielsystemobjekte definiert und deren Risiken bewertet werden. Unternehmensrichtlinien werden im Manager definiert. Verantwortliche nutzen das Web Portal, um Richtlinienverletzungen zu überprüfen und Ausnahmegenehmigungen zu erteilen.

- Risikobewertung

  Über den Risikoindex von Gruppen, Administratorrollen und Abonnements kann das Risiko von Zuweisungen für das Unternehmen bewertet werden. Dafür stellt der One Identity Manager Standard-Berechnungsvorschriften bereit. Im Web Portal können die Berechnungsvorschriften modifiziert werden.

- Berichte und Statistiken

  Das Web Portal stellt verschiedene Berichte und Statistiken über die Identitäten, Benutzerkonten, deren Berechtigungen und Risiken bereit.

Ausführliche Informationen zu den genannten Themen finden Sie unter Managen von Azure Active Directory Benutzerkonten und Identitäten auf Seite 66, Managen von Mitgliedschaften in Azure Active Directory Gruppen auf Seite 108, Managen von Zuweisungen von Azure Active Directory Administratorrollen auf Seite 127, Managen von Zuweisungen von Azure Active Directory Abonnements und Azure Active Directory Dienstplänen auf Seite 138 und in folgenden Handbüchern:

- *One Identity Manager Web Designer Web Portal Anwenderhandbuch*
- *One Identity Manager Administrationshandbuch für Attestierungen*

- *One Identity Manager Administrationshandbuch für Complianceregeln*
- *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien*
- *One Identity Manager Administrationshandbuch für Risikobewertungen*

11

Empfehlungen für Verbund-Umgebungen

HINWEIS: Für die Unterstützung von Verbund-Umgebungen im One Identity Manager müssen folgende Module vorhanden sein:

- Active Directory Modul
- Azure Active Directory Modul

In einer Verbund-Umgebung sind die lokalen Active Directory Benutzerkonten mit Azure Active Directory Benutzerkonten verbunden. Die Verbindung erfolgt über die Eigenschaft `ms-ds-consistencyGUID` am Active Directory Benutzerkonto und die Eigenschaft `immutableId` am Azure Active Directory Benutzerkonto. Die Synchronisation der Active Directory Benutzerkonten und Azure Active Directory Benutzerkonten in der Verbund-Umgebung übernimmt Azure AD Connect. Ausführliche Informationen zu Azure AD Connect finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

Im One Identity Manager wird die Verbindung über die Azure AD Connect Anker-ID des Active Directory Benutzerkontos (`ADSAccount.MSDsConsistencyGuid`) und den unveränderlichen Bezeichner des Azure Active Directory Benutzerkontos (`AADUser.OnPremImmutableId`) abgebildet.

Einige der zielsystemrelevanten Eigenschaften von Azure Active Directory Benutzerkonten, die mit lokalen Active Directory Benutzerkonten verbunden sind, können im One Identity Manager nicht bearbeitet werden. Die Zuweisung von Berechtigungen an Azure Active Directory Benutzerkonten im One Identity Manager ist jedoch möglich.

Zuweisungen zu Azure Active Directory Gruppen, die mit dem lokalen Active Directory synchronisiert werden, sind im One Identity Manager nicht erlaubt. Diese Gruppen können nicht über das Web Portal bestellt werden. Sie können diese Gruppen nur in Ihrer lokalen Umgebung verwalten. Ausführliche Informationen finden Sie in der *Azure Active Directory Dokumentation* von Microsoft.

Der One Identity Manager unterstützt folgende Szenarien für Verbund-Umgebungen.

Szenario 1

1. Die Active Directory Benutzerkonten werden im One Identity Manager erstellt und in die lokale Active Directory-Umgebung provisioniert.

2. Azure AD Connect erzeugt die Azure Active Directory Benutzerkonten im Azure Active Directory Mandanten.
3. Die Azure Active Directory Synchronisation liest die Azure Active Directory Benutzerkonten in den One Identity Manager ein.

Dieses Szenario ist das empfohlene Vorgehen. Das Erzeugen eines Azure Active Directory Benutzerkontos über Azure AD Connect und das anschließende Einlesen in den One Identity Manager dauern in der Regel einige Zeit. Die Azure Active Directory Benutzerkonten sind nicht sofort im One Identity Manager verfügbar.

Szenario 2

1. Die Active Directory Benutzerkonten und die Azure Active Directory Benutzerkonten werden im One Identity Manager erstellt.

