One Identity Manager 8.0

Administrationshandbuch für die Anbindung einer Universal Cloud Interface-Umgebung

Patente

One Identity ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente und anhängige Patente gelten. Für die aktuellsten Informationen über die geltenden Patente für dieses Produkt besuchen Sie bitte unsere Website unter http://www.OneIdentity.com/legal/patents.aspx.

Marken

Legende

WARNUNG: Das Symbol WARNUNG weist auf mögliche Personen- oder Sachschäden oder Schaden mit Todesfolge hin.

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

WICHTIG, HINWEIS, TIPP, MOBIL, oder VIDEO: Ein Informationssymbol weist auf Begleitinformationen hin.

One Identity Manager Administrationshandbuch für die Anbindung einer Universal Cloud Interface-Umgebung

Aktualisiert - Oktober 2017

Version - 8.0

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 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 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.

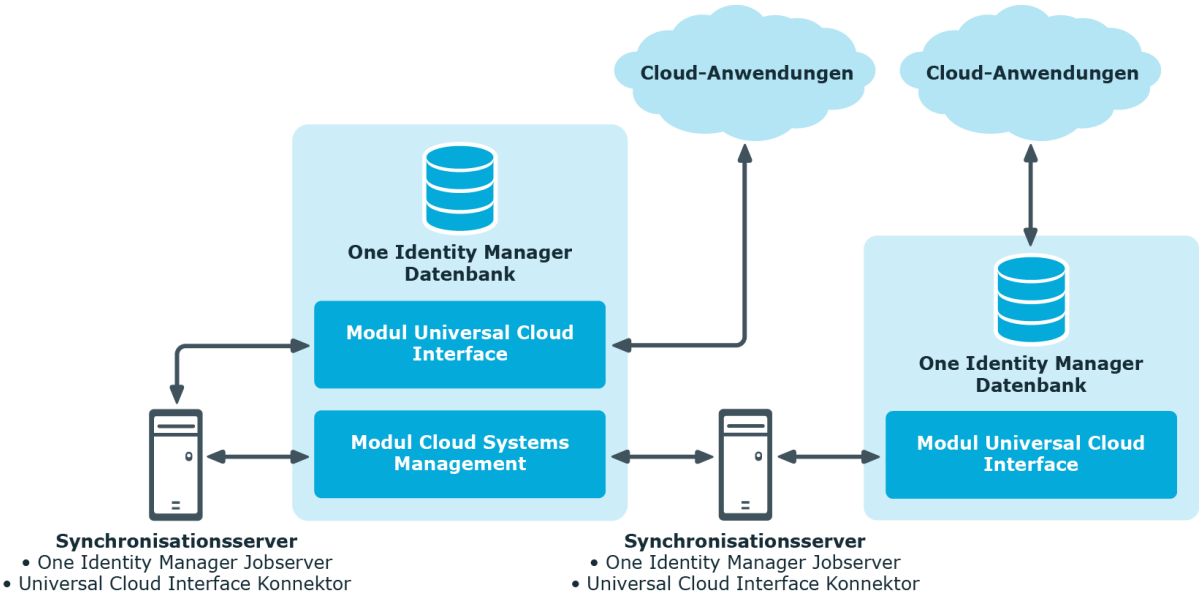
Da im Modul Universal Cloud Interface nur die Daten gespeichert werden, die in den Cloud-Anwendungen verfügbar sein müssen, kann dieses Modul in einer separaten Datenbank installiert werden. Diese Datenbank kann sich auch außerhalb der Unternehmensinfrastruktur befinden.

In Verbindung mit der Cloud-Lösung "One Identity Connect For Cloud" 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 sich fest, welche Anwendungsrollen für Zielsystemverantwortliche sich widersprechen. • 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, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.

Benutzer	Aufgaben
	• Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
Administratoren für den IT Shop	Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an IT Shop-Strukturen zu.
Administratoren für Organisationen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Organisationen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Abteilungen, Kostenstellen und Standorte zu.
Administratoren für Geschäftsrollen	Die Administratoren müssen der Anwendungsrolle **Identity Management | Geschäftsrollen | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an Geschäftsrollen zu.

Einrichten der Synchronisation mit 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 Anhang: Standardprojektvorlage für Cloud-Anwendungen im Universal Cloud Interface auf Seite 137.

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.
- 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.

   Damit das Synchronisationsprojekt erstellt werden kann, muss die Cloud-Anwendung bereits im Modul Universal Cloud Interface vorhanden sein.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation auf Seite 13
- Einrichten des Synchronisationsservers auf Seite 14
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung auf Seite 18

Ausführliche Informationen zum Einrichten der initialen Synchronisation mit einer Cloud-Anwendung finden Sie im One Identity Manager Administrationshandbuch für die Anbindung von Cloud-Anwendungen.

Benutzer und Berechtigungen für die Synchronisation

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 System-benutzer mit der Rechtegruppe "DPR_EditRights_ Methods"

Benutzer	Berechtigungen
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen (Rechtevergabe, Verzeichnisse und Dateien anlegen und bearbeiten). Das Benutzerkonto muss der Gruppe "Domänen-Benutzer" (Domain Users) angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht "Anmelden als Dienst" (Log on as a service). Das Benutzerkonto benötigt Rechte 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 Rechte 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

Für die Einrichtung der Synchronisation muss ein Server zur Verfügung gestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- One Identity Manager Service
  - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.

1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
2. Wählen Sie die Maschinenrolle **Server | Jobserver**.

Ausführliche Informationen zu den Systemanforderungen für die Installation des One Identity Manager Service finden Sie im One Identity Manager Installationshandbuch.

Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

Um den One Identity Manager Service zu installieren, nutzen Sie das Programm Server Installer. Das Programm führt die folgenden 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. Die Remote-Installation wird nur innerhalb einer Domäne oder in Domänen mit Vertrauensstellung unterstützt.

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 und klicken Sie **Weiter**.
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.

Tabelle 4: Eigenschaften eines Jobservers

Eigenschaft	Beschreibung
Server	Bezeichnung des Jobservers.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-

Eigenschaft	Beschreibung
	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. Beispiel: `<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** legen Sie fest, welche Rolle der Jobserver im One Identity Manager übernimmt. Abhängig von der gewählten Maschinenrolle werden die Installationspakete ermittelt, die auf dem Jobserver installiert werden.
   - Job Server
5. Auf der Seite **Serverfunktionen** legen Sie die Funktion des Servers in der One Identity Manager-Umgebung fest. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

   Die Serverfunktionen sind abhängig von den gewählten Maschinenrollen bereits ausgewählt. Sie können die Serverfunktionen hier weiter einschränken.
   - Universal Cloud Interface Konnektor
6. Auf der Seite **Dienstkonfiguration** 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.
7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.
10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.

    HINWEIS: Diese Seite wird nur angezeigt, wenn die Datenbank verschlüsselt ist.

11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.

