One Identity Manager 8.2

Administrationshandbuch für die Anbindung einer Universal Cloud Interface-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 Universal Cloud Interface-Umgebung
Aktualisiert - 24. November 2021, 10:41 Uhr
Version - 8.2

Inhalt

1

Verwalten einer Universal Cloud Interface-Umgebung

Der One Identity Manager unterstützt die Umsetzung von Identity und Access Governance Anforderungen in IT-Umgebungen, die häufig eine Mischung aus traditionellen, intern gehosteten Applikationen und modernen Cloud-Anwendungen darstellen. Benutzer und Berechtigungen aus Cloud-Anwendungen können im One Identity Manager abgebildet werden. Damit ist es möglich, die Identity und Access Governance Prozesse wie Attestierung, Identity Audit, Management von Benutzern und Systemberechtigungen, IT Shop oder Berichtsabonnements auch für Cloud-Anwendungen zu nutzen.

Datenschutzrichtlinien, wie die Datenschutz-Grundverordnung, erfordern eine Abstimmung, welche Daten eines Mitarbeiters in Cloud-Anwendungen gespeichert werden dürfen. Bei entsprechender Konfiguration der Systemumgebung gewährleistet der One Identity Manager, dass Cloud-Anwendungen und deren verantwortliche Administratoren keinerlei Zugriff auf die Personenstammdaten sowie die Identity und Access Governance Prozesse erhalten. Aus diesem Grund werden Cloud-Anwendungen in zwei getrennten Modulen verwaltet, die bei Bedarf in getrennten Datenbanken installiert sein können.

Das Modul Universal Cloud Interface bildet die Schnittstelle, über die Benutzer und Berechtigungen aus Cloud-Anwendungen in eine One Identity Manager-Datenbank übertragen werden können. Hier wird die Synchronisation mit den Cloud-Anwendungen konfiguriert und ausgeführt. Jede Cloud-Anwendung wird als eigenes Basisobjekt im One Identity Manager abgebildet. Die Benutzerdaten werden als Benutzerkonten, Gruppen, Systemberechtigungen und Berechtigungselemente gespeichert und können in Containern organisiert werden. Sie können im One Identity Manager nicht bearbeitet werden. Eine Verbindung zu Identitäten (Personen) wird hier nicht hergestellt.

Im Modul Cloud Systems Management wird die Verbindung zu Identitäten hergestellt; Benutzerkonten, Gruppen, Systemberechtigungen und Berechtigungselemente können erstellt und bearbeitet werden. Damit können die Identity und Access Governance Prozesse zur Verwaltung der Cloud-Benutzerkonten und ihren Berechtigungen genutzt werden. Per Synchronisation werden die Daten zwischen den Modulen Universal Cloud Interface und Cloud Systems Management ausgetauscht. Provisionierungsprozesse sorgen dafür, dass Änderungen an den Objekten aus dem Modul Cloud Systems Management in das Modul Universal Cloud Interface übertragen werden.

Für manche Cloud-Anwendungen kann (aus technischen Gründen) oder soll (aufgrund der zu geringen Änderungsmenge) keine automatisierte Schnittstelle zum Provisionieren von

Änderungen aus dem Modul Universal Cloud Interface in die Cloud-Anwendung eingesetzt werden. In diesem Fall können die Änderungen manuell provisioniert werden.

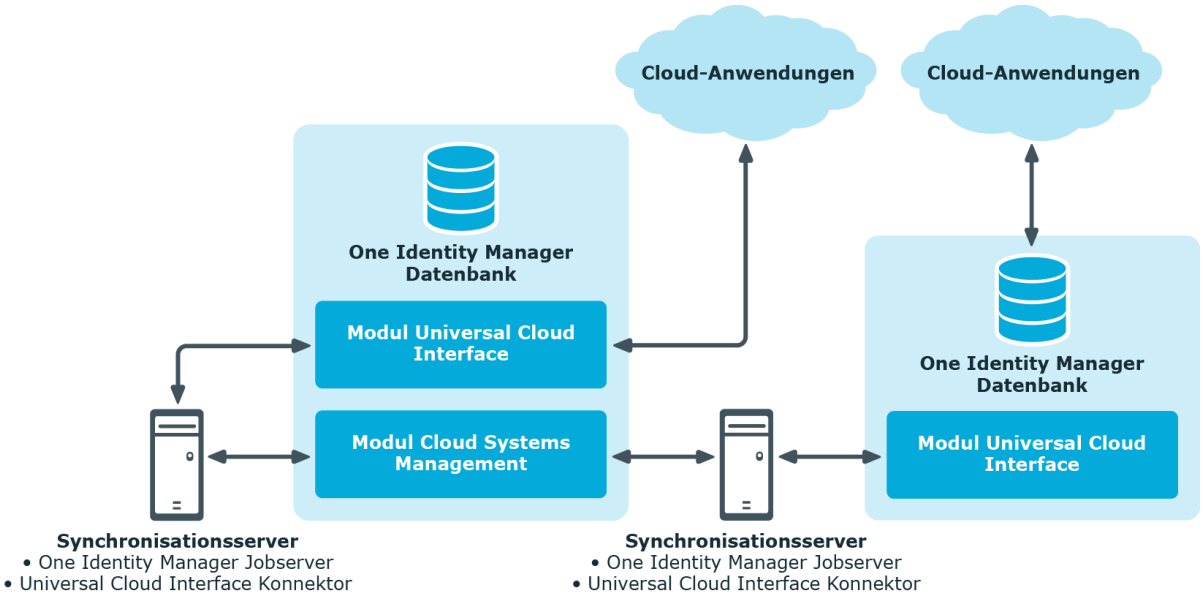
Da im Modul Universal Cloud Interface nur die Daten gespeichert werden, die in den Cloud-Anwendungen verfügbar sein müssen, kann dieses Modul in einer separaten Datenbank installiert werden. Diese Datenbank kann sich auch außerhalb der Unternehmensinfrastruktur befinden.

In Verbindung mit der Cloud-Lösung One Identity Starling Connect entsteht eine einfache und umfassende Lösung zur Integration von Cloud-Anwendungen und zur Abbildung der Anforderungen an hybride Lösungsszenarien.

Architekturüberblick

Für die Synchronisation mit Cloud-Anwendungen im Modul Universal Cloud Interface wird ein Synchronisationsserver benötigt, auf dem der Universal Cloud Interface Konnektor installiert ist. Das Modul Universal Cloud Interface kann in der selben One Identity Manager-Datenbank vorhanden sein, in der auch das Modul Cloud Systems Management installiert ist. Die Synchronisation kann aber auch mit einer anderen One Identity Manager-Datenbank eingerichtet werden, die auf einem externen Datenbankserver bereitgestellt wird.

Abbildung 1: Architektur für die Synchronisation



Ausführliche Informationen über die Kommunikation zwischen dem Universal Cloud Interface und den Cloud-Anwendungen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung von Cloud-Anwendungen*.

One Identity Manager Benutzer für die Verwaltung von Cloud Zielsystemen

In die Einrichtung und Verwaltung von Cloud Zielsystemen sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der 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 Personen als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Cloud Zielsysteme** 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 und Systemberechtigungen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.

Benutzer	Aufgaben
	• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	One Identity Manager Administratoren sind administrative Systembenutzer. Administrative Systembenutzer werden 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.
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. • Weisen Systemberechtigungen an IT Shop-Strukturen zu.
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. • Weisen Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zu.

Benutzer	Aufgaben
Administratoren für Geschäftsrollen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Geschäftsrollen zu. • Weisen Systemberechtigungen an Geschäftsrollen zu.

2

Synchronisieren einer Cloud-Anwendung im Universal Cloud Interface

Per Synchronisation werden die Daten zwischen den Modulen Universal Cloud Interface und Cloud Systems Management ausgetauscht. Damit die Identity und Data Governance Prozesse auf die Objekte aus einer Cloud-Anwendung angewendet werden können, muss die Synchronisation zwischen beiden Modulen eingerichtet werden.

HINWEIS: Im Folgenden ist häufig von **Zielsystem** und **(One Identity Manager) Datenbank** die Rede. Dabei meint **Zielsystem** immer eine Cloud-Anwendung im Universal Cloud Interface. **One Identity Manager-Datenbank** oder **Datenbank** bezieht sich immer auf die Objekte im Modul Cloud Systems Management.

Tabelle 2: Begriffe

	One Identity Manager-Datenbank	Zielsystem
Verbundenes System	Modul Cloud Systems Management	Modul Universal Cloud Interface
Basisobjekt	Cloud Zielsystem	Cloud-Anwendung

Wie die Schematypen der verbundenen Systeme aufeinander abgebildet werden, ist im Mapping festgelegt. Weitere Informationen finden Sie unter Standardprojektvorlage für Cloud-Anwendungen im Universal Cloud Interface auf Seite 189.

Informieren Sie sich hier:

- wie Sie die Synchronisation zwischen den Modulen Universal Cloud Interface und Cloud Systems Management einrichten,
- wie Sie eine Synchronisationskonfiguration anpassen, beispielsweise um verschiedene Zielsysteme mit ein und demselben Synchronisationsprojekt zu synchronisieren,
- wie Sie die Synchronisation starten und deaktivieren,
- wie Sie die Synchronisationsergebnisse auswerten.

TIPP: Bevor Sie die Synchronisation 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 einer Cloud-Anwendung im Universal Cloud Interface

Der Synchronization Editor stellt eine Projektvorlage bereit, mit der die Synchronisation von Benutzerkonten und Berechtigungen eingerichtet werden kann. Nutzen Sie diese Projektvorlage für die Einrichtung des initialen Synchronisationsprojektes. Zusätzlich werden die notwendigen Prozesse angelegt, über die Änderungen an Zielsystemobjekten in das Zielsystem provisioniert werden.

Um die Objekte einer Cloud-Anwendung initial in das Modul Cloud Systems Management zu übernehmen

1. Statten Sie One Identity Manager Benutzer mit den erforderlichen Berechtigungen für die Einrichtung der Synchronisation und die Nachbehandlung der Synchronisationsobjekte aus.
2. Die One Identity Manager Bestandteile für die Verwaltung von Cloud Zielsystemen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | CSM** 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.

3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

   HINWEIS: Damit das Synchronisationsprojekt erstellt werden kann, muss die Cloud-Anwendung bereits im Modul Universal Cloud Interface vorhanden sein. Ausführliche Informationen zum Einrichten der initialen Synchronisation mit einer Cloud-Anwendung finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung von Cloud-Anwendungen*.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung auf Seite 16
- Einrichten des Synchronisationsservers auf Seite 17
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung auf Seite 21
- Startkonfigurationen für die Synchronisation von Cloud-Anwendungen auf Seite 27
- Konfigurationsparameter für die Verwaltung von Cloud Zielsystemen auf Seite 186
- Standardprojektvorlage für Cloud-Anwendungen im Universal Cloud Interface auf Seite 189

Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung

Bei der Synchronisation des One Identity Manager mit einer Cloud-Anwendung im Universal Cloud Interface spielen folgende Benutzer eine Rolle.

Tabelle 3: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzer für den Zugriff auf die Cloud-Anwendung im Universal Cloud Interface	Für die Anmeldung an der Datenbank, die das Universal Cloud Interface enthält, nutzen Sie: • bei rollenbasierter Anmeldung: einen Benutzer mit der Anwendungsrolle **Universal Cloud Interface | Administratoren** - ODER - • bei nicht-rollenbasierter Anmeldung: einen

Benutzer	Berechtigungen
	Systembenutzer mit der Berechtigungsgruppe **DPR_EditRights_Methods**
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.

Einrichten des 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 Universal Cloud Interface Konnektor installiert werden.

Detaillierte Informationen zum Thema

- Systemanforderungen für den Synchronisationsserver auf Seite 18
- One Identity Manager Service mit Universal Cloud Interface Konnektor installieren auf Seite 18

Systemanforderungen für den Synchronisationsserver

Für die Einrichtung der Synchronisation 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 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.

One Identity Manager Service mit Universal Cloud Interface Konnektor installieren

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Universal Cloud Interface Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

Tabelle 4: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	Universal Cloud Interface Konnektor
Maschinenrolle	Server | Jobserver

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

Verbindungen).

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

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

HINWEIS: Das Programm führt eine Remote-Installation des One Identity Manager Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich.

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

HINWEIS: Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Einrichten des Jobservers finden Sie im *One Identity Manager Konfigurationshandbuch*.

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

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

       - ODER -

       Um einen neuen Jobserver zur erstellen, klicken Sie **Hinzufügen**.
    b. Bearbeiten Sie folgende Informationen für den Jobserver.
        - **Server**: Bezeichnung des Jobservers.
        - **Queue**: Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder 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 **Job Server**.
5. Auf der Seite **Serverfunktionen** wählen Sie **Universal Cloud Interface Konnektor**.
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:
     1. Wählen Sie **Prozessabholung > sqlprovider**
     2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     3. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
   - Für eine Verbindung zum Anwendungsserver:
     1. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
     2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     3. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
     4. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
     5. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.

8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Wenn die Datenbank verschlüsselt ist, wählen Sie auf der Seite **Datenbankschlüsseldatei auswählen** die Datei mit dem privaten Schlüssel.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
    - **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.
12. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

    Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.
13. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

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

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen dem Modul Cloud Systems Management und dem Modul Universal Cloud Interface 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 die Erstellung eines Synchronisationsprojektes auf Seite 22
- Initiales Synchronisationsprojekt für eine Cloud-Anwendung erstellen auf Seite 23

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

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

Tabelle 5: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Cloud-Anwendung	Bezeichnung der Cloud-Anwendung im Modul Universal Cloud Interface, die synchronisiert werden soll.
Synchronisationsserver	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 Universal Cloud Interface Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. **Tabelle 6: Zusätzliche Eigenschaften für den Jobserver** Eigenschaft: Serverfunktion — Wert: Universal Cloud Interface Konnektor Eigenschaft: Maschinenrolle — Wert: Server | Jobserver Weitere Informationen finden Sie unter Systemanforderungen für den Synchronisationsserver auf Seite 18.
Verbindungsdaten zur One Identity Manager-	• Datenbankserver • Name der Datenbank

Angaben	Erläuterungen
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 • Universal Cloud Interface Konnektor ist installiert Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Initiales Synchronisationsprojekt für eine Cloud-Anwendung 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 eine Cloud-Anwendung 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 Universal Cloud Interface** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors wird gestartet.

3. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.

   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, möglich, nehmen Sie keine Einstellungen vor.
   - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, nicht möglich, können Sie eine Remoteverbindung herstellen.

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

4. Auf der Startseite des Systemverbindungsassistenten klicken Sie **Weiter**.
5. Auf der Seite **Datenbanksystem auswählen** wählen Sie das Datenbanksystem aus, für das Sie die Verbindung einrichten möchten.
6. Auf der Seite **Verbindungsparameter** geben Sie die Verbindungsdaten zur Datenbank an, die das Modul Universal Cloud Interface enthält.

   - **Server**: Datenbankserver.
   - (Optional) **Windows Authentifizierung**: Gibt an, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
   - **Nutzer**: SQL Server Anmeldename des Installationsbenutzer.
   - **Kennwort**: Kennwort für den Installationsbenutzer.
   - **Datenbank**: Wählen Sie die Datenbank.
   - Um zusätzliche Informationen zur Datenbankverbindung zu erfassen, klicken Sie **Erweiterte Optionen**.
   - Um zu testen, ob die Datenbank erreichbar ist, klicken Sie **Testen**.

7. Auf der Seite **Verschlüsselung** geben Sie den privaten Schlüssel zur Entschlüsselung der Datenbank an.
8. 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**.
9. 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.
10. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
11. Auf der Seite **Cloud-Anwendung auswählen** wählen Sie die Cloud-Anwendung, die synchronisiert werden soll.
12. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

Tabelle 7: 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	Gibt an, ob zusätzlich zum Synchronisationsworkflow zum

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

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

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

    a. Klicken Sie , um einen neuen Jobserver anzulegen.

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

    c. Klicken Sie **OK**.

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

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

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

    Es werden zwei Startkonfigurationen und zwei Standardzeitpläne für regelmäßige Synchronisationen erstellt.

Tabelle 8: Startkonfigurationen

Startkonfiguration	Ausführungsintervall
Synchronization of the cloud application	täglich
Synchronization of pending changes	stündlich

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.