   Dabei wird die Verbindung über die Spalten `ADSAccount.MSDsConsistencyGuid` und `AADUser.OnPremImmutableId` hergestellt. Dies kann über kundenspezifische Skripte oder kundenspezifische Bildungsregeln erfolgen.
2. Die Active Directory Benutzerkonten und die Azure Active Directory Benutzerkonten werden unabhängig voneinander in ihre Zielumgebungen provisioniert.
3. Azure AD Connect erkennt die Verbindung zwischen den Benutzerkonten, stellt die Verbindung auch in der Verbund-Umgebung her und aktualisiert die erforderlichen Eigenschaften.
4. Die nächste Azure Active Directory Synchronisation aktualisiert die Azure Active Directory Benutzerkonten im One Identity Manager.

Mit diesem Szenario sind die Azure Active Directory Benutzerkonten sofort im One Identity Manager vorhanden und können ihre Berechtigungen erhalten.

HINWEIS:

- Wenn Sie mit Kontendefinitionen arbeiten, wird empfohlen die Kontendefinition für Active Directory als vorausgesetzte Kontendefinition in der Kontendefinition für Azure Active Directory einzutragen.
- Wenn Sie mit Kontendefinitionen arbeiten, wird empfohlen im Automatisierungsgrad die Eigenschaft **IT Betriebsdaten überschreibend** mit dem Wert **Nur initial** verwenden. Die Daten werden in diesem Fall nur initial ermittelt.
- Nachträgliche Änderungen der Azure Active Directory Benutzerkonten per Bildungsregeln sollten nicht erfolgen, da einige der Zielsystem-relevanten Eigenschaften nicht bearbeitbar sind und es zu Fehlermeldungen kommen kann:

  ```
  [Exception]: ServiceException occured

  Code: Request_BadRequest

  Message: Unable to update the specified properties for on-premises mastered Directory Sync objects or objects currently undergoing migration.
  ```

```
[ServiceException]: Code: Request_BadRequest - Message: Unable to
update the specified properties for on-premises mastered Directory
Sync objects or objects currently undergoing migration.
```

Verwandte Themen

- Informationen zum lokalen Active Directory Benutzerkonto auf Seite 222
- Kontendefinitionen für Azure Active Directory Benutzerkonten auf Seite 67
- Stammdaten einer Kontendefinition auf Seite 69

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.

- Zielsystemtypen

  Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können. Es werden Einstellungen für die Provisionierung von Mitgliedschaften und die Einzelobjektsynchronisation vorgenommen. Zusätzlich dient der Zielsystemtyp zur Abbildung der Objekte im Unified Namespace.

  Weitere Informationen finden Sie unter Ausstehende Objekte nachbehandeln auf Seite 58.

- Zielsystemverantwortliche

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

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

  Weitere Informationen finden Sie unter Zielsystemverantwortliche für Azure Active Directory auf Seite 275.

- 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.

  Ausführliche Informationen zum Bearbeiten von Jobservern für Azure Active Directory finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Azure Active Directory-Umgebung*.

Zielsystemverantwortliche für Azure Active Directory

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

Wenn Sie die Berechtigungen 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 Identitäten als Zielsystemadministratoren fest.
2. Die Zielsystemadministratoren nehmen die Identitäten 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 Identitäten als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen Mandanten zuweisen.

Tabelle 46: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Azure Active Directory** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Identitäten anlegen, die nicht den Identitätstyp **Primäre Identität** haben. • Konfigurieren im Synchronization Editor die

Benutzer	Aufgaben
	Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Identitäten als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Identitäten 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 **Identitäten zuweisen**.
4. Weisen Sie die Identität zu und speichern Sie die Änderung.

Um initial Identitäten 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 **Identitäten zuweisen**.
4. Weisen Sie die Identitäten zu und speichern Sie die Änderungen.

Um als Zielsystemverantwortlicher weitere Identitäten 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 **Identitäten zuweisen**.
4. Weisen Sie die Identitäten 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 Identitäten 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 12
- Azure Active Directory Mandant auf Seite 200

Jobserver für Azure Active Directory-spezifische Prozessverarbeitung

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

- Allgemeine Stammdaten für Jobserver auf Seite 278
- Festlegen der Serverfunktionen auf Seite 281

Allgemeine Stammdaten für Jobserver

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 47: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS-Syntax. Syntax: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Zielsystem	Zielsystem des Computerkontos.
Sprache	Sprache des Servers.
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.