Tabelle 5: Installationsinformationen

Eingabe	Beschreibung
Computer	Server, auf dem der Dienst installiert und gestartet wird. ***Um einen Server auszuwählen*** • Erfassen Sie den Servernamen. -ODER- • Wählen Sie einen Eintrag in der Liste.
Dienstkonto	Angaben zum Benutzerkonto des One Identity Manager Service. ***Um ein Benutzerkonto für den One Identity Manager Service zu erfassen*** • Aktivieren Sie die Option **Lokales Systemkonto**. Damit wird der One Identity Manager Service unter dem Konto "NT AUTHORITY\SYSTEM" gestartet. - ODER- • Erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung. Als Benutzerkonto für den One Identity Manager Service muss das Serverfarmkonto der SharePoint Farm genutzt werden.
Installationskonto	Angaben zum administrativen Benutzerkonto für die Installation des Dienstes. ***Um ein administratives Benutzerkonto für die Installation zu erfassen*** • Aktivieren Sie die Option **Erweitert**. • Aktivieren Sie die Option **Angemeldeter Benutzer**. Es wird das Benutzerkonto des aktuell angemeldeten Benutzers verwendet. - ODER- • Geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.

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: Der Dienst wird 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.

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

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

Tabelle 6: 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.

<table>
<tr><th>Angaben</th><th>Erläuterungen</th></tr>
<tr><td></td><td>Tabelle 7: Zusätzliche Eigenschaften für den Jobserver
<table>
<tr><th>Eigenschaft</th><th>Wert</th></tr>
<tr><td>Serverfunktion</td><td>Universal Cloud Interface Konnektor</td></tr>
<tr><td>Maschinenrolle</td><td>Server/Jobserver</td></tr>
</table>
Weitere Informationen finden Sie unter Einrichten des Synchronisationsservers auf Seite 14. </td></tr>
<tr><td>Verbindungsdaten zur One Identity Manager Datenbank</td><td>SQL Server:
Datenbankserver
Datenbank
Datenbankbenutzer und Kennwort
Angabe, ob integrierte Windows Authentifizierung verwendet wird.
Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows Authentifizierung unterstützt.
Oracle:
Angabe, ob der Zugriff direkt oder über Oracle Client erfolgt
Die erforderlichen Verbindungsdaten sind abhängig von der Einstellung dieser Option.
Datenbankserver
Port der Oracle Instanz
Service Name
Oracle Datenbankbenutzer und Kennwort
Datenquelle (TNS Alias Name aus der <code>TNSNames.ora</code>)</td></tr>
<tr><td>Remoteverbindungsserver</td><td>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. Wenn der direkte Zugriff von der Arbeitsstation, auf der der Synchronization Editor installiert ist, nicht möglich ist, beispielsweise aufgrund der Firewall-Konfiguration, kann eine Remoteverbindung eingerichtet werden.</td></tr>
</table>

Angaben	Erläuterungen
	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.

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

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

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

Um ein initiales Synchronisationsprojekt für 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**. 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.

Tabelle 8: Verbindungsdaten zur SQL Server Datenbank

Eingabe	Beschreibung
Server	Datenbankserver.
Windows Authentifizierung	Angabe, ob integrierte Windows Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows Authentifizierung unterstützt.
Nutzer	Datenbankbenutzer.
Kennwort	Kennwort des Datenbankbenutzers.
Datenbank	Datenbank.

Tabelle 9: Verbindungsdaten zur Oracle Datenbank

Eingabe	Beschreibung
Direktzugriff (ohne Oracle Client)	Für den direkten Zugriff aktivieren Sie die Option. Für den Zugriff über Oracle Clients deaktivieren Sie die Option. Die erforderlichen Verbindungsdaten sind abhängig von der Einstellung dieser Option.
Server	Datenbankserver.
Port	Port der Oracle Instanz.
Service Name	Service Name.
Benutzer	Oracle Datenbankbenutzer.
Kennwort	Kennwort des Datenbankbenutzers.
Datenquelle	TNS Alias Name aus der `TNSNames.ora`.

- 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 10: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	Angabe, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager Datenbank eingerichtet werden soll. 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"

Option	Bedeutung
	definiert.
Es sollen auch Änderungen im Zielsystem durchgeführt werden.	Angabe, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll. Der Provisionierungsworkflow zeigt folgende Besonderheiten: • Die Synchronisationsrichtung ist "In das Zielsystem". • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die 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.

    - Klicken Sie , um einen neuen Jobserver anzulegen.
    - Erfassen Sie die Bezeichnung des Jobservers und den vollständigen Servernamen gemäß DNS-Syntax.
    - Klicken Sie **OK**.

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

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

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

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

Tabelle 11: Startkonfigurationen

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

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

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

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

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

1. Um das Synchronisationsprotokoll für die Zielsystemverbindung zu konfigurieren, wählen Sie die Kategorie **Konfiguration | Zielsystem**.
2. Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.
3. Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren...**
4. Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.
5. Aktivieren Sie die zu protokollierenden Daten.

   HINWEIS: Einige Inhalte erzeugen besonders viele Protokolldaten!

   Das Synchronisationsprotokoll soll nur die für Fehleranalysen und weitere Auswertungen notwendigen Daten enthalten.
6. Klicken Sie **OK**.

Um regelmäßige Synchronisationen auszuführen

1. Wählen Sie die Kategorie **Konfiguration | Startkonfigurationen**.
2. Wählen Sie in der Dokumentenansicht eine Startkonfiguration aus und klicken Sie **Zeitplan bearbeiten...**.
3. Bearbeiten Sie die Eigenschaften des Zeitplans.
4. Um den Zeitplan zu aktivieren, klicken Sie **Aktiviert**.
5. Klicken Sie **OK**.

Um die initiale Synchronisation manuell zu starten

1. Wählen Sie die Kategorie **Konfiguration | Startkonfigurationen**.
2. Wählen Sie in der Dokumentenansicht eine Startkonfiguration und klicken Sie **Ausführen**.
3. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

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

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie dem Zielsystem eine Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand "Linked" (verbunden) die Kontendefinition und den Automatisierungsgrad zu.
    a. Wählen Sie die Kategorie **Cloud Zielsysteme | <Zielsystem> | Benutzerkonten | Verbunden aber nicht konfiguriert | <Zielsystem>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

Detaillierte Informationen zum Thema

- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 14
- Benutzer und Berechtigungen für die Synchronisation auf Seite 13
- Startkonfigurationen auf Seite 25
- Synchronisationsergebnisse anzeigen auf Seite 26
- Anpassen einer Synchronisationskonfiguration auf Seite 27
- Beschleunigung der Synchronisation durch Revisionsfilterung auf Seite 31
- Anhang: Standardprojektvorlage für Cloud-Anwendungen im Universal Cloud Interface auf Seite 137
- Einrichten von Kontendefinitionen auf Seite 38
- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 99

Startkonfigurationen

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 128

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. Wählen Sie die Kategorie **Protokolle**.
2. Klicken Sie in der Symbolleiste der Navigationsansicht ▶.

   In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.
3. 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. Wählen Sie die Kategorie **Protokolle**.
2. Klicken Sie in der Symbolleiste der Navigationsansicht .

   In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.
3. 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.