Detaillierte Informationen zum Thema

- Benötigte Informationen für die Erstellung eines Synchronisationsprojektes auf Seite 22
- Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung auf Seite 16
- Einrichten des Synchronisationsservers auf Seite 17
- Startkonfigurationen für die Synchronisation von Cloud-Anwendungen auf Seite 27
- Synchronisationsprotokoll konfigurieren auf Seite 28
- Anpassen einer Synchronisationskonfiguration auf Seite 29
- Ausführen einer Synchronisation auf Seite 37
- Aufgaben nach der Synchronisation auf Seite 41
- Standardprojektvorlage für Cloud-Anwendungen im Universal Cloud Interface auf Seite 189

Startkonfigurationen für die Synchronisation von Cloud-Anwendungen

Der Projektassistent legt zwei Startkonfigurationen an, welche die Synchronisation der Cloud-Anwendung ausführen.

- Synchronization of the cloud application (Synchronisation der Cloud-Anwendung)

  Die Objekte der Cloud-Anwendung, wie Benutzerkonten, Gruppen, Gruppenmitgliedschaften, werden synchronisiert. Es wird der Workflow **Initial**

Synchronization verwendet. Mit dem zugeordneten Standardzeitplan wird die Sychronisation täglich ausgeführt.

- Synchronization of pending changes (Synchronisation von anstehenden Änderungen)

  Wenn Cloud-Objekte im Modul Cloud Systems Management geändert werden, müssen diese Änderungen zuerst in das Modul Universal Cloud Interface übertragen werden und können danach in die Cloud-Anwendung selbst provisioniert werden. Um nachvollziehen zu können, ob die Änderungen erfolgreich in die Cloud-Anwendung provisioniert wurden, werden diese Änderungen als **anstehende Änderungen** aufgezeichnet. Zu jeder anstehenden Änderung werden die Details, der Erstellungszeitpunkt und der Verarbeitungsstatus gespeichert. Sobald die Provisionierung abgeschlossen ist, muss der Verarbeitungsstatus aus der Universal Cloud Interface-Umgebung in das Modul Cloud Systems Management übertragen werden. Dazu wird die Startkonfiguration **Synchronization of pending changes** ausgeführt. Es wird der Workflow **State Synchronization** verwendet. Mit dem zugeordneten Standardzeitplan wird die Synchronisation stündlich ausgeführt.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 47
- Synchronisationen starten auf Seite 38

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 separat konfiguriert werden.

Um den Inhalt des Synchronisationsprotokolls 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**.

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 40

Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation einer Universal Cloud Interface-Umgebung eingerichtet. Mit diesem Synchronisationsprojekt können Sie Objekte aus einer Cloud-Anwendung in das Modul Cloud Systems Management einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in die Universal Cloud Interface-Umgebung provisioniert.

Um die Cloud-Anwendung regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation das Modul Cloud Systems Management 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 Cloud-Anwendungen eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an den Datenbanken als Variablen.
- Um festzulegen, welche Zielsystemobjekte 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 Daten zu synchronisieren, für die keine Schematypen im Konnektorschema angelegt sind, legen Sie eigene Schematypen an. Nehmen Sie die Schemaerweiterungen in das Mapping auf.
- Wenn das Schema der Cloud-Anwendung nicht durch die Standard-Projektvorlage ausreichend abgebildet werden kann, passen Sie die Synchronisationskonfiguration an. Definieren Sie dabei, wie die Systemberechtigungen im One Identity Manager Schema abgebildet werden. Stellen Sie sicher, dass bei der Einrichtung der Synchronisation das Basisobjekt für die Cloud-Anwendung (`CSMRoot`) in der Datenbank angelegt wird und die Eigenschaften **Typen der verwendeten Systemberechtigungen** (`GroupUsageMask`) und **Benutzerkonto enthält Mitgliedschaften** (`UserContainsGroupList`) korrekt gesetzt werden.

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

Detaillierte Informationen zum Thema

- Synchronisation in die Universal Cloud Interface-Umgebung konfigurieren auf Seite 30
- Synchronisation verschiedener Cloud-Anwendungen konfigurieren auf Seite 31
- Schema aktualisieren auf Seite 34
- Einstellungen der Systemverbindung zur Cloud-Anwendung im Universal Cloud Interface ändern auf Seite 32

Synchronisation in die Universal Cloud Interface-Umgebung 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 die Universal Cloud Interface-Umgebung 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 Cloud-Anwendungen konfigurieren auf Seite 31

Synchronisation verschiedener Cloud-Anwendungen konfigurieren

Voraussetzungen

- Alle virtuellen Schemaeigenschaften, die im Mapping genutzt werden, müssen in den erweiterten Schemas beider Cloud-Anwendungen vorhanden sein.

Um ein Synchronisationsprojekt für die Synchronisation einer weiteren Cloud-Anwendung anzupassen

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Erstellen Sie für die weitere Cloud-Anwendung ein neues Basisobjekt.
    - Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
    - Wählen Sie im Assistenten den Universal Cloud Interface 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 die Universal Cloud Interface-Umgebung konfigurieren auf Seite 30

Einstellungen der Systemverbindung zur Cloud-Anwendung im Universal Cloud Interface 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 32
- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 33

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 Cloud-Anwenungen 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 33

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 32

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 durch Revisionsfilterung

Beim Start der Synchronisation werden alle zu synchronisierenden Objekte geladen. Ein Teil dieser Objekte wurde gegebenenfalls seit der letzten Synchronisation nicht geändert und muss daher bei der Synchronisation nicht verarbeitet werden. Indem nur solche Objekte geladen werden, die sich seit der letzten Synchronisation geändert haben, kann die Synchronisation beschleunigt werden. Zur Beschleunigung der Synchronisation nutzt der One Identity Manager die Revisionsfilterung.

Der One Identity Manager unterstützt die Revisionsfilterung. Als Revisionszähler wird das Datum der letzten Änderung der Zielsystemobjekte (Spalte `XDateUpdated`) genutzt. Jede Synchronisation speichert ihr letztes Ausführungsdatum als Revision in der One Identity Manager-Datenbank (Tabelle `DPRRevisionStore`, Spalte `Value`). Dieser Wert wird als Vergleichswert für die Revisionsfilterung bei der nächsten Synchronisation mit dem selben Workflow genutzt. Bei der Synchronisation mit diesem Workflow wird das Änderungsdatum der Zielsystemobjekte mit der in der One Identity Manager-Datenbank gespeicherten Revision verglichen. Es werden nur noch die Objekte aus dem Zielsystem gelesen, die sich seit diesem Datum verändert haben.

Die Revision wird zu Beginn einer Synchronisation ermittelt. Objekte, die durch die Synchronisation geändert werden, werden bei der nächsten Synchronisation nochmals geladen und überprüft. Die zweite Synchronisation nach der Initialsynchronisation ist daher noch nicht deutlich schneller.

Die Revisionsfilterung kann an den Workflows oder an den Startkonfigurationen zugelassen werden.

Um die Revisionsfilterung an einem Workflow zuzulassen

- Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
- Bearbeiten Sie die Eigenschaften des Workflows. Wählen Sie in der Auswahlliste **Revisionsfilterung** den Eintrag **Revisionsfilter nutzen**.

Um die Revisionsfilterung an einer Startkonfiguration zuzulassen

- Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
- Bearbeiten Sie die Eigenschaften der Startkonfiguration. Wählen Sie in der Auswahlliste **Revisionsfilterung** den Eintrag **Revisionsfilter nutzen**.

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

Einzelobjektsynchronisation konfigurieren

Die Einzelobjektsynchronisation wird nicht unterstützt.

Beschleunigung der Provisionierung

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

HINWEIS: Die Lastverteilung sollte nicht permanent für Provisionierungen 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 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 **Universal Cloud Interface Konnektor** zu.

   Alle Jobserver müssen auf das gleiche Cloud Zielsystem 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 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 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 Universal Cloud Interface-spezifische Prozessverarbeitung auf Seite 180

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 38
- Synchronisation deaktivieren auf Seite 39
- Synchronisationsergebnisse anzeigen auf Seite 40
- Startkonfigurationen für die Synchronisation von Cloud-Anwendungen auf Seite 27

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**.

Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung auf Seite 21

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 28
- Fehleranalyse auf Seite 44

Aufgaben nach der 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 41
- Konfiguration des Zielsystemabgleichs anzeigen auf Seite 43
- Cloud Benutzerkonten über Kontendefinitionen verwalten auf Seite 44

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 **Cloud Zielsysteme > Zielsystemabgleich: Universal Cloud Interface**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **Universal Cloud Interface** 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. Die Markierung **Ausstehend** wird für das Objekt entfernt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	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.

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.

Verwandte Themen

- Weitere Informationen finden Sie unter Konfiguration des Zielsystemabgleichs anzeigen auf Seite 43.

Konfiguration des Zielsystemabgleichs anzeigen

Am Zielsystemtyp ist festgelegt, für welche Tabellen ein Zielsystemabgleich durchgeführt werden kann. Die Synchronisation in kundenspezifische Tabellen ist im Modul Cloud Systems Management nicht möglich. Damit kann auch kein Zielsystemabgleich für kundenspezifische Tabellen konfiguriert werden.

Um die Konfiguration des Zielsystemabgleichs anzuzeigen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp Universal Cloud Interface.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.

   Alle Tabellen, für die der Zielsystemabgleich durchgeführt werden kann, sind aktiviert.
4. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.

   An allen Tabellen, für die ausstehende Objekte in das Zielsystem publiziert werden dürfen, ist die Option **Publizierbar** aktiviert.

Verwandte Themen

- Ausstehende Objekte nachbehandeln auf Seite 41

Cloud Benutzerkonten über Kontendefinitionen verwalten

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

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

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. 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 **Cloud Zielsysteme > <Zielsystem> > Benutzerkonten > Verbunden aber nicht konfiguriert > <Zielsystem>**.
    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 Cloud Benutzerkonten auf Seite 51

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 40

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.

   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.

3

Provisionierung von Objektänderungen

Änderungen an Cloud-Objekten können nur im Modul Cloud Systems Management vorgenommen werden. Provisionierungsprozesse sorgen dafür, dass Objektänderungen aus dem Modul Cloud Systems Management in das Modul Universal Cloud Interface übertragen werden. Standardmäßig werden diese Objektänderungen anschließend durch automatische Provisionierungsprozesse in die Cloud-Anwendungen publiziert.

Der One Identity Manager zeichnet die Objektänderungen als anstehende Änderungen in separaten Tabellen auf. Die Tabelle `QBMPendingChange` enthält die geänderten Objekte und deren Verarbeitungsstatus. In der Tabelle `QBMPendingChangeDetail` werden die Details der Änderungen, die auszuführenden Operationen, der Erstellungszeitpunkt und der Verarbeitungsstatus gespeichert.

Der Verarbeitungsstatus für ein Objekt wird erst dann abschließend auf erfolgreich gesetzt, wenn alle zugehörigen Änderungen für dieses Objekt erfolgreich provisioniert wurden. Der Verarbeitungsstatus eines Objekts ist fehlgeschlagen, wenn alle zugehörigen Änderungen verarbeitet wurden und mindestens eine dieser Änderungen fehlgeschlagen ist.

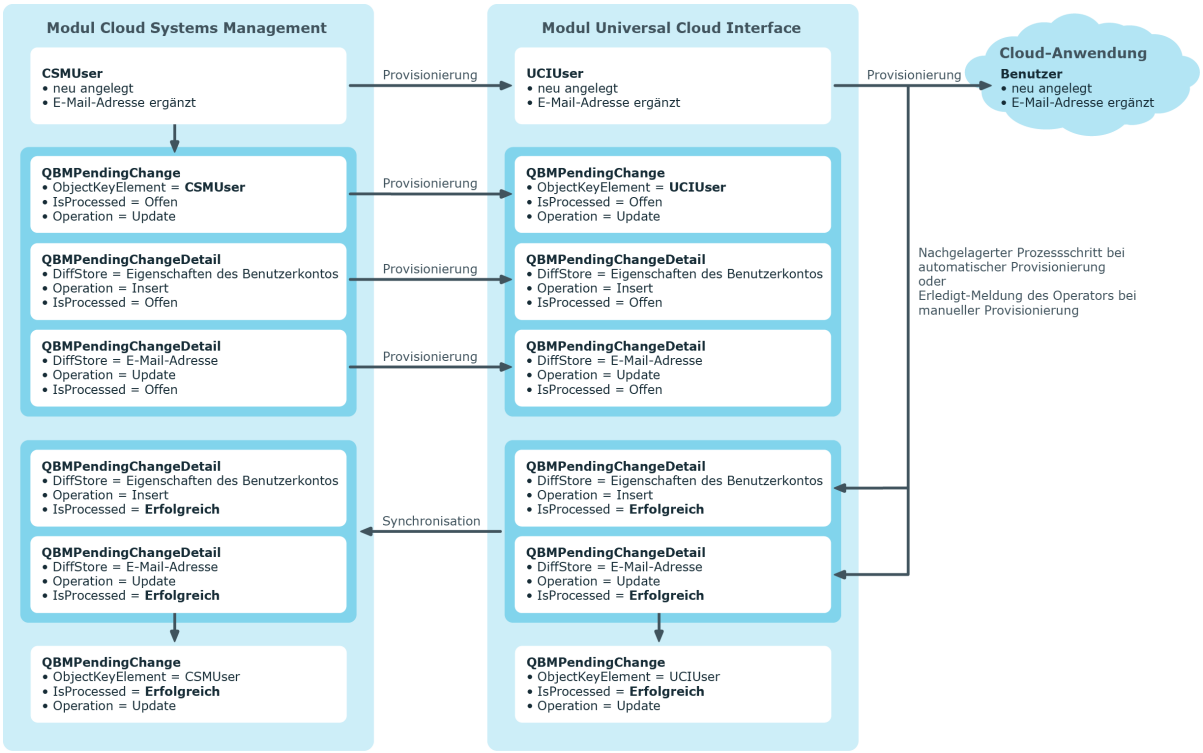
Detaillierte Informationen zum Thema

- Ablauf der Provisionierung auf Seite 47
- Aufbewahrungszeitraum für anstehende Änderungen auf Seite 49

Ablauf der Provisionierung

Folgende Grafik zeigt die Provisionierung von Objektänderungen und die zugehörige Verarbeitung der anstehenden Änderungen. Der Ablauf ist unabhängig davon, ob die Module Cloud Systems Management und Universal Cloud Interface in der selben oder in separaten Datenbanken installiert sind.

Abbildung 2: Ablauf der Provisionierung von anstehenden Änderungen



Standardmäßig wird die Synchronisation zwischen den Modulen Cloud Systems Management und Universal Cloud Interface stündlich ausgeführt. Damit ist sichergestellt, dass der Verarbeitungsstatus für die anstehenden Änderungen zeitnah im Modul Cloud Systems Management bekannt ist.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 47

Anstehende Änderungen anzeigen

Die anstehenden Änderungen können Sie auch im Manager einsehen. Hier werden sowohl die manuellen als auch die automatischen Provisionierungsvorgänge angezeigt.

Um anstehende Änderungen anzuzeigen

- Wählen Sie im Manager das Menü **Datenbank > Anstehende Änderungen**.

Tabelle 10: Bedeutung der Einträge in der Symbolleiste

Symbol	Bedeutung
	Ausgewähltes Objekt anzeigen.
	Ansicht aktualisieren.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 47

Aufbewahrungszeitraum für anstehende Änderungen

Anstehende Änderungen werden für einen festgelegten Zeitraum gespeichert. Nach Ablauf der Frist werden die Einträge durch den DBQueue Prozessor aus den Tabellen `QBMPendingChange` und `QBMPendingChangeDetail` gelöscht. Der Aufbewahrungszeitraum ist vom Verarbeitungsstatus der Provisionierungsvorgänge abhängig und kann über Konfigurationsparameter konfiguriert werden.