Eigenschaft	Bedeutung
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. 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. 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. Mit dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**,

Eigenschaft	Bedeutung
	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	Gibt an, 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. 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	Gibt an, 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. Den Dienst können Sie mit entsprechenden administrativen Berechtigungen im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Pausiert wegen Nichtverfügbarkeit eines Zielsystems	Gibt an, ob die Verarbeitung von Aufträgen für diese Queue angehalten wurde, weil das Zielsystem, für den dieser Jobserver der Synchronisationsserver ist, vorübergehend nicht erreichbar ist. Sobald das Zielsystem wieder erreichbar ist, wird die Verarbeitung gestartet und alle anstehenden Aufträge werden ausgeführt. Ausführliche Informationen zum Offline-Modus finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
Kein automatisches Softwareupdate	Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist,

Eigenschaft	Bedeutung
	müssen Sie manuell aktualisieren.
Softwareupdate läuft	Gibt an, ob gerade eine Softwareaktualisierung ausgeführt wird.
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 281

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 48: 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.

Serverfunktion	Anmerkungen
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. 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. 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.
Generischer 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.
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 Berichtsserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell Konnektor	Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen.

Verwandte Themen

- Allgemeine Stammdaten für Jobserver auf Seite 278

Anhang A

Fehlerbehebung

Mögliche Fehler bei der Synchronisation eines Azure Active Directory Mandanten

Problem

Beim Laden der Azure Active Directory Benutzerkonten tritt ein Fehler auf:

```
[Exception]: ServiceException occured
Code: BadRequest
Message: Tenant does not have a SPO license.
[ServiceException]: Code: BadRequest - Message: Tenant does not have a SPO license.
```

Ursache

Es wird ein Azure Active Directory Mandant synchronisiert, der keine Lizenz mit dem Dienst **SharePoint Online** besitzt.

Mögliche Lösungen

- Stellen Sie sicher, dass der Azure Active Directory Mandant eine Lizenz besitzt, welche den Dienst **SharePoint Online** beinhaltet. (Empfohlen)
- Wenn Sie einen Azure Active Directory Mandanten synchronisieren wollen, der keine Lizenz mit dem Dienst **SharePoint Online** besitzt, passen Sie das Synchronisationsprojekt im Synchronization Editor an.

  Deaktivieren Sie im Mapping **Users** die Property-Mapping-Regeln für die folgenden Schemaeigenschaften. Setzen Sie dazu die Mappingrichtungen auf den Wert **Nicht zuordnen**.

- BirthDay
- PreferedName
- Responsibilities
- Schools
- Skills
- PastProjects
- Interests
- HireDate
- EmployeeID
- AboutMe
- MySite
- ImAddresses
- FaxNumber
- OtherMails

Ausführliche Informationen zum Bearbeiten der Property-Mapping-Regeln im Synchronization Editor finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*

Anhang B

Konfigurationsparameter für die Verwaltung einer Azure Active Directory-Umgebung

Mit der Installation des Moduls sind folgende Konfigurationsparameter im One Identity Manager verfügbar.

Tabelle 49: Konfigurationsparameter

Konfi-gurationsparameter	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. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
TargetSystem | AzureAD | Accounts	Erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem | AzureAD | Accounts | InitialRandomPassword	Gibt an, 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	Identität, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Rolle, Verantwortlicher der Identität oder `XUserInserted`). Ist kein Empfänger ermittelbar,

Konfi-gurationsparameter	Beschreibung
	dann wird an die im Konfigurationsparameter **TargetSystem | AzureAD | DefaultAddress** hinterlegte Adresse versandt.
TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Identität - Erstellung neues Benutzerkonto** verwendet.
TargetSystem | AzureAD | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Identität - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem | AzureAD | Accounts | MailTemplateDefaultValues	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 **Identität - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | AzureAD | Accounts | PrivilegedAccount	Erlaubt die Konfiguration der Einstellungen für privilegierte Azure Active Directory Benutzerkonten.
TargetSystem | AzureAD | Accounts | PrivilegedAccount | AccountName_Postfix	Postfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | AzureAD | Accounts | PrivilegedAccount | AccountName_Prefix	Präfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | AzureAD | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | AzureAD | DeltaTokenDirectory	Verzeichnis, in dem die Delta-Token-Dateien für die Delta-Synchronisation abgelegt werden.
TargetSystem | AzureAD | MaxFullsyncDuration	Maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei