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt. Den Aufbewahrungszeitraum legen Sie über den Konfigurationsparameter "DPR\Journal\LifeTime" und seine untergeordneten Konfigurationsparameter fest.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

- Aktivieren Sie im Designer den Konfigurationsparameter "Common\Journal\LifeTime" und tragen Sie die maximale Aufbewahrungszeit für die Einträge im Systemprotokoll ein. Mit den untergeordneten Konfigurationsparametern legen Sie die Aufbewahrungszeit je Meldungstyp fest.
- Bei großen Datenmengen können Sie zur Performance-Optimierung die Menge der zu löschenden Objekte pro Operation und Verarbeitungslauf des DBQueue Prozessor festlegen. Verwenden Sie dazu die Konfigurationsparameter "Common\Journal\Delete\BulkCount" und "Common\Journal\Delete\TotalCount".
- Konfigurieren und aktivieren Sie im Designer den Zeitplan "Journal löschen".

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 Mastersystem zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung "In das Zielsystem".

- 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.
- 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.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschema geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.

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

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus "Frozen". Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.
- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Planen Sie die Startzeiten sorgfältig. Wenn möglich, legen Sie die Startzeiten so fest, dass sich die Synchronisationen zeitlich nicht überschneiden.

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 29
- Synchronisation verschiedener Cloud-Anwendungen konfigurieren auf Seite 29
- Schema aktualisieren auf Seite 30

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

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

Verwandte Themen

- Synchronisation verschiedener Cloud-Anwendungen konfigurieren auf Seite 29

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 das Synchronisationsprojekt im Synchronization Editor.
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 und geben Sie die Verbindungsparameter bekannt. Die Verbindungsparameter werden in einem spezialisierten Variablenset gespeichert.

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

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 29

Schema aktualisieren

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

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

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

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

Um das Schema einer Systemverbindung zu aktualisieren

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

   - ODER -

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

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

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

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

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

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 nach diesem Zeitpunkt geändert werden, werden erst mit der nächsten Synchronisation erfasst.

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

Um die Revisionsfilterung an einem Workflow zuzulassen

- Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
- 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 das Synchronisationsprojekt im Synchronization Editor.
- 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.

Nachbehandlung ausstehender Objekte

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.

Objekte, die als ausstehend gekennzeichnet wurden,

- können im One Identity Manager nicht bearbeitet werden,
- werden bei jeder weiteren Synchronisation ignoriert,
- müssen im One Identity Manager einzeln nachbearbeitet werden.

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie 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.

1. Wählen Sie in der Navigationsansicht die Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

   Das Formular für den Zielsystemabgleich wird geöffnet. Hier werden alle Objekte angezeigt, die als ausstehend markiert sind.

TIPP:

Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

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

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

2. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.
3. Klicken Sie in der Formularsymbolleiste eins der folgenden Symbole, um die jeweilige Methode auszuführen.

Tabelle 12: 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. Die Methode löst das Ereignis "HandleOutstanding" aus. Dadurch 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.

4. 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 .

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.

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 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.

Unterstützung bei der Analyse von Synchronisationsproblemen

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

- Ergebnisse der Konsistenzprüfung
- Einstellungen zur Revisionsfilterung

- Verwendeter Scope
- Analyse des Synchronisationspuffers
- Zugriffszeiten auf die Objekte in der One Identity Manager Datenbank und im Zielsystem

Um den Synchronisationsanalysebericht zu erstellen

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

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

Deaktivieren der Synchronisation

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

Um regelmäßige Synchronisationen zu verhindern

- 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 geladene Synchronisationsprojekt zu deaktivieren

1. Wählen Sie auf der Startseite die Ansicht **Allgemein**.
2. Klicken Sie **Projekt deaktivieren**.

Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung auf Seite 18

3

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 Anhang: Konfigurationsparameter für die Verwaltung von Cloud Zielsystemen auf Seite 134.

- Zielsystemtypen

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

  Weitere Informationen finden Sie unter Nachbehandlung ausstehender Objekte auf Seite 32.

- Kontendefinitionen

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

Weitere Informationen finden Sie unter Einrichten von Kontendefinitionen auf Seite 38.

- 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 eine 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 auf Seite 56.

- Initiales Kennwort für neue Benutzerkonten

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

  Weitere Informationen finden Sie unter Initiales Kennwort für neue Benutzerkonten auf Seite 66.

- 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 68.

- 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 Bearbeitungsrechte 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 70.

- 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 Bearbeiten eines Servers auf Seite 72.

Einrichten von Kontendefinitionen

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

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

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

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- Erstellen einer Kontendefinition
- Erstellen der Automatisierungsgrade
- Erstellen einer Abbildungsvorschrift für IT Betriebsdaten
- Erfassen der IT Betriebsdaten
- Zuweisen der Kontendefinition an Personen
- Zuweisen der Kontendefinition an ein Cloud Zielsystem

Erstellen einer Kontendefinition

Um eine Kontendefinition zu erstellen

1. Wählen Sie die Kategorie **Cloud Zielsysteme | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

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

Detaillierte Informationen zum Thema

- Stammdaten einer Kontendefinition auf Seite 39

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 13: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Vorausgesetzte Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch mitbestellt oder zugeordnet. 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. Erfassen Sie einen Wert zwischen 0 und 1. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter "QER\CalculateRiskIndex" aktiviert ist. Ausführliche Informationen finden Sie im One Identity Manager Administrationshandbuch für Risikobewertungen.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Angabe, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von

Eigenschaft	Beschreibung
	den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.
Automatische Zuweisung zu Personen	Angabe, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Kontendefinition an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition. Um die automatische Zuweisung der Kontendefinition an alle Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei verzögertem Löschen beibehalten	Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
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: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.

Eigenschaft	Beschreibung
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.

Erstellen der Automatisierungsgrade

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

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

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- Unmanaged

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

- Full managed

  Benutzerkonten mit dem Automatisierungsgrad "Full managed" erben definierte Eigenschaften der zugeordneten Person.

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

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

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

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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie 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.

   - ODER -

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

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

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie die Kategorie **Cloud Zielsysteme | Basisdaten zur Konfiguration | Kontendefinitionen | Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

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

Verwandte Themen

- Stammdaten eines Automatisierungsgrades auf Seite 42

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 14: Stammdaten eines Automatisierungsgrades

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

Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

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 die Kategorie **Cloud Zielsysteme | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Mapping bearbeiten** und erfassen Sie folgende Daten.

Tabelle 15: Abbildungsvorschrift für IT Betriebsdaten

Eigenschaft	Beschreibung
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.
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: Verwenden Sie die primäre Geschäftsrolle nur, 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.

Eigenschaft	Beschreibung
Immer Standardwert verwenden	Angabe, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.
Benachrichtigung bei Verwendung des Standards	Angabe, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage "Person - Erstellung neues Benutzerkontos mit Standardwerten" verwendet. Um die Mailvorlage zu ändern, passen Sie den Konfigurationsparameter "TargetSystem\CSM\Accounts\MailTemplateDefaultValues" an.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Erfassen der IT Betriebsdaten auf Seite 45

Erfassen der IT Betriebsdaten

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 Abteilungen, Kostenstellen, Standorten und Geschäftsrollen definiert. Einer Person wird eine primäre Abteilung, eine primäre Kostenstelle, ein primärer Standort oder eine primäre Geschäftsrolle 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 in der Kategorie **Organisationen** bzw. **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten** und erfassen Sie folgende Daten.