Um den Aufbewahrungszeitraum von anstehenden Änderungen zu konfigurieren

1. Um den Aufbewahrungszeitraum für erfolgreiche Provisionierungsvorgänge zu ändern, bearbeiten Sie im Designer den Wert des Konfigurationsparameters **QBM | PendingChange | LifeTimeSuccess**. Erfassen Sie den Aufbewahrungszeitraum in Tagen. Der Standardzeitraum beträgt **2** Tage.
2. Um den Aufbewahrungszeitraum für fehlgeschlagene Provisionierungsvorgänge zu konfigurieren, aktivieren Sie im Designer den Konfigurationsparameter **QBM | PendingChange | LifeTimeError** und erfassen Sie den Aufbewahrungszeitraum in Tagen. Der Standardzeitraum beträgt **30** Tage.
3. Um den Aufbewahrungszeitraum für offene Provisionierungsvorgänge zu konfigurieren, aktivieren Sie im Designer den Konfigurationsparameter **QBM | PendingChange | LifeTimeRunning** und erfassen Sie den Aufbewahrungszeitraum in Tagen. Der Standardzeitraum beträgt **60** Tage.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 47

4

Managen von Cloud Benutzerkonten und Personen

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

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

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

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

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

Verwandte Themen

- Kontendefinitionen für Cloud Benutzerkonten auf Seite 51
- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 74
- Löschverzögerung für Benutzerkonten der Cloud Zielsysteme festlegen auf Seite 87
- Cloud Benutzerkonten erstellen und bearbeiten auf Seite 141

Kontendefinitionen für Cloud Benutzerkonten

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

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

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

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

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 Personen und Zielsysteme

Detaillierte Informationen zum Thema

- Kontendefinition erstellen auf Seite 52
- Kontendefinitionen bearbeiten auf Seite 53
- Stammdaten für Kontendefinitionen auf Seite 53
- Automatisierungsgrade bearbeiten auf Seite 56
- Automatisierungsgrade erstellen auf Seite 57
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 58
- Abbildungsvorschrift für IT Betriebsdaten erstellen auf Seite 59
- IT Betriebsdaten erfassen auf Seite 61
- IT Betriebsdaten ändern auf Seite 62
- Zuweisen der Kontendefinitionen an Personen auf Seite 63
- Kontendefinitionen an Cloud Zielsysteme zuweisen auf Seite 71
- Kontendefinitionen löschen auf Seite 71

Kontendefinition erstellen

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > 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.

Detaillierte Informationen zum Thema

- Stammdaten für Kontendefinitionen auf Seite 53
- Kontendefinitionen bearbeiten auf Seite 53
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 58

Kontendefinitionen bearbeiten

Um eine Kontendefinition zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > 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 für Kontendefinitionen auf Seite 53
- Kontendefinition erstellen auf Seite 52
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 58

Stammdaten für Kontendefinitionen

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 11: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Angabe der vorausgesetzten Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch zugeordnet. Für ein Cloud Zielsystem lassen Sie die Angabe leer.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Personen. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar,

Eigenschaft	Beschreibung
	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 von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.
Automatische Zuweisung zu Personen	Gibt an, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Um die Kontendefinition automatisch an alle internen Personen zuzuweisen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Personen aktivieren**. Die Kontendefinition wird an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine neue interne Person erstellt wird, erhält diese Person ebenfalls automatisch diese Kontendefinition. Um die automatische Zuweisung der Kontendefinition von allen Personen zu entfernen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Personen deaktivieren**. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam.

Eigenschaft	Beschreibung
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam.
Kontendefinition bei verzögertem Löschen beibehalten	Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam.
Kontendefinition bei Sicherheitsgefährdung beibehalten	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam.
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.
Gruppen erbbar	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.
Systemberechtigungen 1 erbbar	Gibt an, ob das Benutzerkonto Systemberechtigungen des entsprechenden Typs über die verbundene Person erben darf. Ist die Option aktiviert, werden Systemberechtigungen über

Eigenschaft	Beschreibung
Systemberechtigungen 2 erbbar	hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.
Systemberechtigungen 3 erbbar	• Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Systemberechtigungen zugewiesen haben, dann erbt das Benutzerkonto diese Systemberechtigungen. • Wenn eine Person eine Zuweisung zu einer Systemberechtigung im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Systemberechtigung nur, wenn die Option aktiviert ist.

Automatisierungsgrade bearbeiten

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

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

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

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

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

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > 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 für Automatisierungsgrade auf Seite 58
- Automatisierungsgrade erstellen auf Seite 57
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 58

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 **Cloud Zielsysteme > 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 für Automatisierungsgrade auf Seite 58
- Automatisierungsgrade bearbeiten auf Seite 56
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 58

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 **Cloud Zielsysteme > 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 für Automatisierungsgrade

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 12: 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.

Eigenschaft	Beschreibung
	(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 Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Gibt an, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei dauerhafter Deaktivierung sperren	Gibt an, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.
Gruppen bei verzögertem Löschen beibehalten	Gibt an, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren	Gibt an, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Gibt an, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Gibt an, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

Abbildungsvorschrift für IT Betriebsdaten erstellen

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

- Container (je Zielsystem)
- Gruppen erbbar
- Identität
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > 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 Person, 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 **Person - Erstellung neues Benutzerkontos mit Standardwerten** verwendet.

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

Verwandte Themen

- IT Betriebsdaten erfassen auf Seite 61

IT Betriebsdaten erfassen

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

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

Beispiel:

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

Erstellen Sie eine Kontendefinition A für die Standardbenutzerkonten des Cloud Zielsystems A und eine Kontendefinition B für die administrativen Benutzerkonten des Cloud Zielsystems 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 das Cloud Zielsystem 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

- Abbildungsvorschrift für IT Betriebsdaten erstellen auf Seite 59

IT Betriebsdaten ändern

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

Voraussetzungen

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

  - ODER -

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

HINWEIS: Ändert sich die Zuordnung einer Person zu einer primären Abteilung, Kostenstelle, 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 **Cloud Zielsysteme > 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 Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

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

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

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

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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 65
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 65
- Kontendefinitionen an alle Personen zuweisen auf Seite 66
- Kontendefinitionen direkt an Personen zuweisen auf Seite 67
- Kontendefinitionen an Systemrollen zuweisen auf Seite 68

- Kontendefinitionen in den IT Shop aufnehmen auf Seite 68
- Kontendefinitionen an Cloud Zielsysteme zuweisen auf Seite 71

Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > 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 65
- Kontendefinitionen an alle Personen zuweisen auf Seite 66
- Kontendefinitionen direkt an Personen zuweisen auf Seite 67
- Kontendefinitionen an Systemrollen zuweisen auf Seite 68
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 68

Kontendefinitionen an Geschäftsrollen zuweisen

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

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > 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 65
- Kontendefinitionen an alle Personen zuweisen auf Seite 66
- Kontendefinitionen direkt an Personen zuweisen auf Seite 67
- Kontendefinitionen an Systemrollen zuweisen auf Seite 68
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 68

Kontendefinitionen an alle Personen zuweisen

Über diese Aufgaben wird die Kontendefinition an alle internen Personen zugewiesen. Personen, die als externe Personen gekennzeichnet sind, erhalten die Kontendefinition nicht. Sobald eine neue interne Person erstellt wird, erhält diese Person 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 Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen!

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > 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 Personen aktivieren**.

5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Speichern Sie die Änderungen.

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

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 65
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 65
- Kontendefinitionen direkt an Personen zuweisen auf Seite 67
- Kontendefinitionen an Systemrollen zuweisen auf Seite 68
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 68

Kontendefinitionen direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 65
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 65
- Kontendefinitionen an alle Personen zuweisen auf Seite 66
- Kontendefinitionen an Systemrollen zuweisen auf Seite 68
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 68

Kontendefinitionen an Systemrollen zuweisen

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

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 **Cloud Zielsysteme > 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 65
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 65
- Kontendefinitionen an alle Personen zuweisen auf Seite 66
- Kontendefinitionen direkt an Personen zuweisen auf Seite 67
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 68

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 Personen zugewiesen werden können, muss sie zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.

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

Um eine Kontendefinition in den IT Shop aufzunehmen (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 **Cloud Zielsysteme > 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 **Cloud Zielsysteme > 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 **Cloud Zielsysteme > 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 für Kontendefinitionen auf Seite 53
- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 65
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 65
- Kontendefinitionen direkt an Personen zuweisen auf Seite 67
- Kontendefinitionen an Systemrollen zuweisen auf Seite 68

Kontendefinitionen an Cloud Zielsysteme zuweisen

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **Cloud Zielsysteme** das Zielsystem.
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.

Für kundendefinierte Zielsysteme müssen Sie die automatische Zuordnung von Personen zu Benutzerkonten kundenspezifisch implementieren.

Detaillierte Informationen zum Thema

- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 74

Kontendefinitionen löschen

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

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > 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 Personen deaktivieren**.

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

f. Speichern Sie die Änderungen.

2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.

   a. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **An Personen zuweisen**.

   d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.

   e. Speichern Sie die Änderungen.

3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorten.

   a. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > 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 **Cloud Zielsysteme > 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 **Cloud Zielsysteme > 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 **Cloud Zielsysteme > 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 **Cloud Zielsysteme** das Zielsystem.

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 **Cloud Zielsysteme > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Klicken Sie , um die Kontendefinition zu löschen.

Automatische Zuordnung von Personen zu Benutzerkonten

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

Für die automatische Personenzuordnung definieren Sie Kriterien für die Ermittlung der Personen. Wird durch den eingesetzten Modus ein Benutzerkonto mit einer Person verbunden, so erhält das Benutzerkonto durch interne Verarbeitung den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

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

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

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

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

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

  Beispiel:

```
ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $
```

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

Um die Ausschlussliste für die automatische Personenzuordnung zu bearbeiten

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

   Der Dialog **Ausschlussliste für die automatische Personenzuordnung** 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 Personen 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**.

- Weisen Sie dem Cloud Zielsystem eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Personenzuordnung am Cloud Zielsystem.

HINWEIS:

Für die Synchronisation gilt:

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

Außerhalb der Synchronisation gilt:

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

HINWEIS:

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

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

Weitere Informationen finden Sie unter Cloud Benutzerkonten über Kontendefinitionen verwalten auf Seite 44.

Verwandte Themen

- Kontendefinition erstellen auf Seite 52
- Kontendefinitionen an Cloud Zielsysteme zuweisen auf Seite 71
- Automatisierungsgrade für Cloud Benutzerkonten ändern auf Seite 79
- Suchkriterien für die automatische Personenzuordnung bearbeiten auf Seite 76
- Personen suchen und direkt an Benutzerkonten zuordnen auf Seite 77

Suchkriterien für die automatische Personenzuordnung bearbeiten

Die Kriterien für die Personenzuordnung werden an den Zielsystemen definiert. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person dem Benutzerkonto zugeordnet werden kann. Die Suchkriterien können Sie durch Formatdefinitionen weiter einschränken.

Das zusammengestellte Suchkriterium wird in XML-Notation in die Spalte **Suchkriterien für die automatische Personenzuordnung** (`AccountToPersonMatchingRule`) der Tabelle `CSMRoot` geschrieben.

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

HINWEIS: 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 die Kriterien für die Personenzuordnung für ein Cloud Zielsystem zu definieren

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > Basisdaten zur Konfiguration > Cloud Zielsysteme**.
2. Wählen Sie in der Ergebnisliste das Zielsystem.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person mit dem

Benutzerkonto verbunden wird.

Tabelle 13: Beispiel für die Suchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
Cloud Benutzerkonten	Vorname (FirstName) UND Nachname (LastName)	Vorname (FirstName) UND Nachname (LastName)

5. Speichern Sie die Änderungen.

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

Verwandte Themen

- Personen suchen und direkt an Benutzerkonten zuordnen auf Seite 77
- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 74

Personen suchen und direkt an Benutzerkonten zuordnen

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

Tabelle 14: Ansichten zur manuellen Zuordnung

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

Um Suchkriterien auf die Benutzerkonten anzuwenden

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem>**.
2. Wählen Sie in der Ergebnisliste das Zielsystem.

3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung 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 Person geöffnet und Sie können die Stammdaten einsehen.

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

Um Personen direkt über die Vorschlagsliste zuzuordnen

- Klicken Sie **Vorgeschlagene Zuordnungen**.
  1. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die vorgeschlagene Person 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 Personen zugeordnet. Wenn eine Kontendefinition ausgewählt wurde, wird diese an alle ausgewählten Benutzerkonten zugeordnet.

  - ODER -

- Klicken Sie **Ohne Personenzuordnung**.
  1. Klicken Sie **Person auswählen** für das Benutzerkonto, dem eine Person zugeordnet werden soll. Wählen Sie eine Person aus der Auswahlliste.
  2. Klicken Sie **Auswahl** für alle Benutzerkonten, denen die ausgewählten Personen 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 Personen zugeordnet, die in der Spalte **Person** 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 Personenzuordnung 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 Personen entfernt.

Automatisierungsgrade für Cloud Benutzerkonten ändern

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

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > 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

- Cloud Benutzerkonten erstellen und bearbeiten auf Seite 141

Unterstützte Typen von Benutzerkonten

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

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität

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

Tabelle 15: Identitäten von Benutzerkonten

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

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

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

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

Benutzerkonten mit einer Zusatzidentität, einer Gruppenidentität oder einer Dienstidentität verbinden Sie mit Pseudo-Personen, die keinen Bezug zu einer realen Person haben. Diese Pseudo-Personen werden benötigt, um Berechtigungen an die Benutzerkonten vererben zu können. Bei der Auswertung von Berichten,

Attestierungen oder Complianceprüfungen prüfen Sie, ob die Pseudo-Personen gesondert betrachtet werden müssen.

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

- Privilegiertes Benutzerkonto

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

Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 81
- Administrative Benutzerkonten auf Seite 82
- Administratives Benutzerkonto für eine Person bereitstellen auf Seite 83
- Administratives Benutzerkonto für mehrere Personen bereitstellen auf Seite 84
- Privilegierte Benutzerkonten auf Seite 85

Standardbenutzerkonten

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

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

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

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

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

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

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

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

5. Weisen Sie die Kontendefinition an die Personen zu.

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

Verwandte Themen

- Kontendefinitionen für Cloud Benutzerkonten auf Seite 51

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

- Administratives Benutzerkonto für eine Person bereitstellen auf Seite 83
- Administratives Benutzerkonto für mehrere Personen bereitstellen auf Seite 84

Administratives Benutzerkonto für eine Person bereitstellen

Voraussetzungen

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

Um ein administratives Benutzerkonto für eine Person bereitzustellen

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

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

Verwandte Themen

- Administratives Benutzerkonto für mehrere Personen bereitstellen auf Seite 84
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administratives Benutzerkonto für mehrere Personen bereitstellen

Voraussetzung

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

Um ein administratives Benutzerkonto für mehrere Personen bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als Gruppenidentität.
    a. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > 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 Pseudo-Person.
    a. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Pseudo-Person.

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Person und doppelklicken Sie ✓.

Verwandte Themen

- Administratives Benutzerkonto für eine Person bereitstellen auf Seite 83
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Privilegierte Benutzerkonten

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

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

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

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

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

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

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsPrivilegedAccount` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert**

verwenden.

- Zusätzlich können Sie eine Abbildungsvorschrift für die Spalte `IdentityType` festlegen. Die Spalte besitzt verschiedene zulässige Werte, die privilegierte Benutzerkonten repräsentieren.
- Um zu verhindern, das privilegierte Benutzerkonten die Berechtigungen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschrift für die Spalte `IsGroupAccount` mit dem Standardwert **0** und aktivieren Sie die Option **Immer Standardwert verwenden**.

5. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem.

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

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

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

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

- Um ein Präfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | CSM | Accounts | PrivilegedAccount | SAMAccountName_Prefix**.
- Um ein Postfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | CSM | Accounts | PrivilegedAccount | SAMAccountName_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 Cloud Benutzerkonten auf Seite 51

Löschverzögerung für Benutzerkonten der Cloud Zielsysteme 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.
- Zielsystemspezifische Löschverzögerung: Die Löschverzögerung kann je Zielsystem individuell konfiguriert werden. Diese Löschverzögerung überschreibt die globale Löschverzögerung.

Um eine individuelle Löschverzögerung je Zielsystem zu ermöglichen

1. Konfigurieren Sie im Manager die Löschverzögerungen für die Zielsysteme.
    a. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > Basisdaten zur Konfiguration > Cloud Zielsysteme**.
    b. Wählen Sie in der Ergebnisliste ein Zielsystem und wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    c. Auf dem Tabreiter **Allgemein** erfassen Sie unter **Löschverzögerung [Tage]** die Löschverzögerung für das Zielsystem in Tagen.
    d. Speichern Sie die Änderungen.
2. Erstellen Sie im Designer für die Tabelle `CSMUser` ein **Skript (Löschverzögerung)**.

> **Beispiel:**
>
> Die Löschverzögerung der Benutzerkonten in einem Cloud Zielsystem soll von der Löschverzögerung des Zielsystems (`CSMRoot.DeleteDelayDays`) abhängig sein. An der Tabelle `CSMUser` wird folgendes Skript eingetragen.
>
> ```
> If $FK(UID_CSMRoot).DeleteDelayDays:Int$ > 0 Then
> ```

```
      Value = $FK(UID_CSMRoot).DeleteDelayDays:Int$
End If
```

- 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 `CSMUser` 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*.

Verwandte Themen

- Allgemeine Stammdaten für Cloud Zielsysteme auf Seite 134
- Cloud Benutzerkonten löschen auf Seite 151

Managen der Zuweisungen von Cloud Gruppen und Cloud Systemberechtigungen

Gruppen und Systemberechtigungen bilden die Objekte ab, über die in der Cloud-Anwendung der Zugriff auf die Cloud-Ressourcen gesteuert wird. Ein Benutzerkonto erhält durch die Zuweisung zu Gruppen und Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Cloud-Ressourcen.