Konfi-gurationsparameter	Beschreibung
	Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.
TargetSystem | AzureAD | PersonAutoDefault	Modus für die automatische Identitätenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | AzureAD | PersonAutoDisabledAccounts	Gibt an, ob an deaktivierte Benutzerkonten automatisch Identitäten zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | AzureAD | PersonAutoFullSync	Modus für die automatische Identitätenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem | AzureAD | PersonExcludeList	Auflistung aller Benutzerkonten, für die keine automatische Identitätenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $`
TargetSystem | AzureAD | PersonUpdate	Gibt an, ob Identitäten bei Änderung ihrer Benutzerkonten aktualisiert werden. Aktivieren Sie diesen Konfigurationsparameter, um eine fortlaufende Aktualisierung von Identitäten aus verbundenen Benutzerkonten zu erreichen.
QER | ITShop | AutoPublish | AADGroup	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der automatischen Übernahme von Azure Active Directory Gruppen in den IT Shop. Ist der Parameter aktiviert, werden alle Gruppen automatisch als Produkte dem IT Shop zugewiesen. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
QER | ITShop | AutoPublish |	Auflistung aller Azure Active Directory Gruppen, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Jeder

Konfigurationsparameter	Beschreibung
AADGroup | ExcludeList	Eintrag ist Bestandteil eines regulären Suchmusters und unterstützt die Notation für reguläre Ausdrücke. Beispiel: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
QER | ITShop | AutoPublish | AADSubSku	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der automatischen Übernahme von Azure Active Directory Abonnements in den IT Shop. Ist der Parameter aktiviert, werden alle Abonnements automatisch als Produkte dem IT Shop zugewiesen. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
QER | ITShop | AutoPublish | AADSubSku | ExcludeList	Auflistung aller Azure Active Directory Abonnements, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Jeder Eintrag ist Bestandteil eines regulären Suchmusters und unterstützt die Notation für reguläre Ausdrücke.
QER | ITShop | AutoPublish | AADDeniedServicePlan	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der automatischen Übernahme von Azure Active Directory Dienstpläne in den IT Shop. Ist der Parameter aktiviert, werden alle Dienstpläne automatisch als Produkte dem IT Shop zugewiesen. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
QER | ITShop | AutoPublish | AADDeniedServicePlan | ExcludeList	Auflistung aller Azure Active Directory Dienstpläne, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Jeder Eintrag ist Bestandteil eines regulären Suchmusters und unterstützt die Notation für reguläre Ausdrücke.

Anhang C

Standardprojektvorlagen 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.

Detaillierte Informationen zum Thema

- Projektvorlage für Azure Active Directory Mandanten auf Seite 290
- Projektvorlage für Azure Active Directory B2C Mandanten auf Seite 291

Projektvorlage für Azure Active Directory Mandanten

Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 50: Abbildung der Azure Active Directory Schematypen

Schematyp im Azure Active Directory	Tabelle im One Identity Manager Schema
DirectoryRole	AADDirectoryRole
Group	AADGroup
LicenseAssignments	AADUserHasSubSku

Schematyp im Azure Active Directory	Tabelle im One Identity Manager Schema
GroupLicenseAssignments	AADGroupHasSubSku
Organization	AADOrganization
ServicePlanInfo	AADServicePlan
SubscribedSku	AADSubSku
User	AADUser
VerifiedDomain	AADVerifiedDomain
Application	AADApplication
AppRole	AADAppRole
AppRoleAssignment	AADAppRoleAssignment
ServicePrincipal	AADServicePrincipal
ActivityBasedTimeoutPolicy	AADActivityBasedTimeoutPolicy
HomeRealmDiscoveryPolicy	AADHomeRealmDiscoveryPolicy
TokenIssuancePolicy	AADTokenIssuancePolicy
TokenLifetimePolicy	AADTokenLifetimePolicy
AdministrativeUnit	AADAdministrativeUnit

Projektvorlage für Azure Active Directory B2C Mandanten

Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 51: Abbildung der Azure Active Directory Schematypen

Schematyp im Azure Active Directory	Tabelle im One Identity Manager Schema
AdministrativeUnit	AADAdministrativeUnit
ActivityBasedTimeoutPolicy	AADActivityBasedTimeoutPolicy
Application	AADApplication
AppRole	AADAppRole
AppRoleAssignment	AADAppRoleAssignment

Schematyp im Azure Active Directory	Tabelle im One Identity Manager Schema
DirectoryRole	AADDirectoryRole
Group	AADGroup
GroupLicenseAssignments	AADGroupHasSubSku
HomeRealmDiscoveryPolicy	AADHomeRealmDiscoveryPolicy
Organization	AADOrganization
ServicePrincipal	AADServicePrincipal
TokenIssuancePolicy	AADTokenIssuancePolicy
TokenLifetimePolicy	AADTokenLifetimePolicy
User	AADUser
VerifiedDomain	AADVerifiedDomain

Anhang D

Verarbeitung von Azure Active Directory Systemobjekten

Folgende Tabelle beschreibt die zulässigen Verarbeitungsmethoden für die Schematypen von Azure Active Directory und benennt notwendige Einschränkungen bei der Verarbeitung der Systemobjekte.