Tabelle 16: IT Betriebsdaten

Eigenschaft	Beschreibung
Organisation/Geschäftsrolle	Abteilung, Kostenstelle, Standort oder Geschäftsrolle, für die die IT Betriebsdaten gelten sollen.
Wirksam für	Anwendungsbereich der IT Betriebsdaten. 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	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	Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

3. Speichern Sie die Änderungen.

Verwandte Themen

- Erstellen einer Abbildungsvorschrift für IT Betriebsdaten auf Seite 44

Ändern der IT Betriebsdaten

Sobald sich die IT Betriebsdaten ändern, müssen diese Änderungen für bestehende Benutzerkonten übernommen werden. Dafür müssen die Bildungsregeln an den betroffenen Spalten erneut ausgeführt werden. Bevor die Bildungsregeln ausgeführt werden, können Sie prüfen, 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 Datenbank übernommen werden soll.

Voraussetzungen

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

  - ODER -

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

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

Um die Bildungsregeln auszuführen

1. Wählen Sie 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.

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

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinition an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen. Das Standardverfahren für die Zuweisung von Kontendefinitionen an Personen ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Personen werden gemäß ihrer Funktion im Unternehmen in diese Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet und erhalten so ihre Kontendefinitionen. Um auf Sonderanforderungen zu reagieren, können einzelne Kontendefinitionen direkt an Personen zugewiesen werden. Kontendefinitionen können automatisch an alle Personen eines Unternehmens zugewiesen werden. Es ist möglich, die Kontendefinitionen als bestellbare Produkte dem IT Shop zuzuordnen. Der Abteilungsleiter kann dann für seine Mitarbeiter Benutzerkonten über das Web Portal bestellen. Zusätzlich ist es möglich, Kontendefinitionen in Systemrollen aufzunehmen. Diese Systemrollen können über hierarchische Rollen oder direkt an Personen zugewiesen werden oder als Produkte in den IT Shop aufgenommen werden.

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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

Detaillierte Informationen zum Thema

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 49
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 49
- Kontendefinition an alle Personen zuweisen auf Seite 50
- Kontendefinition direkt an Personen zuweisen auf Seite 51
- Kontendefinition an Systemrollen zuweisen auf Seite 51
- Kontendefinition in den IT Shop aufnehmen auf Seite 52
- Zuweisen der Kontendefinition an ein Cloud Zielsystem auf Seite 53

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie 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.

   - ODER -

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

Verwandte Themen

- Kontendefinition an Geschäftsrollen zuweisen auf Seite 49
- Kontendefinition an alle Personen zuweisen auf Seite 50
- Kontendefinition direkt an Personen zuweisen auf Seite 51
- Kontendefinition an Systemrollen zuweisen auf Seite 51
- Kontendefinition in den IT Shop aufnehmen auf Seite 52

Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie 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. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

   - ODER -

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 49
- Kontendefinition an alle Personen zuweisen auf Seite 50
- Kontendefinition direkt an Personen zuweisen auf Seite 51
- Kontendefinition an Systemrollen zuweisen auf Seite 51
- Kontendefinition in den IT Shop aufnehmen auf Seite 52

Kontendefinition an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie 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. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.

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

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

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 49
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 49
- Kontendefinition direkt an Personen zuweisen auf Seite 51
- Kontendefinition an Systemrollen zuweisen auf Seite 51
- Kontendefinition in den IT Shop aufnehmen auf Seite 52

Kontendefinition direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

1. Wählen Sie 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.

   - ODER -

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 49
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 49
- Kontendefinition an alle Personen zuweisen auf Seite 50
- Kontendefinition an Systemrollen zuweisen auf Seite 51
- Kontendefinition in den IT Shop aufnehmen auf Seite 52

Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

1. Wählen Sie 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.

   - ODER -

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 49
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 49
- Kontendefinition an alle Personen zuweisen auf Seite 50
- Kontendefinition direkt an Personen zuweisen auf Seite 51
- Kontendefinition in den IT Shop aufnehmen auf Seite 52

Kontendefinition in den IT Shop aufnehmen

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

- Die Kontendefinition muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Kontendefinition muss eine Leistungsposition zugeordnet sein.
- Soll die Kontendefinition nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss sie zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.

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

Um eine Kontendefinition in den IT Shop aufzunehmen

1. Wählen Sie die Kategorie **Cloud Zielsysteme | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Cloud Zielsysteme | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

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

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Cloud Zielsysteme | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

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

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

Verwandte Themen

- Stammdaten einer Kontendefinition auf Seite 39
- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 49
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 49
- Kontendefinition direkt an Personen zuweisen auf Seite 51
- Kontendefinition an Systemrollen zuweisen auf Seite 51

Zuweisen der Kontendefinition an ein Cloud Zielsystem

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 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 99

Löschen einer Kontendefinition

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

HINWEIS: Wird eine Kontendefinition gelöscht, dann werden die Benutzerkonten, die aus dieser Kontendefinition entstanden sind, gelöscht.

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie 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. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.
    e. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
    a. Wählen Sie 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 Standorte.

   a. Wählen Sie 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 die Kategorie **Cloud Zielsysteme | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

   c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

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

   d. Speichern Sie die Änderungen.

5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden. Ausführliche Informationen dazu finden Sie im One Identity Manager Administrationshandbuch für IT Shop.

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 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 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 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.

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 eine 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 56
- Bearbeiten von Kennwortrichtlinien auf Seite 58
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 60
- Ausschlussliste für Kennwörter auf Seite 63
- Prüfen eines Kennwortes auf Seite 63
- Generieren eines Kennwortes testen auf Seite 64
- Zuweisen einer Kennwortrichtlinie auf Seite 64

Vordefinierte Kennwortrichtlinien

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

Kennwortrichtlinie für die Anmeldung am One Identity Manager

Für die Anmeldung am One Identity Manager wird die Kennwortrichtlinie "One Identity Manager Kennwortrichtlinie" verwendet. 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).

Die Kennwortrichtlinie "One Identity Manager Kennwortrichtlinie" ist zusätzlich als Standardrichtlinie gekennzeichnet und wird angewendet, wenn keine andere Kennwortrichtlinie ermittelt werden kann.

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).

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

Kennwortrichtlinien für Zielsysteme

Für jedes Zielsystem wird eine vordefinierte Kennwortrichtlinie bereitgestellt, die Sie auf die Kennwortspalten der Benutzerkonten anwenden können.

HINWEIS: Bei der Aktualisierung von One Identity Manager Version 7.x auf One Identity Manager Version 8.0 werden die Einstellung der Konfigurationsparameter zur Bildung von Kennwörtern auf die zielsystemspezifischen Kennwortrichtlinien umgesetzt.

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

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.