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

Detaillierte Informationen zum Thema

- Typen von Systemberechtigungen in Cloud Zielsystemen auf Seite 89
- Zuweisen von Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten im One Identity Manager auf Seite 92
- Wirksamkeit von Mitgliedschaften in Cloud Gruppen und Systemberechtigungen auf Seite 111
- Vererbung von Cloud Gruppen und Systemberechtigungen anhand von Kategorien auf Seite 114
- Übersicht aller Zuweisungen auf Seite 116

Typen von Systemberechtigungen in Cloud Zielsystemen

Viele Cloud-Anwendungen nutzen verschiedene Berechtigungstypen, um Benutzerberechtigungen zu administrieren. Das können neben Gruppen beispielsweise auch Rollen oder Berechtigungssets sein. Über Synchronisationsprojekte, die mit der

Standard-Projektvorlage erstellt wurden, werden die verschiedenen Typen folgendermaßen im One Identity Manager abgebildet.

Tabelle 16: Abbildung von Systemberechtigungen im Modul Cloud Systems Management

Tabelle im Universal Cloud Interface	Tabelle im Modul Cloud Systems Management	Anzeigename
UCIGroup	CSMGroup	Gruppen
UCIGroup1	CSMGroup1	Systemberechtigungen 1
UCIGroup2	CSMGroup2	Systemberechtigungen 2
UCIGroup3	CSMGroup3	Systemberechtigungen 3
UCIItem	CSMItem	Berechtigungselemente

Ein Benutzerkonto erhält über seine Zuweisungen zu den Gruppen oder Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Zielsystemressourcen. Abhängig vom Zielsystem werden die Zuweisungen entweder an den Benutzerkonten (benutzerbasierte Zuweisung) oder an den Systemberechtigungen (berechtigungsbasierte Zuweisung) gepflegt. Beim Einrichten der Synchronisation mit der Standard-Projektvorlage ermittelt der Universal Cloud Interface Konnektor, an welchem Objekttyp die Zuweisungen gespeichert sind. Die Zuweisungen werden in den folgenden Tabellen abgebildet:

Tabelle 17: Benutzerbasierte Zuweisung

CSMUserHasGroup	**Gruppen: Zuweisungen zu Benutzerkonten**
CSMUserHasGroup1	**Systemberechtigungen 1: Zuweisungen zu Benutzerkonten**
CSMUserHasGroup2	**Systemberechtigungen 2: Zuweisungen zu Benutzerkonten**
CSMUserHasGroup3	**Systemberechtigungen 3: Zuweisungen zu Benutzerkonten**
CSMUserHasItem	**Benutzerkonten: Zuweisungen Berechtigungselemente**

Tabelle 18: Berechtigungsbasierte Zuweisung

CSMUserInGroup	**Benutzerkonten: Zuweisungen zu Gruppen**
CSMUserInGroup1	**Benutzerkonten: Zuweisungen zu Systemberechtigungen 1**
CSMUserInGroup2	**Benutzerkonten: Zuweisungen zu Systemberechtigungen 2**
CSMUserInGroup3	**Benutzerkonten: Zuweisungen zu Systemberechtigungen 3**

Zuweisungen zu Berechtigungselementen sind immer benutzerbasiert.

An den Cloud Zielsystemen ist hinterlegt, welche Typen von Systemberechtigungen verwendet werden und ob die Zuweisungen an den Benutzerkonten oder den Systemberechtigungen gespeichert werden.

Um die verwendeten Typen von Systemberechtigungen anzuzeigen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > Basisdaten zur Konfiguration > Cloud Zielsysteme**.
2. Wählen Sie in der Ergebnisliste ein Cloud Zielsystem und wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    - **Typen der verwendeten Systemberechtigungen**: Liste der im Cloud Zielsystem verwendeten Typen von Systemberechtigungen.
    - **Benutzerkonto enthält Mitgliedschaften**: Liste der Typen von Systemberechtigungen mit benutzerbasierten Zuweisungen. Für Typen, die hier nicht aufgelistet sind, werden die Zuweisungen an den Systemberechtigungen gespeichert.

TIPP: Wenn das Schema der Cloud-Anwendung nicht durch die Standard-Projektvorlage ausreichend abgebildet werden kann, passen Sie die Synchronisationskonfiguration an. Definieren Sie dabei, wie die Systemberechtigungen im One Identity Manager Schema abgebildet werden. Stellen Sie sicher, dass bei der Einrichtung der Synchronisation das Basisobjekt für die Cloud-Anwendung (`CSMRoot`) in der Datenbank angelegt wird und die Eigenschaften **Typen der verwendeten Systemberechtigungen** (`GroupUsageMask`) und **Benutzerkonto enthält Mitgliedschaften** (`UserContainsGroupList`) korrekt gesetzt werden.

HINWEIS: Wenn Sie Attestierungsverfahren, Complianceregeln oder Unternehmensrichtlinien über Systemberechtigungen einrichten, achten Sie darauf, die korrekten Zuweisungstabellen auszuwählen, um sowohl benutzerbasierte als auch berechtigungsbasierte Zuweisungen zu betrachten.

Um die Funktionen unabhängig von der Konfiguration der Zielsysteme einzurichten, nutzen Sie die Abbildung der Zielsysteme im Unified Namespace. In der Tabelle `UNSAccountInUNSGroup` sind sowohl benutzerbasierte als auch berechtigungsbasierte Zuweisungen für alle Typen von Systemberechtigungen abgebildet; die Tabelle `UNSGroup` enthält alle Systemberechtigungen unabhängig vom Typ.

Ausführliche Informationen zum Unified Namespace finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Ausführliche Informationen zur Attestierungsfunktion, zu Complianceregeln und Unternehmensrichtlinien finden Sie in folgenden Handbüchern:

One Identity Manager Administrationshandbuch für Attestierungen
One Identity Manager Administrationshandbuch für Complianceregeln
One Identity Manager Administrationshandbuch für Unternehmensrichtlinien

Verwandte Themen

- Allgemeine Stammdaten für Cloud Zielsysteme auf Seite 134

Zuweisen von Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten im One Identity Manager

Cloud Gruppen und Systemberechtigungen können direkt oder indirekt an Personen zugewiesen werden.

Bei der indirekten Zuweisung werden Personen sowie Gruppen und Systemberechtigungen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Gruppen und Systemberechtigungen, die einer Person zugewiesen ist. Wenn Sie eine Person in hierarchische Rollen aufnehmen und die Person ein Cloud Benutzerkonto besitzt, dann wird dieses Benutzerkonto an die Cloud Gruppen und Systemberechtigungen zugewiesen.

Des Weiteren können Cloud Gruppen und Systemberechtigungen im Web Portal bestellt werden. Dazu werden Personen als Kunden in einen Shop aufgenommen. Alle Cloud Gruppen und Systemberechtigungen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Cloud Gruppen und Systemberechtigungen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

Über Systemrollen können Cloud Gruppen und Systemberechtigungen zusammengefasst und als Paket an Personen zugewiesen werden. Sie können Systemrollen erstellen, die ausschließlich Cloud Gruppen oder Systemberechtigungen enthalten. Ebenso können Sie in einer Systemrolle beliebige Unternehmensressourcen zusammenfassen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Cloud Gruppen und Systemberechtigungen auch direkt an Benutzerkonten zuweisen.

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 Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten auf Seite 93

- Cloud Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 94
- Cloud Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- Cloud Gruppen an Geschäftsrollen zuweisen auf Seite 97
- Cloud Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 99
- Cloud Gruppen in Systemrollen aufnehmen auf Seite 100
- Cloud Systemberechtigungen in Systemrollen aufnehmen auf Seite 101
- Cloud Gruppen in den IT Shop aufnehmen auf Seite 102
- Cloud Systemberechtigungen in den IT Shop aufnehmen auf Seite 104
- Cloud Benutzerkonten direkt an Cloud Gruppen zuweisen auf Seite 107
- Cloud Benutzerkonten direkt an Cloud Systemberechtigungen zuweisen auf Seite 108
- Cloud Gruppen direkt an Cloud Benutzerkonten zuweisen auf Seite 109
- Cloud Systemberechtigungen direkt an Cloud Benutzerkonten zuweisen auf Seite 110

Voraussetzungen für indirekte Zuweisungen von Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten

Bei der indirekten Zuweisung werden Personen sowie Cloud Gruppen Systemberechtigungen in hierarchische Rollen eingeordnet. Für die indirekte Zuweisung von Cloud Gruppen und Systemberechtigungen 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 Personen und Cloud Gruppen und Systemberechtigungen erlaubt.

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

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

   a. 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.

   b. 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**.

c. Speichern Sie die Änderungen.

2. Einstellungen für die Zuweisung von Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten.
   - Die Cloud Benutzerkonten sind mit Personen verbunden.
   - Die Cloud Benutzerkonten sind mit der Option **Gruppen erbbar**, **Systemberechtigungen 1 erbbar**, **Systemberechtigungen 2 erbbar**, **Systemberechtigungen 3 erbbar** gekennzeichnet.
   - Die Cloud Benutzerkonten, Cloud Gruppen und Systemberechtigungen gehören zum selben Zielsystem.

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 Personen 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

- Cloud Benutzerkonten erstellen und bearbeiten auf Seite 141
- Allgemeine Stammdaten für Cloud Benutzerkonten auf Seite 142

Cloud Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen

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

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

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > 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 **Cloud Gruppen und Systemberechtigungen zuweisen**.
4. Wählen Sie den Tabreiter **Cloud Gruppen**.
5. 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 ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten auf Seite 93
- Cloud Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- Cloud Benutzerkonten direkt an Cloud Gruppen zuweisen auf Seite 107
- Cloud Gruppen in Systemrollen aufnehmen auf Seite 100
- Cloud Gruppen in den IT Shop aufnehmen auf Seite 102
- Cloud Gruppen an Geschäftsrollen zuweisen auf Seite 97

- Cloud Gruppen direkt an Cloud Benutzerkonten zuweisen auf Seite 109
- One Identity Manager Benutzer für die Verwaltung von Cloud Zielsystemen auf Seite 11

Cloud Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie eine Systemberechtigung an Abteilungen, Kostenstellen oder Standorte zu, damit die Systemberechtigung über diese Organisationen an Benutzerkonten vererbt wird.

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

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
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 Systemberechtigungen 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 **Cloud Gruppen und Systemberechtigungen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemberechtigungen zu.
   - Weisen Sie auf dem Tabreiter **Cloud Systemberechtigungen 1** die Systemberechtigungen 1 zu.
   - Weisen Sie auf dem Tabreiter **Cloud Systemberechtigungen 2** die Systemberechtigungen 2 zu.
   - Weisen Sie auf dem Tabreiter **Cloud Systemberechtigungen 3** die Systemberechtigungen 3 zu.

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

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten auf Seite 93
- Cloud Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 94
- Cloud Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 99
- Cloud Systemberechtigungen in Systemrollen aufnehmen auf Seite 101
- Cloud Systemberechtigungen in den IT Shop aufnehmen auf Seite 104
- Cloud Benutzerkonten direkt an Cloud Systemberechtigungen zuweisen auf Seite 108
- Cloud Systemberechtigungen direkt an Cloud Benutzerkonten zuweisen auf Seite 110

Cloud Gruppen an Geschäftsrollen zuweisen

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

Weisen Sie Gruppen an Geschäftsrollen zu, damit sie über diese Geschäftsrollen an Benutzerkonten zugewiesen werden.

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

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > 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 **Cloud Gruppen und Systemberechtigungen zuweisen**.
4. Wählen Sie den Tabreiter **Cloud Gruppen**.
5. 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 ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten auf Seite 93
- Cloud Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 99
- Cloud Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 94
- Cloud Gruppen in Systemrollen aufnehmen auf Seite 100
- Cloud Gruppen in den IT Shop aufnehmen auf Seite 102
- Cloud Benutzerkonten direkt an Cloud Gruppen zuweisen auf Seite 107

- Cloud Gruppen direkt an Cloud Benutzerkonten zuweisen auf Seite 109
- One Identity Manager Benutzer für die Verwaltung von Cloud Zielsystemen auf Seite 11

Cloud Systemberechtigungen an Geschäftsrollen zuweisen

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

Weisen Sie eine Systemberechtigung an Geschäftsrollen zu, damit die Systemberechtigung über diese Geschäftsrollen an Benutzerkonten vererbt wird.

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

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
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 Systemberechtigungen 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 **Cloud Gruppen und Systemberechtigungen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemberechtigungen zu.

- Weisen Sie auf dem Tabreiter **Cloud Systemberechtigungen 1** die Systemberechtigungen 1 zu.
- Weisen Sie auf dem Tabreiter **Cloud Systemberechtigungen 2** die Systemberechtigungen 2 zu.
- Weisen Sie auf dem Tabreiter **Cloud Systemberechtigungen 3** die Systemberechtigungen 3 zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Systemberechtigung und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten auf Seite 93
- Cloud Gruppen an Geschäftsrollen zuweisen auf Seite 97
- Cloud Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- Cloud Systemberechtigungen in Systemrollen aufnehmen auf Seite 101
- Cloud Systemberechtigungen in den IT Shop aufnehmen auf Seite 104
- Cloud Benutzerkonten direkt an Cloud Systemberechtigungen zuweisen auf Seite 108
- Cloud Systemberechtigungen direkt an Cloud Benutzerkonten zuweisen auf Seite 110

Cloud 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 Personen zuweisen, wird die Gruppe an alle Benutzerkonten vererbt, die diese Personen besitzen.

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 **Cloud Zielsysteme > <Zielsystem> > 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 Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten auf Seite 93
- Cloud Systemberechtigungen in Systemrollen aufnehmen auf Seite 101
- Cloud Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 94
- Cloud Gruppen an Geschäftsrollen zuweisen auf Seite 97
- Cloud Gruppen in den IT Shop aufnehmen auf Seite 102
- Cloud Benutzerkonten direkt an Cloud Gruppen zuweisen auf Seite 107
- Cloud Gruppen direkt an Cloud Benutzerkonten zuweisen auf Seite 109

Cloud Systemberechtigungen in Systemrollen aufnehmen

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

Mit dieser Aufgabe nehmen Sie eine Systemberechtigung in Systemrollen auf.

Wenn Sie eine Systemrolle an Personen zuweisen, wird die Systemberechtigung an alle Benutzerkonten des kundendefinierten Zielsystems vererbt, die diese Personen besitzen.

HINWEIS: Systemberechtigungen, 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 Systemberechtigung an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

- ODER -

Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
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 Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten auf Seite 93
- Cloud Gruppen in Systemrollen aufnehmen auf Seite 100
- Cloud Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- Cloud Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 99
- Cloud Systemberechtigungen in den IT Shop aufnehmen auf Seite 104
- Cloud Benutzerkonten direkt an Cloud Systemberechtigungen zuweisen auf Seite 108
- Cloud Systemberechtigungen direkt an Cloud Benutzerkonten zuweisen auf Seite 110

Cloud 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 muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Gruppe muss eine Leistungsposition zugeordnet sein.

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Gruppe im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.
- Soll die Gruppe nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Gruppe zusätzlich mit der Option **Verwendung nur im IT Shop**

gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen oder Benutzerkonten ist dann nicht mehr zulässig.

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

Um eine Gruppe in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud 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 **Cloud Zielsysteme > <Zielsystem> > Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud 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 **Cloud Zielsysteme > <Zielsystem> > Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud 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 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 Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten auf Seite 93
- Allgemeine Stammdaten für Cloud Gruppen auf Seite 154
- Cloud Systemberechtigungen in den IT Shop aufnehmen auf Seite 104
- Cloud Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 94
- Cloud Gruppen an Geschäftsrollen zuweisen auf Seite 97
- Cloud Gruppen in Systemrollen aufnehmen auf Seite 100
- Cloud Benutzerkonten direkt an Cloud Gruppen zuweisen auf Seite 107
- Cloud Gruppen direkt an Cloud Benutzerkonten zuweisen auf Seite 109

Cloud Systemberechtigungen in den IT Shop aufnehmen

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

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

  TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Systemberechtigung im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.
- Soll die Systemberechtigung nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Systemberechtigung 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 Systemberechtigungen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Systemberechtigungen in den IT Shop aufzunehmen.

Um eine Systemberechtigung in den IT Shop aufzunehmen

1. Bei nicht-rollenbasierter Anmeldung:

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

   Bei rollenbasierter Anmeldung:

   Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
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 Systemberechtigung an die IT Shop Regale zu.
6. Speichern Sie die Änderungen.