Tabelle 52: Zulässige Verarbeitungsmethoden für Schematypen

Typ	Lesen	Hinzufügen	Löschen	Aktualisieren
Abonnements (`SubscribedSku`)	Ja	Nein	Nein	Nein
Administratorrollen (`DirectoryRole`)	Ja	Nein	Nein	Ja
Benutzerkonten (`User`)	Ja	Ja	Ja	Ja
Dienstpläne (`ServicePlanInfo`)	Ja	Nein	Nein	Nein
Domänen (`VerifiedDomain`)	Ja	Nein	Nein	Nein
Gruppen (`Group`)	Ja	Ja	Ja	Ja
Lizenzzuweisungen an Benutzerkonten (`LicenseAssignments`)	Ja	Ja	Ja	Ja
Lizenzzuweisungen an Gruppen (`GroupLicenseAssignments`)	Ja	Nein	Nein	Nein
Mandanten (`Organization`)	Ja	Nein	Nein	Ja
Anwendungen (`Application`)	Ja	Nein	Nein	Ja
Dienstprinzipale (`ServicePrincipal`)	Ja	Nein	Nein	Ja
App-Rollen (`AppRole`)	Ja	Nein	Nein	Nein

Typ	Lesen	Hinzufügen	Löschen	Aktualisieren
Zuweisungen zu App-Rollen (`AppRoleAssignment`)	Ja	Ja	Ja	Ja
Richtlinien zum Inaktivitätstimeout (`ActivityBasedTimeoutPolicy`)	Ja	Nein	Nein	Nein
Richtlinien zur Startbereichsermittlung (`HomeRealmDiscoveryPolicy`)	Ja	Nein	Nein	Nein
Richtlinien zur Token-Ausstellung (`TokenIssuancePolicy`)	Ja	Nein	Nein	Nein
Richtlinie zur Token-Gültigkeitsdauer (`TokenLifetimePolicy`)	Ja	Nein	Nein	Nein
Klassifizierungen (`AADGroupClassificationLbl`)	Ja	Nein	Nein	Nein
Verwaltungseinheiten (`AdministrativeUnit`)	Ja	Ja	Ja	Ja

Anhang E

Einstellungen des Azure Active Directory Konnektors

Für die Systemverbindung mit dem Azure Active Directory Konnektor werden die folgenden Einstellungen konfiguriert.

Tabelle 53: Einstellungen des Azure Active Directory Konnektors

Einstellung	Bedeutung
Client ID	Anwendungs-ID, die der Integration des One Identity Manager als Anwendung des Azure Active Directory Mandanten erzeugt wurde. Variable: `CP_ClientID`
Anmeldedomäne	Basisdomäne oder eine verifizierte Domäne Ihres Azure Active Directory Mandanten. Variable: `CP_OrganizationDomain`
Benutzername	Name des Benutzerkontos zur Anmeldung am Azure Active Directory, wenn Sie den One Identity Manager als systemeigene Clientanwendung in Ihrem Azure Active Directory Mandanten integriert haben. Variable: `CP_Username`
Kennwort	Kennwort zum Benutzerkonto. Variable: `CP_Password`
Schlüssel	Schlüssel, der bei der Registrierung des One Identity Manager als Webanwendung des Azure Active Directory Mandanten erzeugt wurde. Variable: `CP_Secret`
Organisations-ID	ID des Azure Active Directory Mandanten. Variable: `OrganizationID`

Einstellung	Bedeutung
GuestInviteSendMail	Gibt an, ob eine Einladung für Gastbenutzer verschickt werden soll. Standard: **True** Variable: `GuestInviteSendMail`
GuestInviteLanguage	Sprache, in der die Einladung an Gastbenutzer verschickt werden soll. Standard: **en-us** Variable: `GuestInviteLanguage`
GuestInviteCustomMessage	Persönliche Willkommensnachricht an den Gastbenutzer. Variable: `GuestInviteCustomMessage`
GuestInviteRedirectUrl	URL zur Umleitung von Gastbenutzern, nachdem sie die Einladung angenommen und sich angemeldet haben. Standard: **http://www.office.com** Variable: `GuestInviteRedirectUrl`

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 Kunden von One Identity 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

A

B

E

I

J

S

V

Z