Bearbeiten von Kennwortrichtlinien

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 und wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Kennwortrichtlinie auf Seite 58
- Richtlinieneinstellungen auf Seite 59
- Zeichenklassen für Kennwörter auf Seite 60
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 60

Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 17: 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.

Eigenschaft	Bedeutung
	HINWEIS: Die Kennwortrichtlinie "One Identity Manager Kennwortrichtlinie" ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie ermittelt werden kann.

Richtlinieneinstellungen

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

Tabelle 18: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wird beim Anlegen im Benutzerkonto selbst kein Kennwort angegeben oder ein Zufallskennwort generiert, dann wird das initiale Kennwort benutzt.
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben muss.
Max.Länge	Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Hat ein Benutzer diese Anzahl erreicht, wird das Benutzerkonto gesperrt.
Max. Tage gültig	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert "5" eingegeben, werden die letzten 5 Kennwörter des Benutzers gespeichert.
Min. Kennwortstärke	Angabe, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert "0" wird die Kennwortstärke nicht geprüft. Die Werte "1", "2", "3", und "4" geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert "1" die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert "4" fordert die höchste Komplexität.

Eigenschaft	Bedeutung
Namensbestandteile unzulässig	Angabe, ob Namensbestandteile im Kennwort zulässig sind.

Zeichenklassen für Kennwörter

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

Tabelle 19: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Min. Anzahl Buchstaben	Angabe, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss.
Min. Anzahl Kleinbuchstaben	Angabe, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Großbuchstaben	Angabe, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Ziffern	Angabe, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Angabe, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.
Zulässige Sonderzeichen	Liste zulässiger Sonderzeichen.
Unzulässige Sonderzeichen	Liste unzulässiger 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.

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 61
- Skript zum Generieren eines Kennwortes auf Seite 62

Skript zum Prüfen eines Kennwortes

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

Syntax für Prüfskripte

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

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Kennwort, das zu prüfen ist

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

Beispiel für ein Skript zum Prüfen eines Kennwortes

Ein Kennwort in darf nicht mit "?" oder "!" beginnen. Das 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 62