Um eine Systemberechtigung aus einzelnen Regalen des IT Shops zu entfernen

1. Bei nicht-rollenbasierter Anmeldung:

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

   Bei rollenbasierter Anmeldung:

Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud Systemberechtigungen 1**.

- ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud Systemberechtigungen 2**.

- ODER -

Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud Systemberechtigungen 3**.

2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
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 Systemberechtigung aus den IT Shop Regalen.
6. Speichern Sie die Änderungen.

Um eine Systemberechtigung aus allen Regalen des IT Shops zu entfernen

1. Bei nicht-rollenbasierter Anmeldung:

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

   Bei rollenbasierter Anmeldung:

   Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > Cloud Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

Die Systemberechtigung wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Systemberechtigung 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 Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten auf Seite 93
- Allgemeine Stammdaten für Cloud Gruppen auf Seite 154
- Cloud Gruppen in den IT Shop aufnehmen auf Seite 102
- Cloud Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- Cloud Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 99
- Cloud Systemberechtigungen in Systemrollen aufnehmen auf Seite 101
- Cloud Benutzerkonten direkt an Cloud Systemberechtigungen zuweisen auf Seite 108
- Cloud Systemberechtigungen direkt an Cloud Benutzerkonten zuweisen auf Seite 110

Cloud Benutzerkonten direkt an Cloud Gruppen zuweisen

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

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

Um Benutzerkonten direkt an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > 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

- Cloud Benutzerkonten direkt an Cloud Systemberechtigungen zuweisen auf Seite 108
- Cloud Gruppen direkt an Cloud Benutzerkonten zuweisen auf Seite 109
- Cloud Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 94
- Cloud Gruppen an Geschäftsrollen zuweisen auf Seite 97
- Cloud Gruppen in Systemrollen aufnehmen auf Seite 100
- Cloud Gruppen in den IT Shop aufnehmen auf Seite 102

Cloud Benutzerkonten direkt an Cloud Systemberechtigungen zuweisen

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

Um Benutzerkonten direkt an eine Systemberechtigung zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
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

- Cloud Benutzerkonten direkt an Cloud Gruppen zuweisen auf Seite 107
- Cloud Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- Cloud Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 99
- Cloud Systemberechtigungen in Systemrollen aufnehmen auf Seite 101
- Cloud Systemberechtigungen in den IT Shop aufnehmen auf Seite 104
- Cloud Systemberechtigungen direkt an Cloud Benutzerkonten zuweisen auf Seite 110

Cloud Gruppen direkt an Cloud Benutzerkonten zuweisen

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

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Cloud Gruppen und Systemberechtigungen zuweisen**.
4. Wählen Sie den Tabreiter **Cloud Gruppen**.
5. 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 ✓.
6. Speichern Sie die Änderungen.

HINWEIS: Die primäre Gruppe eines Benutzerkontos ist bereits zugewiesen und wird als **Noch nicht wirksam** gekennzeichnet. Um die primäre Gruppe eines Benutzerkontos zu ändern, bearbeiten Sie die Stammdaten des Benutzerkontos.

Verwandte Themen

- Zuweisen von Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten im One Identity Manager auf Seite 92

- Cloud Systemberechtigungen direkt an Cloud Benutzerkonten zuweisen auf Seite 110
- Cloud Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 94
- Cloud Gruppen an Geschäftsrollen zuweisen auf Seite 97
- Cloud Gruppen in Systemrollen aufnehmen auf Seite 100
- Cloud Gruppen in den IT Shop aufnehmen auf Seite 102

Cloud Systemberechtigungen direkt an Cloud Benutzerkonten zuweisen

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

Um Systemberechtigungen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Cloud Gruppen und Systemberechtigungen zuweisen**.
4. Wählen Sie den Tabreiter **Cloud Systemberechtigungen 1**.

   - ODER -

   Wählen Sie den Tabreiter **Cloud Systemberechtigungen 2**.

   - ODER -

   Wählen Sie den Tabreiter **Cloud Systemberechtigungen 3**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemberechtigungen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemberechtigung und doppelklicken Sie ✓.
6. Speichern Sie die Änderungen.

Verwandte Themen

- Cloud Gruppen direkt an Cloud Benutzerkonten zuweisen auf Seite 109
- Cloud Systemberechtigungen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 96
- Cloud Systemberechtigungen an Geschäftsrollen zuweisen auf Seite 99
- Cloud Systemberechtigungen in Systemrollen aufnehmen auf Seite 101

- Cloud Systemberechtigungen in den IT Shop aufnehmen auf Seite 104
- Cloud Benutzerkonten direkt an Cloud Systemberechtigungen zuweisen auf Seite 108

Wirksamkeit von Mitgliedschaften in Cloud Gruppen und Systemberechtigungen

HINWEIS: Die hier für Gruppen beschriebene Funktionalität gilt gleichermaßen für die Systemberechtigungen.

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

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

HINWEIS:

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

Die Wirksamkeit der Zuweisungen wird in den Tabellen CSMUserInGroup/CSMUserHasGroup und CSMBaseTreeHasGroup über die Spalte XIsInEffect abgebildet.

Beispiel: Wirksamkeit von Gruppenmitgliedschaften

- 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 Zielsystem. Sie gehört primär der Abteilung "Marketing" an. Sekundär sind ihr die Geschäftsrolle "Kontrollgruppe" und

die Abteilung "Finanzen" zugewiesen. Ohne Ausschlussdefinition erhält das Benutzerkonto alle Berechtigungen der Gruppen A, B und C.

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

Tabelle 19: Festlegen der ausgeschlossenen Gruppen (Tabelle `CSMGroupExclusion`)

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

Tabelle 20: Wirksame Zuweisungen

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

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

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

Tabelle 21: Ausgeschlossene Gruppen und wirksame Zuweisungen

Person	Mitglied in Rolle	Zugewiesene Gruppe	Ausgeschlossene Gruppe	Wirksame Gruppe
Jenny Basset	Marketing	Gruppe A		Gruppe C
	Kontrollgruppe	Gruppe C	Gruppe B 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 Cloud Zielsystem.

Um Gruppen auszuschließen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > 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.

Um Systemberechtigungen auszuschließen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste eine Systemberechtigung.
3. Passend zur gewählten Systemberechtigung, wählen Sie die Aufgabe **Systemberechtigungen 1 ausschließen**, **Systemberechtigungen 2 ausschließen** oder **Systemberechtigungen 3 ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemberechtigungen zu, die sich mit der gewählten Systemberechtigung ausschließen.

- ODER -

Entfernen Sie im Bereich **Zuordnungen entfernen** die Systemberechtigungen, die sich nicht länger ausschließen.

5. Speichern Sie die Änderungen.

Vererbung von Cloud Gruppen und Systemberechtigungen anhand von Kategorien

HINWEIS: Die hier für Gruppen beschriebene Funktionalität gilt gleichermaßen für die Systemberechtigungen.

Im One Identity Manager können Gruppen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen 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 der Gruppentabelle geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 63**.

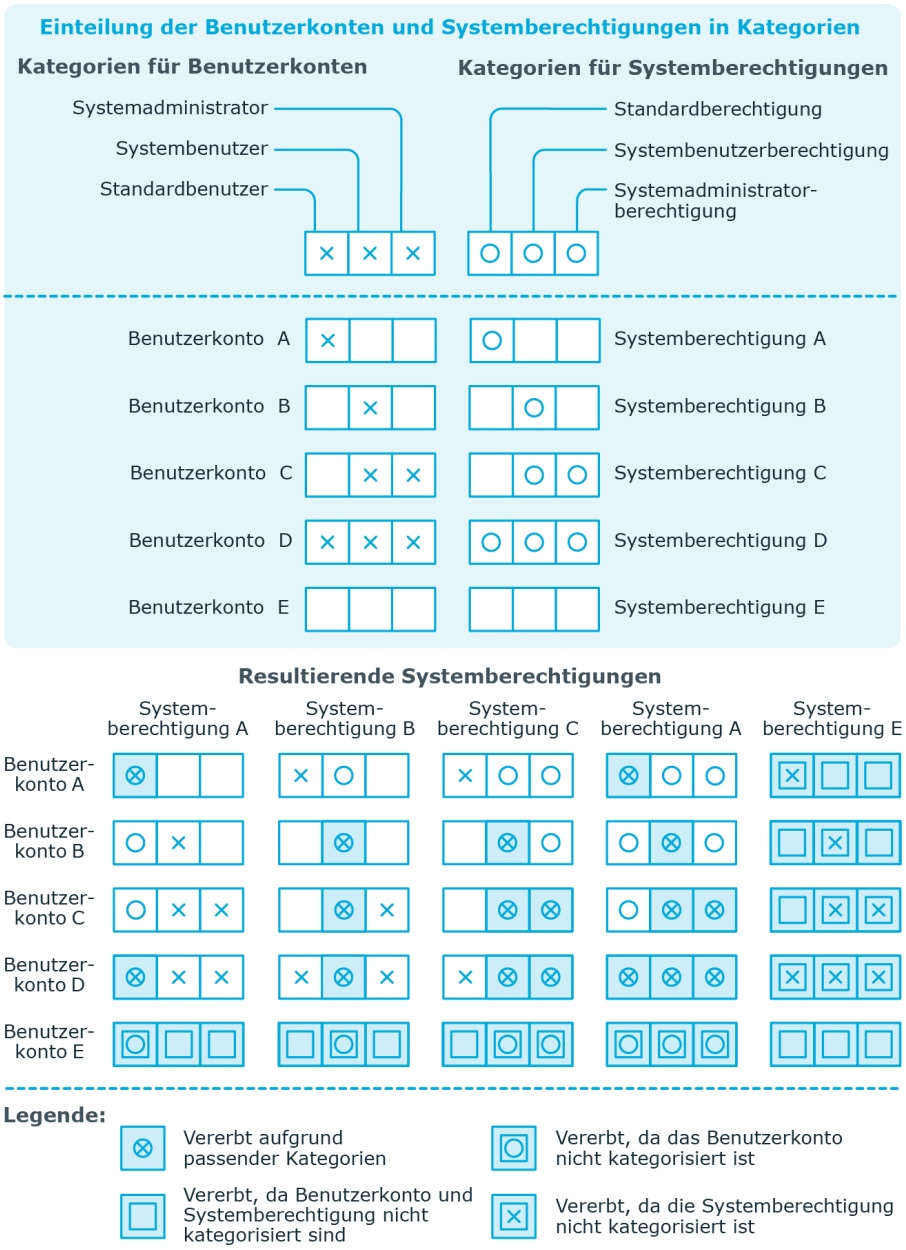
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist 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 22: Beispiele für Kategorien

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

Abbildung 3: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

- Definieren Sie im Manager am Cloud Zielsystem die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Gruppen und Systemberechtigungen über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von Cloud Gruppen und Systemberechtigungen definieren auf Seite 137
- Allgemeine Stammdaten für Cloud Benutzerkonten auf Seite 142
- Allgemeine Stammdaten für Cloud Gruppen auf Seite 154

Übersicht aller Zuweisungen

Für einige Objekte, wie beispielsweise Berechtigungen, Complianceregeln oder Rollen wird der Bericht **Übersicht aller Zuweisungen** angezeigt. Der Bericht ermittelt alle Rollen, wie beispielsweise Abteilungen, Kostenstellen, Standorte, Geschäftsrollen und IT Shop Strukturen, in denen sich Personen befinden, die das gewählte Basisobjekt besitzen. Dabei werden sowohl direkte als auch indirekte Zuweisungen des Basisobjektes berücksichtigt.

Beispiele:

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

Um detaillierte Informationen über Zuweisungen anzuzeigen

- Um den Bericht anzuzeigen, wählen Sie in der Navigation oder in der Ergebnisliste das Basisobjekt und wählen Sie den Bericht **Übersicht aller Zuweisungen**.
- Wählen Sie über die Schaltfläche **Verwendet von** in der Symbolleiste des Berichtes die Rollenklasse, für die Sie ermitteln möchten, ob es Rollen gibt, in denen sich Personen mit dem ausgewählten Basisobjekt befinden.

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des

Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.

- Mit einem Maus-Doppelklick auf das Steuerelement einer Rolle zeigen Sie alle untergeordneten Rollen der ausgewählten Rolle an.
- Mit einem einfachen Mausklick auf die Schaltfläche im Steuerelement einer Rolle zeigen Sie alle Personen dieser Rolle an, die das Basisobjekt besitzen.
- Über den Pfeil rechts neben der Schaltfläche starten Sie einen Assistenten, mit dem Sie die Liste der angezeigten Personen zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Personen werden der Geschäftsrolle zugeordnet.

Abbildung 4: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 23: 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.

6

Bereitstellen von Anmeldeinformationen für Cloud 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 Cloud Benutzerkonten auf Seite 118
- Initiales Kennwort für neue Cloud Benutzerkonten auf Seite 130
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 131

Kennwortrichtlinien für Cloud Benutzerkonten

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

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

Detaillierte Informationen zum Thema

- Vordefinierte Kennwortrichtlinien auf Seite 119
- Kennwortrichtlinien anwenden auf Seite 120
- Kennwortrichtlinien erstellen auf Seite 122
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 126
- Ausschlussliste für Kennwörter auf Seite 129
- Kennwörter prüfen auf Seite 130
- Generieren eines Kennwortes testen auf Seite 130

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 Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

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

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

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

Kennwortrichtlinien für Benutzerkonten

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

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

HINWEIS: Bei der Aktualisierung von One Identity Manager Version 7.x auf One Identity Manager Version 8.2 werden die Einstellung der Konfigurationsparameter zur Bildung von Kennwörtern auf die zielsystemspezifischen Kennwortrichtlinien umgesetzt.

Für Cloud Zielsysteme ist die Kennwortrichtlinie **Kennwortrichtlinie für Cloud Zielsysteme** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Benutzerkonten (`CSMUser.Password`) eines Cloud Zielsystems oder eines Containers anwenden.

Wenn die Kennwortanforderungen der Cloud Zielsysteme oder Container unterschiedlich sind, wird empfohlen, je Cloud Zielsystem oder Container 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 Cloud Zielsysteme ist die Kennwortrichtlinie **Kennwortrichtlinie für Cloud Zielsysteme** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Benutzerkonten (`CSMUser.Password`) eines Cloud Zielsystems oder eines Containers anwenden.

Wenn die Kennwortanforderungen der Cloud Zielsysteme oder Container unterschiedlich sind, wird empfohlen, je Cloud Zielsystem oder Container 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. Kennwortrichtlinie des Containers des Benutzerkontos.
4. Kennwortrichtlinie des Zielsystems des Benutzerkontos.
5. 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 **Cloud Zielsysteme > 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 **Cloud Zielsysteme > 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 **Cloud Zielsysteme > 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 123
- Richtlinieneinstellungen auf Seite 123
- Zeichenklassen für Kennwörter auf Seite 125
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 126

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 **Cloud Zielsysteme > 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 123
- Richtlinieneinstellungen auf Seite 123
- Zeichenklassen für Kennwörter auf Seite 125
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 126
- Kennwortrichtlinien erstellen auf Seite 122

Allgemeine Stammdaten für Kennwortrichtlinien

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 24: 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 Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

Richtlinieneinstellungen

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

Tabelle 25: 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 Personen-basierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen überschritten, kann sich die Person oder der Systembenutzer nicht mehr am One Identity Manager anmelden. Kennwörter gesperrter Personen 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**, **3** und **4** geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert **1** die geringsten

Eigenschaft	Bedeutung
	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 26: 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.
Min. Anzahl Ziffern	Gibt an, wie viele Ziffern ein Kennwort mindestens enthalten muss.

Eigenschaft	Bedeutung
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 Kleinbuchstaben erzeugen	Gibt an, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keinen Großbuchstaben 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 berücksichtigt.
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 127
- Skript zum Generieren eines Kennwortes auf Seite 128

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 **Cloud Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
    b. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Prüfskript** den Namen des Skriptes ein, das zum Prüfen eines Kennwortes verwendet wird.
    c. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Generieren eines Kennwortes auf Seite 128

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 **Cloud Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
    b. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Generierungsskript** den Namen des Skriptes ein, das zum Generieren eines Kennwortes verwendet wird.
    c. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Prüfen eines Kennwortes auf Seite 127

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 **Cloud Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie den Tabreiter **Test**.
3. Wählen Sie in der Auswahlliste **Basisobjekt für den Test** die Tabelle und das Objekt für die Prüfung.
4. 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 **Cloud Zielsysteme > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie den Tabreiter **Test**.
3. Klicken Sie auf die Schaltfläche **Generieren**.

   Das generierte Kennwort wird angezeigt.