Skript zum Generieren eines Kennwortes

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

Syntax für Generierungsskripte

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

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Generiertes Kennwort

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

Beispiel für ein Skript zum Generieren eines Kennwortes

Das Skript ersetzt die unzulässige Zeichen "?" und "!" in Zufallskennwörtern.

```
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 61

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.

Prüfen eines Kennwortes

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.

Zuweisen einer Kennwortrichtlinie

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.

WICHTIG: Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie. Stellen Sie in diesem Fall sicher, dass die Kennwortrichtlinie "One Identity Manager Kennwortrichtlinie" 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.

Tabelle 20: Zuweisen einer Kennwortrichtlinie

Eigenschaft	Beschreibung
Anwenden auf	Anwendungsbereich der Kennwortrichtlinie. ***Um den Anwendungsbereich festzulegen*** a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. b. Wählen Sie unter **Tabelle** die Tabelle, die die Kennwortspalte enthält. c. Wählen Sie unter **Anwenden auf** das konkrete Zielsystem. d. Klicken Sie **OK**.
Kennwortspalte	Bezeichnung der Kennwortspalte.
Kennwortrichtlinie	Bezeichnung der Kennwortrichtlinie, die angewendet werden soll.

5. Speichern Sie die Änderungen.

Um die Zuweisung einer Kennwortrichtlinie zu ändern

1. Wählen Sie im Manager die Kategorie **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.

Initiales Kennwort für neue Benutzerkonten

Tabelle 21: Konfigurationsparameter für die Bildung eines initialen Kennwortes für Benutzerkonten

Konfigurationsparameter	Bedeutung
QER\Person\UseCentralPassword	Der Konfigurationsparameter legt fest, ob das zentrale Kennwort einer Person in den Benutzerkonten verwendet werden soll. Das zentrale Kennwort der Person wird automatisch auf die Benutzerkonten der Person in allen erlaubten Zielsystemen abgebildet. Ausgenommen sind privilegierte Benutzerkonten; diese werden nicht aktualisiert.
QER\Person\UseCentralPassword\PermanentStore	Der Konfigurationsparameter steuert die Aufbewahrungszeit der zentralen Kennworte. Ist der Parameter aktiviert, wird das zentrale Kennwort der Person dauerhaft gespeichert. Ist der Parameter nicht aktiviert, wird das zentrale Kennwort nur zum Publizieren in die Zielsysteme benutzt und anschließend in der One Identity Manager-Datenbank gelöscht.
TargetSystem\CSM\Accounts\InitialRandomPassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von

Konfigurationsparameter	Bedeutung
	Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.

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

A. Verwenden Sie das zentrale Kennwort der Person. Das zentrale Kennwort der zugeordneten Person wird auf das Kennwort des Benutzerkontos abgebildet.

   - Aktivieren Sie im Designer den Konfigurationsparameter "QER\Person\UseCentralPassword".

     Ist der Konfigurationsparameter "QER\Person\UseCentralPassword" aktiviert, wird das zentrale Kennwort der Person automatisch auf die Benutzerkonten einer Person in den einzelnen Zielsystemen abgebildet. Ausgenommen sind privilegierte Benutzerkonten; diese werden nicht aktualisiert.

   - Aktivieren Sie im Designer den Konfigurationsparameter "QER\Person\UseCentralPassword\PermanentStore" und legen Sie fest, ob das zentrale Kennwort der Personen dauerhaft oder nur bis zum Publizieren in die Zielsysteme in der One Identity Manager-Datenbank gespeichert wird.

   Bei der Bildung des zentralen Kennwortes wird die Kennwortrichtlinie "Kennwortrichtlinie für zentrales Kennwort von Personen" angewendet.

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

B. Erstellen Sie Benutzerkonten manuell und tragen Sie in den Stammdaten der Benutzerkonten ein Kennwort ein.

C. Legen Sie ein initiales Kennwort fest, welches beim Erstellen von Benutzerkonten automatisch verwendet wird.

   - Verwenden Sie zielsystemspezifische Kennwortrichtlinien und tragen Sie in den Kennwortrichtlinien ein initiales Kennwort ein.

D. 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 auf Seite 56
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 68

E-Mail-Benachrichtigungen über Anmeldeinformationen

Tabelle 22: Konfigurationsparameter für Benachrichtigungen über Anmeldeinformationen

Konfigurationsparameter	Bedeutung
TargetSystem\CSM\Accounts\ InitialRandomPassword\SendTo	Der Konfigurationsparameter enthält die 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\CSM\DefaultAddress" hinterlegte Adresse versandt.
TargetSystem\CSM\Accounts\ InitialRandomPassword\SendTo\ MailTemplateAccountName	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den initialen Anmeldeinformationen (Name des Benutzerkontos) zu versorgen. Es wird die Mailvorlage "Person - Erstellung neues Benutzerkonto" verwendet.
TargetSystem\CSM\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den initialen Anmeldeinformationen (initiales Kennwort) zu versorgen. Es wird die Mailvorlage "Person - Initiales Kennwort für neues Benutzerkonto" verwendet.
TargetSystem\CSM\Defaul-tAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.

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 über Anmeldeinformationen zu nutzen

1. Stellen Sie sicher, dass das E-Mail-Benachrichtungssystem im One Identity Manager konfiguriert ist. Ausführliche Informationen finden Sie im One Identity Manager Konfigurationshandbuch.
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.

Zielsystemverantwortliche

Ausführliche Informationen zum Einsatz und zur Bearbeitung von Anwendungsrollen finden Sie im One Identity Manager Administrationshandbuch für Anwendungsrollen.

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 23: 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, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches

Benutzer	Aufgaben
	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.

- Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | Cloud Zielsysteme** zu.
- 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 10
- Allgemeine Stammdaten eines Cloud Zielsystems auf Seite 77
- Containerstrukturen in einem Cloud Zielsystem auf Seite 83

Bearbeiten eines Servers

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. Detaillierte Informationen dazu erhalten 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.

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

- Stammdaten eines Jobservers auf Seite 73
- Festlegen der Serverfunktionen auf Seite 75

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 14

Stammdaten eines Jobservers

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

Tabelle 24: Eigenschaften eines Jobservers

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

Eigenschaft	Bedeutung
	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. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte "Win32", "Windows", "Linux" und "Unix". Ist die Angabe leer, wird "Win32" angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden.

Eigenschaft	Bedeutung
	Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	Angabe, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur QBM_PJobQueueLoad aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Angabe, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Rechten im Programm "Job Queue Info" stoppen und starten.
kein automatisches Softwareupdate	Angabe, ob die von der automatischen Softwareaktualisierung auszuschließen sind. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Angabe, 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 75

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 25: 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. Für ein Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
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

- Stammdaten eines Jobservers auf Seite 73

4

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

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Cloud Zielsystems auf Seite 77
- Festlegen der Kategorien für die Vererbung von Gruppen auf Seite 80
- Alternative Spaltenbezeichnungen auf Seite 81

Allgemeine Stammdaten eines Cloud Zielsystems

Für ein Cloud-Zielsystem erfassen Sie die folgenden Stammdaten.

Tabelle 26: 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>`
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.
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	HINWEIS: Die Art der Synchronisation können Sie nur festlegen, wenn Sie ein Cloud Zielsystem neu anlegen. Nach dem Speichern sind keine Änderungen möglich.

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>Beim Erstellen eines Cloud Zielsystems mit dem Synchronization Editor wird "One Identity Manager" verwendet.

Art der Synchronisation, über welche die Daten zwischen dem Zielsystem und dem One Identity Manager synchronisiert werden.

Tabelle 27: 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>Beschreibung</td><td>Freitextfeld für zusätzliche Erläuterungen.</td></tr>
<tr><td>Manuelle Provisionierung</td><td>Angabe, 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.

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.</td></tr>
</table>

Eigenschaft	Beschreibung
	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	Angabe, 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 99
- Zielsystemverantwortliche auf Seite 70

Festlegen der Kategorien für die Vererbung von Gruppen

Im One Identity Manager können Gruppenselektiv 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 zwei Tabellen; die Benutzerkontentabelle und die Gruppentabelle. 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 "Position1" bis "Position 31".

Um Kategorien zu definieren

1. Wählen Sie 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. Wechseln Sie auf den Tabreiter **Abbildungsvorschrift Kategorien**.
5. Öffnen Sie den jeweiligen Basisknoten der Benutzerkontentabelle bzw. der Gruppentabelle.

6. Aktivieren Sie die Kategorie per Maus-Doppelklick auf das Symbol .
7. Tragen Sie eine beliebige Benennung der Kategorie für Benutzerkonten und Gruppen in der verwendeten Anmeldesprache ein.
8. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbung von Gruppen anhand von Kategorien auf Seite 120

Alternative Spaltenbezeichnungen

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 die Kategorie **Cloud Zielsysteme | Basisdaten zur Konfiguration | Cloud Zielsysteme**.
2. Wählen Sie in der Ergebnisliste ein Zielsystem. 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 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 die Kategorie **Cloud Zielsysteme | Basisdaten zur Konfiguration | Cloud Zielsysteme**.
2. Wählen Sie in der Ergebnisliste das Zielsystem. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten...**.

Verwandte Themen

- Anpassen einer Synchronisationskonfiguration auf Seite 27

Containerstrukturen in einem Cloud Zielsystem

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

Um die Stammdaten eines Containers zu bearbeiten

1. Wählen Sie 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 28: 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 Einga-

Eigenschaft	Beschreibung
	befeld. 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 70

6

Cloud Benutzerkonten

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

Detaillierte Informationen zum Thema

- Benutzerkonten mit Personen verbinden auf Seite 85
- Unterstützte Typen von Benutzerkonten auf Seite 86
- Erfassen der Stammdaten für Benutzerkonten auf Seite 90

Benutzerkonten mit Personen verbinden

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

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

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

- 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.

  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.

- 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 eine 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.

Verwandte Themen

- Erfassen der Stammdaten für Benutzerkonten auf Seite 90
- Einrichten von Kontendefinitionen auf Seite 38
- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 99

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

Unterstützte Typen von Benutzerkonten

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

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität (Spalte `IdentityType`)

  Die Identität beschreibt den Typ des Benutzerkontos.

Tabelle 29: Identitäten von Benutzerkonten

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

- Privilegiertes Benutzerkonto (Spalte `IsPrivilegedAccount`)

  Mit dieser Option werden Benutzerkonten mit besonderen privilegierten Berechtigungen gekennzeichnet. Dazu gehören beispielsweise administrative Benutzerkonten oder Dienstkonten. Standardbenutzerkonten werden nicht mit dieser Option gekennzeichnet.

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, beispielsweise ob der Container für ein Benutzerkonto über die Abteilung, die Kostenstelle, den Standort oder die Geschäftsrolle einer Person gebildet wird, 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.

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. Um administrativen Benutzerkonten einen Verantwortlichen zuzuweisen, weisen Sie dem Benutzerkonto im One Identity Manager eine Person zu.

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

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** (`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, beispielsweise ob der Container für ein Benutzerkonto über die Abteilung, die Kostenstelle, den Standort oder die Geschäftsrolle einer Person gebildet wird, 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 Gruppen 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.

HINWEIS: Wenn es unternehmensspezifisch erforderlich ist, dass die Anmeldenamen privilegierter Benutzerkonten einen definierten Namensschema folgen, legen Sie die Bildungsregel fest, nach denen Anmeldenamen gebildet werden.

Erfassen der Stammdaten für Benutzerkonten

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 die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie die Kategorie **Cloud Zielsysteme | <Zielsystem> | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Um ein Benutzerkonto für eine Person manuell zuzuweisen oder zu erstellen

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Benutzerkontos auf Seite 91
- Logindaten eines Benutzerkontos auf Seite 95
- Angaben zur Identifikation auf Seite 95
- Kontaktinformationen auf Seite 96
- Benutzerdefinierte Stammdaten auf Seite 97

Verwandte Themen

- Löschen von Benutzerkonten auf Seite 106

Allgemeine Stammdaten eines Benutzerkontos

Tabelle 30: Konfigurationsparameter für die Risikobewertung von Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
QER\CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

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

Tabelle 31: 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 erzeugt und in das Benutzerkonto übernommen.
Zielsystem	Cloud Zielsystem des Benutzerkontos.
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des

Eigenschaft	Beschreibung
	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. Um das Benutzerkonto manuell über eine Kontendefinition zu erstellen, tragen Sie im Eingabefeld **Person** eine Person ein. Es können alle Kontendefinitionen ausgewählt werden, die dieser Person zugewiesen sind und über die noch kein Benutzerkonto für diese Person erstellt wurde.
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.
Namenszusatz	Namenszusatz des Benutzers, beispielsweise "von" oder "zu".
Anzeigename	Anzeigename des Benutzerkontos.
Alias	Alias des Benutzerkontos zur weiteren Identifizierung.
Bezeichnung	Bezeichnung des Benutzerkontos.

Eigenschaft	Beschreibung
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. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
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.

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>Tabelle 32: Zulässige Werte für die Identität
<table>
<tr><th>Wert</th><th>Beschreibung</th></tr>
<tr><td>Primäre Identität</td><td>Standardbenutzerkonto einer Person.</td></tr>
<tr><td>Organisatorische Identität</td><td>Sekundäres Benutzerkonto, welches für unterschiedlichen Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen.</td></tr>
<tr><td>Persönliche Administratoridentität</td><td>Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird.</td></tr>
<tr><td>Zusatzidentität</td><td>Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird.</td></tr>
<tr><td>Gruppenidentität</td><td>Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird.</td></tr>
<tr><td>Dienstidentität</td><td>Dienstkonto.</td></tr>
</table></td></tr>
<tr><td>Privilegiertes Benutzerkonto</td><td>Angabe, ob es sich um ein privilegiertes Benutzerkonto handelt.</td></tr>
<tr><td>Gruppen erbbar</td><td>Angabe, ob das Benutzerkonto Gruppen über die Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt.
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.</td></tr>
<tr><td>Benutzerkonto ist deaktiviert</td><td>Angabe, ob das Benutzerkonto gesperrt ist. Wird ein Benutzerkonto vorübergehend nicht benötigt, können Sie das Benutzerkonto über die Option zeitweilig deaktivieren.</td></tr>
</table>

Verwandte Themen

- Sperren und Entsperren von Benutzerkonten auf Seite 104

Logindaten eines Benutzerkontos

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 33: Logindaten eines Benutzerkontos

Eigenschaft	Beschreibung
Kennwort/Kennwortbestätigung	Kennwort für das Benutzerkonto. Abhängig vom Konfigurationsparameter "Person\UseCentralPassword" wird das zentrale Kennwort der zugeordneten Person auf das Kennwort des Benutzerkontos abgebildet. Wenn Sie ein initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen.
Letzte Kennwortänderung	Datum der letzten Änderung des Kennwortes.
Letzte Anmeldung	Datum und Uhrzeit der letzten Anmeldung an der Cloud-Anwendung.

Verwandte Themen

- Kennwortrichtlinien auf Seite 56

Angaben zur Identifikation

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

Tabelle 34: Identifikationsdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Straße	Straße.
Postfach	Postfach.
Ort	Ort.
Postleitzahl	Postleitzahl.
Bundesland	Bundesland.

Eigenschaft	Beschreibung
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 Anstellung	Art der Anstellung.
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

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

Tabelle 35: Kontaktdaten eines Benutzerkontos

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

Benutzerdefinierte Stammdaten

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

Tabelle 36: 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.
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.

Zusätzliche Aufgaben für die Verwaltung von Benutzerkonten

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Überblick über das Benutzerkonto

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

Um einen Überblick über ein Benutzerkonto zu erhalten

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

Gruppen direkt an ein Benutzerkonto 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 die Kategorie **Cloud Zielsysteme | <Zielsystem> | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppen.
5. 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

- Gruppen an Benutzerkonten zuweisen auf Seite 111

Berechtigungselemente zuweisen

Mit dieser Aufgabe können Sie Berechtigungselemente an Benutzerkonten zuweisen.

Um Berechtigungselemente an ein Benutzerkonto zuzuweisen

1. Wählen Sie 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.

   - ODER -

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

5. Speichern Sie die Änderungen.

Zusatzeigenschaften 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 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.

   - ODER -

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

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

Automatische Zuordnung von Personen zu Benutzerkonten

Tabelle 37: Konfigurationsparameter für die Synchronisation einer Cloud-Anwendung

Konfigurationsparameter	Bedeutung
TargetSystem\CSM\PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\CSM\PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die

Konfigurationsparameter	Bedeutung
	Benutzerkonten erhalten keine Kontendefinition.
TargetSystem\CSM\PersonAutoFullSync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem\CSM\PersonExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird.

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

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

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

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

- Wenn Personen bei der Synchronisation von Benutzerkonten zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter „TargetSystem\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
  ```