Initiales Kennwort für neue Cloud Benutzerkonten

Um das initiale Kennwort für neue 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 | CSM | Accounts | InitialRandomPassword**.
- Verwenden Sie zielsystemspezifische Kennwortrichtlinien und definieren Sie in den Kennwortrichtlinien die Zeichenklassen, die das Kennwort enthalten muss.
- Legen Sie fest, an welche Person das initiale Kennwort per E-Mail versendet wird.

Verwandte Themen

- Kennwortrichtlinien für Cloud Benutzerkonten auf Seite 118
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 131

E-Mail-Benachrichtigungen über Anmeldeinformationen

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

Um Benachrichtigungen zu nutzen, sind folgende Voraussetzungen zu erfüllen:

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

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

Um die initialen Anmeldeinformationen per E-Mail zu versenden

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

   Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Person - Erstellung neues Benutzerkonto** versendet. Die Benachrichtigung enthält den Namen des Benutzerkontos.
4. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | CSM | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword**.

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

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

Abbildung von Cloud-Objekten im One Identity Manager

Mit dem One Identity Manager verwalten Sie die Benutzer und Berechtigungen einer Cloud-Anwendung. Jede Cloud-Anwendung wird als eigenes Basisobjekt im One Identity Manager abgebildet. Die Benutzerdaten werden als Benutzerkonten, Gruppen, Systemberechtigungen und Berechtigungselemente gespeichert und können in Containern organisiert werden.

Gruppen und Systemberechtigungen bilden die Objekte ab, über die in der Cloud-Anwendung der Zugriff auf die Cloud-Ressourcen gesteuert wird. Ein Benutzerkonto erhält durch die Zuweisung zu Gruppen und Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Cloud-Ressourcen.

Detaillierte Informationen zum Thema

Cloud Zielsysteme

Ein Cloud Zielsystem entspricht einer Cloud-Anwendung im Universal Cloud Interface.

HINWEIS: Die Einrichtung der Cloud Zielsysteme in der One Identity Manager-Datenbank übernimmt der Synchronization Editor.

Um die Stammdaten eines Cloud Zielsystems zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > Basisdaten zur Konfiguration > Cloud Zielsysteme**.
2. Wählen Sie in der Ergebnisliste das Zielsystem.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Zielsystems.
5. Speichern Sie die Änderungen.

TIPP: Die Eigenschaften eines Cloud Zielsystems können Sie im Manager auch in der Kategorie **Cloud Zielsysteme > <Zielsystem>** bearbeiten.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Cloud Zielsysteme auf Seite 134
- Kategorien für die Vererbung von Cloud Gruppen und Systemberechtigungen definieren auf Seite 137
- Alternative Spaltenbezeichnungen festlegen auf Seite 138
- Löschverzögerung für Benutzerkonten der Cloud Zielsysteme festlegen auf Seite 87
- Synchronisationsprojekt für ein Cloud Zielsystem bearbeiten auf Seite 139

Allgemeine Stammdaten für Cloud Zielsysteme

Für ein Cloud Zielsystem erfassen Sie die folgenden Stammdaten.

Tabelle 27: Stammdaten eines Cloud Zielsystems

Eigenschaft	Beschreibung
Cloud Zielsystem	Kennung des Zielsystems.
Kanonischer Name	Name des Zielsystems gemäß DNS Syntax an. `Name dieses Zielsystems.Name des übergeordneten Zielsystems.Name des Stammsystems` Beispiel: `DHW2k01.Testlab.com`
Definierter Name	Definierter Name des Cloud Zielsystems. Der definierte Name wird zur Bildung der definierten Namen untergeordneter Objekte verwendet. Stellt das Zielsystem keinen definierten Namen bereit, können Sie hier beispielsweise die Bezeichnung des Zielsystems eintragen. Syntaxbeispiel: `DC = <Zielsystem>`

Eigenschaft	Beschreibung
Anzeigename	Bezeichnung, unter der das Zielsystem in den Werkzeugen des One Identity Manager angezeigt wird.
Kontendefinition (initial)	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für dieses Cloud Zielsystem die automatische Zuordnung von Personen zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet. Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.
Löschverzögerung [Tage]	Verzögerung der Ausführung von Löschoperationen in Tagen für dieses Zielsystem. Weitere Informationen finden Sie unter Löschverzögerung für Benutzerkonten der Cloud Zielsysteme festlegen auf Seite 87.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Cloud Zielsystems, dem sie zugeordnet sind. Jedem Cloud Zielsystem können somit andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieses Cloud Zielsystems sind. Über die Schaltfläche  neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Synchronisiert durch	Art der Synchronisation, über welche die Daten zwischen dem Zielsystem und dem One Identity Manager synchronisiert werden. Sobald Objekte für dieses Zielsystem im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden. Beim Erstellen eines Cloud Zielsystems mit dem Synchronization Editor wird **One Identity Manager** verwendet

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>
Tabelle 28: Zulässige Werte
<table>
<tr><th>Wert</th><th>Synchronisation durch</th><th>Provisionierung durch</th></tr>
<tr><td>One Identity Manager</td><td>Universal Cloud Interface Konnektor</td><td>Universal Cloud Interface Konnektor</td></tr>
<tr><td>Keine Synchro-nisation</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>Typen der verwendeten Systemberechtigungen</td><td>Typen von Systemberechtigungen, denen in diesem Cloud Zielsystem Benutzerkonten zugewiesen werden können.</td></tr>
<tr><td>Benutzerkonto enthält Mitgliedschaften</td><td>Gibt an, für welche Typen von Systemberechtigungen die Zuweisungen an den Benutzerkonten gepflegt werden.
Aktivieren Sie die Typen, für welche die Zuweisungen an den Benutzerkonten gepflegt werden.
Deaktivieren Sie die Typen, für welche die Zuweisungen an den Systemberechtigungen gepflegt werden.
Beispiel:
Im Eingabefeld Typen der verwendeten Systemberechtigungen sind die Werte Gruppe und Systemberechtigung 1 ausgewählt. Im Eingabefeld Benutzerkonto enthält Mitgliedschaften ist nur der Wert Systemberechtigung 1 ausgewählt.
Die Zuweisungen von Benutzerkonten zu Gruppen werden an den Gruppen gespeichert, die Zuweisungen von Benutzerkonten zu Systemberechtigungen 1 an den Benutzerkonten.</td></tr>
<tr><td>Beschreibung</td><td>Freitextfeld für zusätzliche Erläuterungen.</td></tr>
<tr><td>Manuelle Provisionierung</td><td>Gibt an, ob Änderungen an Cloud-Ojekten in der One Identity Manager-Datenbank automatisch in die Cloud-Anwendung provisioniert werden. Wenn die Option deaktiviert ist, sind die Prozesse zur automatischen Provisionierung von Objektänderungen konfiguriert.</td></tr>
</table>

Eigenschaft	Beschreibung
	Wenn Objektänderungen nicht automatisch in die Cloud-Anwendung publiziert werden dürfen, aktivieren Sie diese Option. Nutzen Sie das Web Portal, um die Änderungen in die Cloud-Anwendung zu übernehmen. Ausführliche Informationen zur Provisionierung von Objektänderungen finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung von Cloud-Anwendungen*. WICHTIG: Wenn Sie die Option aktivieren, stellen Sie durch regelmäßige und häufige Synchronisationen sicher, dass die Daten • zwischen dem Modul Universal Cloud Interface und der Cloud-Anwendung und • zwischen den Modulen Universal Cloud Interface und Cloud Systems Management konsistent gehalten werden!
Benutzerkonten löschen nicht erlaubt	Gibt an, ob Benutzerkonten im Cloud Zielsystem gelöscht werden dürfen. Wenn die Option aktiviert ist, können die Benutzerkonten lediglich deaktiviert werden.

Verwandte Themen

- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 74
- Zielsystemverantwortliche auf Seite 178
- Typen von Systemberechtigungen in Cloud Zielsystemen auf Seite 89

Kategorien für die Vererbung von Cloud Gruppen und Systemberechtigungen definieren

HINWEIS: Die hier für Gruppen beschriebene Funktionalität gilt gleichermaßen für die Systemberechtigungen.

Im One Identity Manager können Gruppen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen 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 der Gruppentabelle geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 63**.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **Cloud Zielsysteme** das Zielsystem.
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 in der verwendeten Anmeldesprache ein.
7. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbung von Cloud Gruppen und Systemberechtigungen anhand von Kategorien auf Seite 114

Alternative Spaltenbezeichnungen festlegen

Wenn auf den Stammdatenformularen abweichende Bezeichnungen der Eingabefelder benötigt werden, können Sie für jeden Objekttyp die alternativ zu verwendenden Spaltenbezeichnungen sprachabhängig festlegen.

Um alternative Spaltenbezeichnungen festzulegen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > Basisdaten zur Konfiguration > Cloud Zielsysteme**.
2. Wählen Sie in der Ergebnisliste ein Zielsystem und wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wechseln Sie auf den Tabreiter **Alternative Spaltenbezeichnungen**.
4. Öffnen Sie den Mitgliederbaum der Tabelle, deren Spaltenbezeichnungen angepasst werden sollen.

   Es werden alle Spalten dieser Tabelle mit den Standard-Spaltenbezeichnungen aufgelistet.
5. Tragen Sie eine beliebige Benennung in der verwendeten Anmeldesprache ein.
6. Speichern Sie die Änderungen.

Synchronisationsprojekt für ein Cloud Zielsystem bearbeiten

Synchronisationsprojekte, in denen ein Cloud-Zielsystem 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 **Cloud Zielsysteme > Basisdaten zur Konfiguration > Cloud Zielsysteme**.
2. Wählen Sie in der Ergebnisliste das Zielsystem.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten**.

Verwandte Themen

- Anpassen einer Synchronisationskonfiguration auf Seite 29

Containerstrukturen

Die Containerstruktur repräsentiert die Strukturelemente eines Cloud Zielsystems. Container werden in einer hierarchischen Baumstruktur dargestellt.

Um einen Container zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Containerstruktur**.
2. Wählen Sie in der Ergebnisliste den Container und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Zu einem Container erfassen Sie die folgenden Stammdaten.

Tabelle 29: Stammdaten eines Containers

Eigenschaft	Beschreibung
Bezeichnung	Name des Containers.
Definierter Name	Definierter Name des Containers.
Übergeordneter Container	Übergeordneter Container zur Abbildung einer hierarchischen Containerstruktur.
Cloud Zielsystem	Cloud Zielsystem des Containers.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Kontomanager	Verantwortlicher für den Container. ***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**.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen des Containers festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Containers, dem sie zugeordnet sind. Jedem Container können andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieses Containers sind. Über die Schaltfläche + neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.

Verwandte Themen

- Zielsystemverantwortliche auf Seite 178

Cloud Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Benutzerkonten einer Cloud-Anwendung. Über die Mitgliedschaft in Gruppen, Systemberechtigungen und Berechtigungselementen erhalten die Benutzerkonten die nötigen Berechtigungen zum Zugriff auf die Cloud-Ressourcen.

Detaillierte Informationen zum Thema

- Managen von Cloud Benutzerkonten und Personen auf Seite 50
- Unterstützte Typen von Benutzerkonten auf Seite 79
- Cloud Benutzerkonten erstellen und bearbeiten auf Seite 141
- Cloud Berechtigungselemente an Cloud Benutzerkonten zuweisen auf Seite 149
- Zusatzeigenschaften an Cloud Benutzerkonten zuweisen auf Seite 149
- Cloud Benutzerkonten sperren und entsperren auf Seite 150
- Cloud Benutzerkonten löschen auf Seite 151
- Überblick über Cloud Benutzerkonten anzeigen auf Seite 152

Cloud Benutzerkonten erstellen und bearbeiten

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

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

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

Um ein Benutzerkonto zu erstellen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > 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 **Cloud Zielsysteme > <Zielsystem> > 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 Person manuell zuzuweisen

1. Wählen Sie im Manager die Kategorie **Personen > Personen**.
2. Wählen Sie in der Ergebnisliste die Person.
3. Wählen Sie die Aufgabe **Cloud Benutzerkonten zuweisen**.
4. Weisen Sie ein Benutzerkonto zu.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Cloud Benutzerkonten auf Seite 142
- Logindaten für Cloud Benutzerkonten auf Seite 146
- Angaben zur Identifikation von Cloud Benutzerkonten auf Seite 147
- Kontaktinformationen für Cloud Benutzerkonten auf Seite 148
- Benutzerdefinierte Stammdaten für Cloud Benutzerkonten auf Seite 148

Verwandte Themen

- Cloud Benutzerkonten löschen auf Seite 151

Allgemeine Stammdaten für Cloud Benutzerkonten

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

Tabelle 30: Eigenschaften eines Benutzerkontos

Eigenschaft	Beschreibung
Person	Person, die das Benutzerkonto verwendet. Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Person bereits eingetragen. Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Person aus der Auswahlliste wählen.Wenn Sie die automatische Personenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Person gesucht und in das Benutzerkonto übernommen. Für ein Benutzerkonto mit einer Identität vom Typ **Organisatorische Identität**, **Persönliche Administratoridentität**, **Zusatzidentität**, **Gruppenidentität** oder **Dienstidentität** können Sie eine neue Person erstellen. Klicken Sie dafür neben dem Eingabefeld und erfassen Sie die erforderlichen Personenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp.

Eigenschaft	Beschreibung
Zielsystem	Cloud Zielsystem des Benutzerkontos.
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 Person 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 Person 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.
Anrede	Anrede der Person.
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.
Vollständiger Name	Vollständiger Name des Benutzers.
Initialen	Initialen des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Berufsbezeichnung	Berufsbezeichnung des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Nickname	Zusätzliche Information zum Benutzerkonto.

Eigenschaft	Beschreibung
Namenszusatz	Namenszusatz des Benutzers, beispielsweise **von** oder **zu**.
Anzeigename	Anzeigename des Benutzerkontos.
Alias	Alias des Benutzerkontos zur weiteren Identifizierung.
Bezeichnung	Bezeichnung des Benutzerkontos.
Container	Container, in dem das Benutzerkonto erzeugt werden soll. Haben Sie eine Kontendefinition zugeordnet, wird der Container, abhängig vom Automatisierungsgrad, aus den gültigen IT Betriebsdaten der zugeordneten Person ermittelt.
Erste primäre Gruppe	Primäre Gruppe des Benutzerkontos.
Zweite primäre Gruppe	Zusätzliche primäre Gruppe des Benutzerkontos. Wenn es im Zielsystem Gruppen mit unterschiedlichen Gruppentypen gibt, können Sie hier eine weitere primäre Gruppe zuordnen.
E-Mail-Adresse	E-Mail-Adresse des Benutzers.
E-Mail-Kodierung	Art der E-Mail-Kodierung.
Kontoverfallsdatum	Tag, bis zu welchem das Benutzerkonto zur Anmeldung genutzt werden darf. Wenn für eine Person ein Austrittsdatum festgelegt ist, wird, abhängig vom Automatisierungsgrad des Benutzerkontos, dieses Austrittsdatum als Kontoverfallsdatum übernommen. Ein bereits eingetragenes Kontoverfallsdatum des Benutzerkontos wird dabei überschrieben. HINWEIS: Wenn zu einem späteren Zeitpunkt das Austrittsdatum der Person gelöscht wird, bleibt das Kontoverfallsdatum des Benutzerkontos erhalten.
Ressourcentyp	Typ der Ressource, beispielsweise **User**.
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.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Eigenschaft	Beschreibung
Anmeldename	Name, mit dem sich der Benutzer am Zielsystem anmeldet. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Identität	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Person. • **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 Person genutzt wird. • **Zusatzidentität**: Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.
Privilegiertes Benutzerkonto	Gibt an, ob es sich um ein privilegiertes Benutzerkonto handelt.
Gruppen erbbar	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.
Systemberechtigungen 1 erbbar Systemberechtigungen 2 erbbar	Gibt an, ob das Benutzerkonto Systemberechtigungen des entsprechenden Typs über die verbundene Person erben darf. Ist die Option aktiviert, werden Systemberechtigungen über hierarchische Rollen, in denen die Person Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.

Eigenschaft	Beschreibung
Systemberechtigungen 3 erbbar	• Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Systemberechtigungen zugewiesen haben, dann erbt das Benutzerkonto diese Systemberechtigungen. • Wenn eine Person eine Zuweisung zu einer Systemberechtigung im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Systemberechtigung nur, wenn die Option aktiviert ist.
Benutzerkonto ist deaktiviert	Gibt an, ob das Benutzerkonto gesperrt ist. Wird ein Benutzerkonto vorübergehend nicht benötigt, können Sie das Benutzerkonto über die Option zeitweilig deaktivieren.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von Cloud Gruppen und Systemberechtigungen an Cloud Benutzerkonten auf Seite 93
- Cloud Benutzerkonten sperren und entsperren auf Seite 150
- Typen von Systemberechtigungen in Cloud Zielsystemen auf Seite 89

Logindaten für Cloud Benutzerkonten

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.

Auf dem Tabreiter **Login** erfassen Sie die folgenden Daten.

Tabelle 31: Logindaten eines Benutzerkontos

Eigenschaft	Beschreibung
Kennwort/Kennwortbestätigung	Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Person kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*. Wenn Sie ein zufällig generiertes initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen. Das Kennwort wird nach dem Publizieren in das

Eigenschaft	Beschreibung
	Zielsystem aus der Datenbank gelöscht.
Letzte Kennwortänderung	Datum der letzten Änderung des Kennwortes.
Letzte Anmeldung	Datum und Uhrzeit der letzten Anmeldung an der Cloud-Anwendung.

Verwandte Themen

- Kennwortrichtlinien für Cloud Benutzerkonten auf Seite 118

Angaben zur Identifikation von Cloud Benutzerkonten

Auf dem Tabreiter **Identifikation** erhalten Sie die Adressinformationen der Person, die dieses Benutzerkonto verwendet.

Tabelle 32: Identifikationsdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Straße	Straße.
Postfach	Postfach.
Ort	Ort.
Postleitzahl	Postleitzahl.
Bundesland	Bundesland.
Land	Land.
Adresse	Formatierte Postanschrift.
Sprachkultur	Bezeichnung der Sprachkultur.
Zeitzone	Bezeichnung der Zeitzone.
Raum	Raum.
Abteilung	Abteilung der Person.
Bereich	Bereich, zu dem das Benutzerkonto gehört.
Organisation	Organisation, zu der das Benutzerkonto gehört.
Personennummer	Nummer zur Kennzeichnung der Person, zusätzlich zur Personenkennung.
Art der Anstel-	Art der Anstellung.

Eigenschaft	Beschreibung
lung	
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**.

Kontaktinformationen für Cloud Benutzerkonten

Auf dem Tabreiter **Kontakt** erhalten Sie die Informationen zur Erreichbarkeit der Person, die dieses Benutzerkonto verwendet.

Tabelle 33: Kontaktdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Telefon	Nummer des Festnetztelefons.
Mobiltelefon	Nummer des Mobiltelefons.
Webseite	Webseite des Benutzers.

Benutzerdefinierte Stammdaten für Cloud Benutzerkonten

Auf dem Tabreiter **Benutzerdefiniert** erhalten Sie unternehmensspezifische Angaben zum Benutzerkonto.

Tabelle 34: Benutzerdefinierte Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Freies Feld Nr. 01- Freies Feld Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01- Freies Datum Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Eigenschaft	Beschreibung
Freier Text Nr. 01- Freier Text Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freie Option Nr. 01 - Freie Option Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Cloud Berechtigungselemente an Cloud Benutzerkonten zuweisen

Mit dieser Aufgabe können Sie Berechtigungselemente an Benutzerkonten zuweisen.

Um Berechtigungselemente an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Berechtigungselemente zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungselemente zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Cloud Benutzerkonten an Cloud Berechtigungselemente zuweisen auf Seite 169

Zusatzeigenschaften an Cloud Benutzerkonten zuweisen

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

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

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

Cloud Benutzerkonten sperren und entsperren

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

Szenario:

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

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

Szenario:

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

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

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

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu deaktivieren

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Benutzerkonto ist deaktiviert**.
5. Speichern Sie die Änderungen.

Szenario:

Benutzerkonten sind nicht mit Personen verbunden.

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

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > 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 Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Kontendefinitionen für Cloud Benutzerkonten auf Seite 51
- Automatisierungsgrade erstellen auf Seite 57

Cloud Benutzerkonten löschen

Ein Benutzerkonto löschen Sie 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.

Um ein Benutzerkonto zu löschen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Sobald ein Benutzerkonto gelöscht wurde, wird es über den Provisionierungsprozess auch im Modul Universal Cloud Interface und anschließend in der Cloud-Anwendung gelöscht. Die Löschung wird als anstehende Änderung aufgezeichnet. Ob das Benutzerkonto in der Cloud-Anwendung gelöscht wurde, ist am Verarbeitungsstatus der anstehenden Änderung ersichtlich. Gleiches gilt, wenn Mitgliedschaften von Benutzerkonten in Gruppen gelöscht werden.

In manchen Cloud-Anwendungen ist das Löschen von Benutzerkonten nicht zulässig. Solche Benutzerkonten können auch im Manager nicht gelöscht, sondern nur deaktiviert werden. Das entsprechende Verhalten konfigurieren Sie am Cloud Zielsystem.

Um das Löschen von Benutzerkonten zu verhindern

1. Wählen Sie im Managerdie Kategorie **Cloud Zielsysteme > Basisdaten zur Konfiguration > Cloud Zielsysteme**.
2. Wählen Sie in der Ergebnisliste das Zielsystem.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie die Option **Benutzerkonten löschen nicht erlaubt**.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Provisionierung von Objektänderungen auf Seite 47
- Allgemeine Stammdaten für Cloud Zielsysteme auf Seite 134
- Cloud Benutzerkonten sperren und entsperren auf Seite 150
- Löschverzögerung für Benutzerkonten der Cloud Zielsysteme festlegen auf Seite 87

Überblick über Cloud 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 **Cloud Zielsysteme > <Zielsystem> > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das Benutzerkonto**.

Cloud Gruppen

Gruppen und Systemberechtigungen bilden die Objekte ab, über die in der Cloud-Anwendung der Zugriff auf die Cloud-Ressourcen gesteuert wird. Ein Benutzerkonto erhält durch die Zuweisung zu Gruppen und Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Cloud-Ressourcen.

Detaillierte Informationen zum Thema

- Cloud Gruppen in Cloud Gruppen aufnehmen auf Seite 156
- Cloud Berechtigungselemente an Cloud Gruppen zuweisen auf Seite 157
- Zusatzeigenschaften an Cloud Gruppen zuweisen auf Seite 158
- Cloud Gruppen löschen auf Seite 159
- Überblick über Cloud Gruppen anzeigen auf Seite 158
- Managen der Zuweisungen von Cloud Gruppen und Cloud Systemberechtigungen auf Seite 89

Verwandte Themen

- Cloud Systemberechtigungen auf Seite 159

Cloud Gruppen erstellen und bearbeiten

Um eine Gruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Gruppen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
4. Speichern Sie die Änderungen.

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > 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 Cloud Gruppen auf Seite 154
- Benutzerdefinierte Stammdaten für Cloud Gruppen auf Seite 156
- Cloud Gruppen löschen auf Seite 159

Allgemeine Stammdaten für Cloud Gruppen

Zu einer Gruppe erfassen Sie die folgenden Stammdaten.

Tabelle 35: Allgemeine Stammdaten einer Gruppe

Eigenschaft	Beschreibung
Bezeichnung	Bezeichnung der Gruppe.
Container	Container, in dem die Gruppe angelegt werden soll.
Zielsystem	Cloud Zielsystem der Gruppe.
Definierter Name	Definierter Name der Gruppe.
Anzeigename	Anzeigename zur Anzeige der Gruppe in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Name der Gruppe	Zusätzliche Bezeichnung der Gruppe.
E-Mail-Adresse	E-Mail-Adresse der Gruppe.
Kontomanager	Verantwortlicher der Gruppe. ***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.

Eigenschaft	Beschreibung
	4. Klicken Sie **OK**.
IT Shop	Gibt an, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.
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 von Ihren Mitarbeitern 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 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. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Gruppentyp	Name des Gruppentyps. Diese Angabe wird nur benötigt, wenn in der Cloud-Anwendung verschiedene Gruppentypen unterschieden werden.
Ressourcentyp	Typ der Ressource, beispielsweise **Group**.

Detaillierte Informationen zum Thema

- Kategorien für die Vererbung von Cloud Gruppen und Systemberechtigungen definieren auf Seite 137

Benutzerdefinierte Stammdaten für Cloud Gruppen

Auf dem Tabreiter **Benutzerdefiniert** erhalten Sie unternehmensspezifische Angaben zur Gruppe.

Tabelle 36: Benutzerdefinierte Stammdaten einer Gruppe

Eigenschaft	Beschreibung
Freies Feld Nr. 01- Freies Feld Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01- Freies Datum Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freier Text Nr. 01- Freier Text Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freie Option Nr. 01 - Freie Option Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Cloud Gruppen in Cloud 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 **Cloud Zielsysteme > <Zielsystem> > 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 **Cloud Zielsysteme > <Zielsystem> > 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.

Verwandte Themen

- Cloud Systemberechtigungen an Cloud Systemberechtigungen zuweisen auf Seite 163

Cloud Berechtigungselemente an Cloud Gruppen zuweisen

Mit dieser Aufgabe können Sie Berechtigungselemente an Gruppen zuweisen.

Um Berechtigungselemente an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Berechtigungselemente zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Berechtigungselemente zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Cloud Berechtigungselemente auf Seite 167
- Cloud Gruppen an Cloud Berechtigungselemente zuweisen auf Seite 168

Zusatzeigenschaften an Cloud Gruppen zuweisen

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

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

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

Verwandte Themen

- Zusatzeigenschaften an Cloud Systemberechtigungen zuweisen auf Seite 165

Überblick über Cloud 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 **Cloud Zielsysteme > <Zielsystem> > Gruppen**.

2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die Cloud Gruppe**.

Cloud Gruppen löschen

Die Gruppe wird endgültig aus der One Identity Manager-Datenbank gelöscht. Sobald eine Gruppe gelöscht wurde, wird sie über den Provisionierungsprozess auch im Modul Universal Cloud Interface und anschließend in der Cloud-Anwendung gelöscht. Die Löschung wird als anstehende Änderung aufgezeichnet. Ob die Gruppe in der Cloud-Anwendung gelöscht wurde, ist am Verarbeitungsstatus der anstehenden Änderung ersichtlich. Gleiches gilt, wenn Zuweisungen von Benutzerkonten an Gruppen gelöscht werden.

Um eine Gruppe zu löschen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Klicken Sie , um die Gruppe zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 47
- Cloud Systemberechtigungen löschen auf Seite 166

Cloud Systemberechtigungen

Gruppen und Systemberechtigungen bilden die Objekte ab, über die in der Cloud-Anwendung der Zugriff auf die Cloud-Ressourcen gesteuert wird. Ein Benutzerkonto erhält durch die Zuweisung zu Gruppen und Systemberechtigungen die nötigen Berechtigungen zum Zugriff auf die Cloud-Ressourcen.

Detaillierte Informationen zum Thema

- Cloud Systemberechtigungen erstellen und bearbeiten auf Seite 160
- Cloud Benutzerkonten direkt an Cloud Systemberechtigungen zuweisen auf Seite 108
- Cloud Systemberechtigungen an Cloud Systemberechtigungen zuweisen auf Seite 163
- Überblick über Cloud Systemberechtigungen anzeigen auf Seite 165

Verwandte Themen

- Cloud Gruppen auf Seite 153

Cloud Systemberechtigungen erstellen und bearbeiten

Um eine Systemberechtigung zu erstellen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Systemberechtigung.
4. Speichern Sie die Änderungen.

Um die Stammdaten einer Systemberechtigung zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Systemberechtigung.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Cloud Systemberechtigungen auf Seite 161
- Benutzerdefinierte Stammdaten für Cloud Systemberechtigungen auf Seite 162

Allgemeine Stammdaten für Cloud Systemberechtigungen

Zu einer Systemberechtigung erfassen Sie die folgenden Stammdaten.

Tabelle 37: Allgemeine Stammdaten einer Systemberechtigung

Eigenschaft	Beschreibung
Bezeichnung	Bezeichnung der Systemberechtigung.
Container	Container, in dem die Systemberechtigung angelegt werden soll.
Zielsystem	Cloud Zielsystem der Systemberechtigung.
Definierter Name	Definierter Name der Systemberechtigung.
Anzeigename	Anzeigename zur Anzeige der Systemberechtigung in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Name der Systemberechtigung	Zusätzliche Bezeichnung der Systemberechtigung.
E-Mail-Adresse	E-Mail-Adresse der Systemberechtigung.
Kontomanager	Verantwortlicher der Systemberechtigung. ***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**.
IT Shop	Gibt an, ob die Systemberechtigung über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Systemberechtigung über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Systemberechtigung kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Eigenschaft	Beschreibung
Verwendung nur im IT Shop	Gibt an, ob die Systemberechtigung ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Systemberechtigung über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Systemberechtigung an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Leistungsposition	Leistungsposition, um die Systemberechtigung über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Systemberechtigung 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 finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Systemberechtigungen. Systemberechtigungen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Systemberechtigungen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Typ der Systemberechtigung	Eindeutige Kennung des Typs der Systemberechtigung. Diese Angabe wird nur benötigt, wenn in der Cloud-Anwendung verschiedene Typen von Systemberechtigungen unterschieden werden.
Ressourcentyp	Bezeichnung des Ressourcentyps, beispielsweise `/Roles`.

Detaillierte Informationen zum Thema

- Kategorien für die Vererbung von Cloud Gruppen und Systemberechtigungen definieren auf Seite 137
- Typen von Systemberechtigungen in Cloud Zielsystemen auf Seite 89

Benutzerdefinierte Stammdaten für Cloud Systemberechtigungen

Auf dem Tabreiter **Benutzerdefiniert** erhalten Sie unternehmensspezifische Angaben zur Systemberechtigung.

Tabelle 38: Benutzerdefinierte Stammdaten einer Systemberechtigung

Eigenschaft	Beschreibung
Freies Feld Nr. 01- Freies Feld Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01- Freies Datum Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freier Text Nr. 01- Freier Text Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freie Option Nr. 01 - Freie Option Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Cloud Systemberechtigungen an Cloud Systemberechtigungen zuweisen

Systemberechtigungen können Mitglied anderer Systemberechtigungen sein. Damit können die Systemberechtigungen hierarchisch strukturiert werden. Es können nur Systemberechtigungen zugewiesen werden, die denselben Typ haben.

Um Systemberechtigungen als Mitglieder an eine Systemberechtigung zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Passend zur gewählten Systemberechtigung, wählen Sie die Aufgabe **Systemberechtigungen 1 zuweisen**, **Systemberechtigungen 2 zuweisen** oder **Systemberechtigungen 3 zuweisen**.
4. Wählen Sie den Tabreiter **Hat Mitglieder**.

5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die untergeordneten Systemberechtigungen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemberechtigung und doppelklicken Sie ✓.

6. Speichern Sie die Änderungen.

Um eine Systemberechtigung als Mitglied in andere Systemberechtigungen aufzunehmen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.

2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Passend zur gewählten Systemberechtigung, wählen Sie die Aufgabe **Systemberechtigungen 1 zuweisen**, **Systemberechtigungen 2 zuweisen** oder **Systemberechtigungen 3 zuweisen**.
4. Wählen Sie den Tabreiter **Ist Mitglied in**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die übergeordneten Systemberechtigungen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemberechtigung und doppelklicken Sie ✓.

6. Speichern Sie die Änderungen.

Verwandte Themen

- Cloud Gruppen in Cloud Gruppen aufnehmen auf Seite 156

Zusatzeigenschaften an Cloud Systemberechtigungen 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 Systemberechtigung festzulegen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
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.

Verwandte Themen

- Zusatzeigenschaften an Cloud Gruppen zuweisen auf Seite 158

Überblick über Cloud Systemberechtigungen anzeigen

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

Um einen Überblick über eine Systemberechtigung zu erhalten

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Passend zur gewählten Systemberechtigung, wählen Sie die Aufgabe **Überblick über Systemberechtigung 1**, **Überblick über Systemberechtigung 2** oder **Überblick über Systemberechtigung 3**.

Cloud Systemberechtigungen löschen

Die Systemberechtigung wird endgültig aus der One Identity Manager-Datenbank gelöscht. Sobald eine Systemberechtigung gelöscht wurde, wird sie über den Provisionierungsprozess auch im Modul Universal Cloud Interface und anschließend in der Cloud-Anwendung gelöscht. Die Löschung wird als anstehende Änderung aufgezeichnet. Ob die Systemberechtigung in der Cloud-Anwendung gelöscht wurde, ist am Verarbeitungsstatus der anstehenden Änderung ersichtlich. Gleiches gilt, wenn Zuweisungen von Benutzerkonten an Systemberechtigungen gelöscht werden.

Um eine Systemberechtigung zu löschen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 1**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 2**.