- 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

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie dem Zielsystem eine Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand "Linked" (verbunden) die Kontendefinition und den Automatisierungsgrad zu.
   a. Wählen Sie die Kategorie **Cloud Zielsysteme | <Zielsystem> | Benutzerkonten | Verbunden aber nicht konfiguriert | <Zielsystem>**.
   b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

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

Verwandte Themen

- Erstellen einer Kontendefinition auf Seite 38
- Zuweisen der Kontendefinition an ein Cloud Zielsystem auf Seite 53

- Bearbeiten der Suchkriterien für die automatische Personenzuordnung auf Seite 102

Bearbeiten der Suchkriterien für die automatische Personenzuordnung

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

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

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

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

Um die Kriterien für die Personenzuordnung für ein Cloud Zielsystem zu definieren

1. Wählen Sie 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 38: Beispiel für die Suchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
Cloud Benut-zerkonten	Vorname (FirstName) UND Nachname (LastName)	Vorname (FirstName) UND Nachname (LastName)

5. Speichern Sie die Änderungen.

Direkte Zuordnung von Personen an Benutzerkonten anhand einer Vorschlagsliste

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

Tabelle 39: Ansichten zur manuellen Zuordnung

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

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

Um die Suchkriterien auf die Benutzerkonten anzuwenden

- Klicken Sie **Neu laden**.

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

Um Personen direkt über die Vorschlagsliste zuzuordnen

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

      Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet.

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

c. Klicken Sie **Ausgewählte zuweisen**.

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

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

Um Zuordnungen zu entfernen

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

   Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

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

Verwandte Themen

- Automatische Zuordnung von Personen zu Benutzerkonten auf Seite 99

Sperren und Entsperren von Benutzerkonten

Tabelle 40: Konfigurationsparameter für das Deaktivieren von Benutzerkonten

Konfigurationsparameter	Bedeutung
QER\Person\TemporaryDeactivation	Der Konfigurationsparameter legt fest, ob die Benutzerkonten der Person gesperrt werden, wenn die Person zeitweilig oder dauerhaft deaktiviert wird.