   - ODER -

   Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Systemberechtigungen 3**.
2. Wählen Sie in der Ergebnisliste die Systemberechtigung.
3. Klicken Sie , um die Systemberechtigung zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 47
- Cloud Gruppen löschen auf Seite 159

Cloud Berechtigungselemente

Berechtigungselemente nutzen Sie, um beliebige, weitere Eigenschaften der Cloud-Anwendung abzubilden.

Um Berechtigungselemente zu erstellen oder zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste ein Berechtigungselement. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER -

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Cloud Berechtigungselemente auf Seite 167
- Benutzerdefinierte Stammdaten für Cloud Berechtigungselemente auf Seite 168

Allgemeine Stammdaten für Cloud Berechtigungselemente

Für ein Berechtigungselement erfassen Sie die folgenden Stammdaten.

Tabelle 39: Stammdaten eines Berechtigungselements

Eigenschaft	Beschreibung
Zielsystem	Cloud Zielsystem, in dem das Berechtigungselement gültig ist.
Berechtigungselement	Bezeichnung des Berechtigungselements.
Berechtigungstyp	Zusätzliche Eigenschaft des Berechtigungselements.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Benutzerdefinierte Stammdaten für Cloud Berechtigungselemente

Auf dem Tabreiter **Benutzerdefiniert** erhalten Sie unternehmensspezifische Angaben zu einem Berechtigungselement.

Tabelle 40: Benutzerdefinierte Stammdaten eines Berechtigungselements

Eigenschaft	Beschreibung
Freies Feld Nr. 01- Freies Feld Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freies Datum Nr. 01- Freies Datum Nr. 03	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freier Text Nr. 01- Freier Text Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Freie Option Nr. 01 - Freie Option Nr. 05	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Cloud Gruppen an Cloud Berechtigungselemente zuweisen

Über diese Aufgabe können Sie ein Berechtigungselement direkt an die Gruppen zuweisen.

Um ein Berechtigungselement an Gruppen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
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

- Cloud Berechtigungselemente an Cloud Gruppen zuweisen auf Seite 157

Cloud Benutzerkonten an Cloud Berechtigungselemente zuweisen

Über diese Aufgabe können Sie ein Berechtigungselement direkt an die Benutzerkonten zuweisen.

Um ein Berechtigungselement an Benutzerkonten zuzuweisen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
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

- Cloud Berechtigungselemente an Cloud Benutzerkonten zuweisen auf Seite 149

Überblick über Cloud Berechtigungselemente anzeigen

Auf dem Überblicksformular erhalten Sie auf einen Blick die wichtigsten Informationen zu einem Berechtigungselement.

Um einen Überblick über ein Berechtigungselement zu erhalten

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Überblick über das Berechtigungselement**.

Cloud Berechtigungselemente löschen

Das Berechtigungselement wird endgültig aus der One Identity Manager-Datenbank gelöscht. Sobald ein Berechtigungselement gelöscht wurde, wird es über den Provisionierungsprozess auch im Modul Universal Cloud Interface und anschließend in der Cloud-Anwendung gelöscht. Die Löschung wird als anstehende Änderung aufgezeichnet. Ob das Berechtigungselement in der Cloud-Anwendung gelöscht wurde, ist am Verarbeitungsstatus der anstehenden Änderung ersichtlich. Gleiches gilt, wenn Zuweisungen von Berechtigungselementen an Benutzerkonten oder Gruppen gelöscht werden.

Um ein Berechtigungselement zu löschen

1. Wählen Sie im Manager die Kategorie **Cloud Zielsysteme > <Zielsystem> > Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Klicken Sie , um das Berechtigungselement zu löschen.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 47

Berichte über Objekte in Cloud Zielsystemen

Der One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen Objekten der One Identity Manager-Datenbank aufbereitet sind. Für Cloud Zielsysteme stehen folgende Berichte zur Verfügung.

HINWEIS: Abhängig von den vorhandenen Modulen können weitere Berichte zur Verfügung stehen.

Tabelle 41: 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

Bericht	Bereitgestellt für	Beschreibung
		der zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Historie)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto 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 anzeigen (inklusive Historie)	Container	Der Bericht zeigt alle Benutzerkonten des Containers 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.
Systemberechtigungen anzeigen (inklusive Historie)	Container	Der Bericht zeigt die Systemberechtigungen des Containers 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	Container	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Container mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen	Systemberechtigung Gruppe	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, welche die ausgewählte Systemberechtigung besitzen.
Übersicht anzeigen	Systemberechtigung Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre Zuwei-

Bericht	Bereitgestellt für	Beschreibung
		sungen.
Übersicht anzeigen (inklusive Herkunft)	Systemberechtigung Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	Systemberechtigung 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	Cloud Zielsystem	Der Bericht enthält alle Systemberechtigungen, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten anzeigen (inklusive Historie)	Cloud Zielsystem	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 überdurchschnittliche Anzahl an Systemberechtigungen anzeigen	Cloud Zielsystem	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
Personen mit mehreren Benutzerkonten anzeigen	Cloud Zielsystem	Der Bericht zeigt alle Personen, die mehrere Benutzerkonten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Systemberechtigungen anzeigen (inklusive Historie)	Cloud Zielsystem	Der Bericht zeigt die Systemberechtigungen mit den zugewiesenen Benutzerkonten 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.
Übersicht aller Zuweisungen	Cloud Zielsystem	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.
Ungenutzte Benutzerkonten anzeigen	Cloud Zielsystem	Der Bericht enthält alle Benutzerkonten, die in den letzten Monaten nicht verwendet wurden.
Unverbundene Benutzerkonten anzeigen	Cloud Zielsystem	Der Bericht zeigt alle Benutzerkonten, denen keine Person zugeordnet ist.

Tabelle 42: Zusätzliche Berichte für das Zielsystem

Bericht	Beschreibung
Cloud Zielsysteme Benutzerkonten- und Gruppenverteilung	Der Bericht enthält eine Zusammenfassung zur Benutzerkonten- und Gruppenverteilung aller Cloud Zielsysteme. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**.
Datenqualität der Cloud Benutzerkonten	Der Bericht enthält verschiedenen Auswertungen zur Datenqualität der Benutzerkonten aller Cloud Zielsysteme. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**.

Verwandte Themen

- Übersicht aller Zuweisungen auf Seite 116

8

Behandeln von Cloud-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 Personen

  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 Person, beispielsweise einen Manager, wird das Benutzerkonto angelegt.

- Managen von Zuweisungen von Gruppen und Systemberechtigungen

  Mit der Zuweisung von Gruppen und Systemberechtigungen 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 Person wird die Gruppe oder Systemberechtigung zugewiesen.

  Manager und Administratoren von Organisationen können im Web Portal Gruppen und Systemberechtigungen an die Abteilungen, Kostenstellen oder Standorte zuweisen, für die sie verantwortlich sind. Die Gruppen und Systemberechtigungen werden an alle Personen vererbt, die Mitglied dieser Abteilungen, Kostenstellen oder Standorte sind.

  Wenn das Geschäftsrollenmodul vorhanden ist, können Manager und Administratoren von Geschäftsrollen im Web Portal Gruppen und Systemberechtigungen an die Geschäftsrollen zuweisen, für die sie verantwortlich sind. Die Gruppen und Systemberechtigungen werden an alle Personen vererbt, die Mitglied dieser Geschäftsrollen sind.

  Wenn das Systemrollenmodul vorhanden ist, können Verantwortliche von Systemrollen im Web Portal Gruppen und Systemberechtigungen an die Systemrollen zuweisen. Die Gruppen und Systemberechtigungen werden an alle Personen vererbt, denen diese Systemrollen zugewiesen sind.

- Attestierung

  Wenn das Modul Attestierung vorhanden ist, kann die Richtigkeit der Eigenschaften von Zielsystemobjekten und von Gruppenmitgliedschaften 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 Gruppenmitgliedschaften 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 Personen 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 Personen nutzen das Web Portal, um Richtlinienverletzungen zu überprüfen und Ausnahmegenehmigungen zu erteilen.

- Risikobewertung

  Über den Risikoindex von Gruppen kann das Risiko von Gruppenmitgliedschaften 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 Personen, Benutzerkonten, deren Berechtigungen und Risiken bereit.

Ausführliche Informationen zu den genannten Themen finden Sie unter Managen von Cloud Benutzerkonten und Personen auf Seite 50, Managen der Zuweisungen von Cloud Gruppen und Cloud Systemberechtigungen auf Seite 89 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*

9

Basisdaten für die Verwaltung einer Universal Cloud Interface-Umgebung

Für die Verwaltung von Cloud-Anwendungen im Modul Cloud Systems Management sind folgende Basisdaten relevant.

- Konfigurationsparameter

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

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

  Weitere Informationen finden Sie unter Konfigurationsparameter für die Verwaltung von Cloud Zielsystemen auf Seite 186.

- 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 41.

- Kontendefinitionen

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

Weitere Informationen finden Sie unter Kontendefinitionen für Cloud Benutzerkonten auf Seite 51.

- Kennwortrichtlinien

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

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

  Weitere Informationen finden Sie unter Kennwortrichtlinien für Cloud Benutzerkonten auf Seite 118.

- Initiales Kennwort für neue Benutzerkonten

  Um das initiale Kennwort für Benutzerkonten zu vergeben, stehen Ihnen verschiedene Möglichkeiten zur Verfügung. Tragen Sie beim Erstellen eines Benutzerkontos ein Kennwort ein oder verwenden Sie ein zufällig generiertes initiales Kennwort.

  Weitere Informationen finden Sie unter Initiales Kennwort für neue Cloud Benutzerkonten auf Seite 130.

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

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

  Weitere Informationen finden Sie unter E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 131.

- Zielsystemverantwortliche

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

  Wenn Sie die Berechtigungen der Zielsystemverantwortlichen auf einzelne Cloud Zielsysteme einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

  Weitere Informationen finden Sie unter Zielsystemverantwortliche auf Seite 178.

- Server

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

  Weitere Informationen finden Sie unter Jobserver für Universal Cloud Interface-spezifische Prozessverarbeitung auf Seite 180.

Zielsystemverantwortliche

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

Wenn Sie die Berechtigungen der Zielsystemverantwortlichen auf einzelne Cloud Zielsysteme einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

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

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

Tabelle 43: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Cloud Zielsysteme** 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 und Systemberechtigungen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.

Benutzer	Aufgaben
	• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Personen als Zielsystemadministrator festzulegen

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

Um initial Personen in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

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

Um als Zielsystemverantwortlicher weitere Personen als Zielsystemverantwortliche zu berechtigen

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

Um Zielsystemverantwortliche für einzelne Cloud Zielsysteme festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **Cloud Zielsysteme > Basisdaten zur Konfiguration > Cloud Zielsysteme**.
3. Wählen Sie in der Ergebnisliste das Zielsystem.
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 | Cloud Zielsysteme** zu.

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

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung von Cloud Zielsystemen auf Seite 11
- Allgemeine Stammdaten für Cloud Zielsysteme auf Seite 134
- Containerstrukturen auf Seite 139

Jobserver für Universal Cloud Interface-spezifische Prozessverarbeitung

Für die Verarbeitung der Universal Cloud Interface-spezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein. 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 **Cloud Zielsysteme > 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.

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 17

Jobserver für Cloud Zielsysteme bearbeiten

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 **Cloud Zielsysteme > 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 181
- Festlegen der Serverfunktionen auf Seite 184

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 44: 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.
Sprachkultur	Sprache des Servers.
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.

Eigenschaft	Bedeutung
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.
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 Pfadaus-

Eigenschaft	Bedeutung
	lösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	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*.
Kein automatisches Softwareupdate	Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, 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 184

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 45: Zulässige Serverfunktionen

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.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtserver	Server, auf dem die Berichte generiert werden.
Universal Cloud Interface Konnektor	Der Server kann sich mit dem Modul Universal Cloud Interface verbinden.

Verwandte Themen

- Allgemeine Stammdaten für Jobserver auf Seite 181

Anhang A

Konfigurationsparameter für die Verwaltung von Cloud Zielsystemen

Mit der Installation des Moduls sind zusätzlich folgende Konfigurationsparameter im One Identity Manager verfügbar.

Tabelle 46: Konfigurationsparameter für die Verwaltung von Cloud Zielsystemen

Konfigurationsparameter	Bedeutung
TargetSystem | CSM	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung von Cloud Zielsystemen. 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 | CSM | Accounts	Erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem | CSM | 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 | CSM | Accounts | InitialRandomPassword | SendTo	Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter **TargetSystem |**

Konfigurationsparameter	Bedeutung
	CSM | DefaultAddress hinterlegte Adresse versandt.
TargetSystem | CSM | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet.
TargetSystem | CSM | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem | CSM | 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 **Person - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | CSM | Accounts | PrivilegedAccount	Erlaubt die Konfiguration der Einstellungen für privilegierte Benutzerkonten.
TargetSystem | CSM | Accounts | PrivilegedAccount | SAMAccountName_ Postfix	Postfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | CSM | Accounts | PrivilegedAccount | SAMAccountName_ Prefix	Präfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | CSM | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | CSM | MaxFullsyncDuration	Maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.

Konfigurationsparameter	Bedeutung
TargetSystem | CSM | PersonAutoDefault	Modus für die automatische Personenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | CSM | PersonAutoDisabledAccounts	Gibt an, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | CSM | PersonAutoFullSync	Modus für die automatische Personenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem | CSM | PersonExcludeList	Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $`

Folgende Konfigurationsparameter werden zusätzlich benötigt.

Tabelle 47: Zusätzliche Konfigurationsparameter

Konfigurationsparameter	Bedeutung
QBM | PendingChange	Allgemeiner Konfigurationsparameter für die Konfiguration von anstehenden Änderungen.
QBM | PendingChange | LifeTimeError	Der Konfigurationsparameter legt den Aufbewahrungszeitraum (in Tagen) für fehlgeschlagene Provisionierungsvorgänge fest. Der Standardzeitraum beträgt **30** Tage.
QBM | PendingChange | LifeTimeRunning	Der Konfigurationsparameter legt den Aufbewahrungszeitraum (in Tagen) für offene Provisionierungsvorgänge fest. Der Standardzeitraum beträgt **60** Tage.
QBM | PendingChange | LifeTimeSuccess	Der Konfigurationsparameter legt den Aufbewahrungszeitraum (in Tagen) für erfolgreiche Provisionierungsvorgänge fest. Der Standardzeitraum beträgt **2** Tage.

Anhang B

Standardprojektvorlage für Cloud-Anwendungen im Universal Cloud Interface

Eine Standardprojektvorlage sorgt dafür, dass alle benötigten Informationen im One Identity Manager angelegt werden. Dazu gehören beispielsweise die Mappings, Workflows und das Basisobjekt der Synchronisation. Wenn Sie keine Standardprojektvorlage verwenden, müssen Sie das Basisobjekt der Synchronisation selbst im One Identity Manager bekannt geben.

Verwenden Sie eine Standardprojektvorlage für die initiale Einrichtung des Synchronisationsprojektes. Für kundenspezifische Implementierungen können Sie das Synchronisationsprojekt mit dem Synchronization Editor erweitern.

Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 48: Abbildung der Universal Cloud Interface Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Universal Cloud Interface	Tabelle im One Identity Manager Schema
UCIRoot	CSMRoot
UCIContainer	CSMContainer
UCIGroup	CSMGroup
UCIGroupInGroup	CSMGroupInGroup
UCIGroupHasItem	CSMGroupHasItem
UCIGroup1	CSMGroup1
UCIGroup1InGroup1	CSMGroup1InGroup1
UCIGroup2	CSMGroup2
UCIGroup2InGroup2	CSMGroup2InGroup2

Schematyp im Universal Cloud Interface	Tabelle im One Identity Manager Schema
UCIGroup3	CSMGroup3
UCIGroup3InGroup3	CSMGroup3InGroup3
UCIItem	CSMItem
UCIUser	CSMUser
UCIUserInGroup	CSMUserInGroup
UCIUserInGroup1	CSMUserInGroup1
UCIUserInGroup2	CSMUserInGroup2
UCIUserInGroup3	CSMUserInGroup3
UCIUserHasGroup	CSMUserHasGroup
UCIUserHasGroup1	CSMUserHasGroup1
UCIUserHasGroup2	CSMUserHasGroup2
UCIUserHasGroup3	CSMUserHasGroup3
UCIUserHasItem	CSMUserHasItem
QBMPendingChange	QBMPendingChange
QBMPendingChangeDetail	QBMPendingChangeDetail

Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie https://www.oneidentity.com/company/contact-us.aspx.

Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter https://support.oneidentity.com/ zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter www.YouTube.com/OneIdentity
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

Index

E

I

J

K

L

O

P

R

S

V

Z