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 sperren

1. Wählen Sie 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 sperren, das nicht mit einer Person verbunden ist

1. Wählen Sie 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.

Verwandte Themen

Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

- Einrichten von Kontendefinitionen auf Seite 38
- Erstellen der Automatisierungsgrade auf Seite 41

Löschen von Benutzerkonten

Ein Benutzerkonto löschen Sie über die Ergebnisliste oder über die Menüleiste. Nach Bestätigung der Sicherheitsabfrage wird das Benutzerkonto aus der One Identity Manager Datenbank gelöscht.

Konfigurieren der Löschverzögerung

Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Während dieser Zeit besteht die Möglichkeit die Benutzerkonten wieder zu aktivieren. Nach Ablauf der Löschverzögerung ist ein Wiederherstellen nicht mehr möglich. Eine abweichende Löschverzögerung konfigurieren Sie im Designer an der Tabelle `CSMUser`.

Um ein Benutzerkonto zu löschen

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

Detaillierte Informationen zum Thema

- Provisionierung von Objektänderungen auf Seite 128
- Allgemeine Stammdaten eines Cloud Zielsystems auf Seite 77
- Sperren und Entsperren von Benutzerkonten auf Seite 104

Cloud Gruppen

Gruppen bilden die Objekte ab, über die in der Cloud-Anwendung der Zugriff auf die Cloud-Ressourcen gesteuert wird. Ein Benutzerkonto erhält über seine Gruppenmitgliedschaften die nötigen Rechte zum Zugriff auf die Cloud-Ressourcen.

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie die Kategorie **Cloud Zielsysteme | <Zielsystem> | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten für eine Gruppe.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Gruppe auf Seite 108
- Benutzerdefinierte Stammdaten einer Gruppe auf Seite 110

Allgemeine Stammdaten einer Gruppe

Tabelle 41: Konfigurationsparameter für die Risikobewertung von Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
QER\CalculateRiskIndex	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Berechnung des Risikoindex. Nach Änderung des Parameters müssen Sie die Datenbank kompilieren. Ist der Parameter aktiviert, können Werte für den Risikoindex erfasst und berechnet werden.

Zu einer Gruppe erfassen Sie die folgenden Stammdaten.

Tabelle 42: 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. 4. Klicken Sie **OK**.
IT Shop	Angabe, ob die Gruppe über den IT Shop bestellbar ist. Die Gruppe kann 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	Angabe, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Die Gruppe kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen ist nicht zulässig.
Leistungsposition	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter

Eigenschaft	Beschreibung
	"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. Über die Auswahlliste ordnen Sie die Gruppe einer oder mehreren Kategorien zu. 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

- Festlegen der Kategorien für die Vererbung von Gruppen auf Seite 80

Benutzerdefinierte Stammdaten einer Gruppe

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

Tabelle 43: 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.

Gruppen an Benutzerkonten zuweisen

Cloud Gruppen können direkt oder indirekt an Personen zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Gruppen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Gruppen, die einer Person zugewiesen ist. Wenn Sie eine Person in hierarchische Rollen aufnehmen und die Person ein Cloud Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Cloud Gruppe aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind:

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

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

Ausführliche Informationen zur Vererbung von Unternehmensressourcen finden Sie im One Identity Manager Administrationshandbuch für das Identity Management Basismodul.

Detaillierte Informationen zum Thema

- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 113
- Gruppen in Systemrollen aufnehmen auf Seite 114
- Gruppen in den IT Shop aufnehmen auf Seite 115

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 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.

    - ODER -

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

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

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

    - ODER -

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

    - ODER -

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

    - ODER -

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

Verwandte Themen

- Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 113
- Gruppen in Systemrollen aufnehmen auf Seite 114
- Gruppen in den IT Shop aufnehmen auf Seite 115
- One Identity Manager Benutzer für die Verwaltung von Cloud Zielsystemen auf Seite 10

Gruppen an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

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

   - ODER -

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

Um Gruppen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

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

   - ODER -

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

Verwandte Themen

- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 113
- Gruppen in Systemrollen aufnehmen auf Seite 114
- Gruppen in den IT Shop aufnehmen auf Seite 115
- One Identity Manager Benutzer für die Verwaltung von Cloud Zielsystemen auf Seite 10

Benutzerkonten direkt an eine Gruppe zuweisen

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

Um eine Gruppe direkt an Benutzerkonten zuzuweisen

1. Wählen Sie 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.

   - ODER -

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

Verwandte Themen

- Gruppen direkt an ein Benutzerkonto zuweisen auf Seite 98
- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Gruppen in Systemrollen aufnehmen auf Seite 114
- Gruppen in den IT Shop aufnehmen auf Seite 115

Gruppen in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

Mit dieser Aufgabe nehmen Sie eine Gruppe in Systemrollen auf. Wenn Sie eine Systemrolle an Personen zuweisen, wird die Gruppe an alle Benutzerkonten vererbt, die diese Personen besitzen.

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 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.

   - ODER -

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

Verwandte Themen

- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 113
- Gruppen in den IT Shop aufnehmen auf Seite 115

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.
- 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 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 die Kategorie **Cloud Zielsysteme | <Zielsystem> | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie 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. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppe an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen

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

   - ODER -

   Wählen Sie 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. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Gruppe aus allen Regalen des IT Shops zu entfernen

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

   - ODER -

   Wählen Sie 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

- Allgemeine Stammdaten einer Gruppe auf Seite 108
- Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- Gruppen an Geschäftsrollen zuweisen auf Seite 112
- Benutzerkonten direkt an eine Gruppe zuweisen auf Seite 113
- Gruppen in Systemrollen aufnehmen auf Seite 114

Zusätzliche Aufgaben für die Verwaltung von Gruppen

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Überblick über die Gruppe

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

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie die Kategorie **Cloud Zielsysteme | <Zielsystem> | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die Cloud Gruppe**.

Gruppen in Gruppen aufnehmen

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

Um Gruppen direkt an eine Gruppe zuzuweisen

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

   - ODER -

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

Wirksamkeit von Gruppenmitgliedschaften

Tabelle 44: Konfigurationsparameter für die bedingte Vererbung

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

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

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

HINWEIS:

- Ein wechselseitiger Ausschluss zweier Gruppen kann nicht definiert werden. Das heißt, die Festlegung "Gruppe A schließt Gruppe B aus" UND "Gruppe B schließt Gruppe A aus" ist nicht zulässig.
- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.

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

Beispiel für die 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 45: Festlegen der ausgeschlossenen Gruppen (Tabelle `CSMGroupExclusion`)

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

Tabelle 46: Wirksame Zuweisungen

Person	Mitglied in Rolle	Wirksame Gruppe
Ben King	Marketing	Gruppe A

Person	Mitglied in Rolle	Wirksame Gruppe
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 47: 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.
- Sich ausschließende Gruppen gehören zum selben Cloud Zielsystem.

Um Gruppen auszuschließen

1. Wählen Sie 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.

Vererbung von Gruppen anhand von Kategorien

Im One Identity Manager können Gruppenselektiv 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 zwei Tabellen; die Benutzerkontentabelle und die Gruppentabelle. 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 "Position1" bis "Position 31".

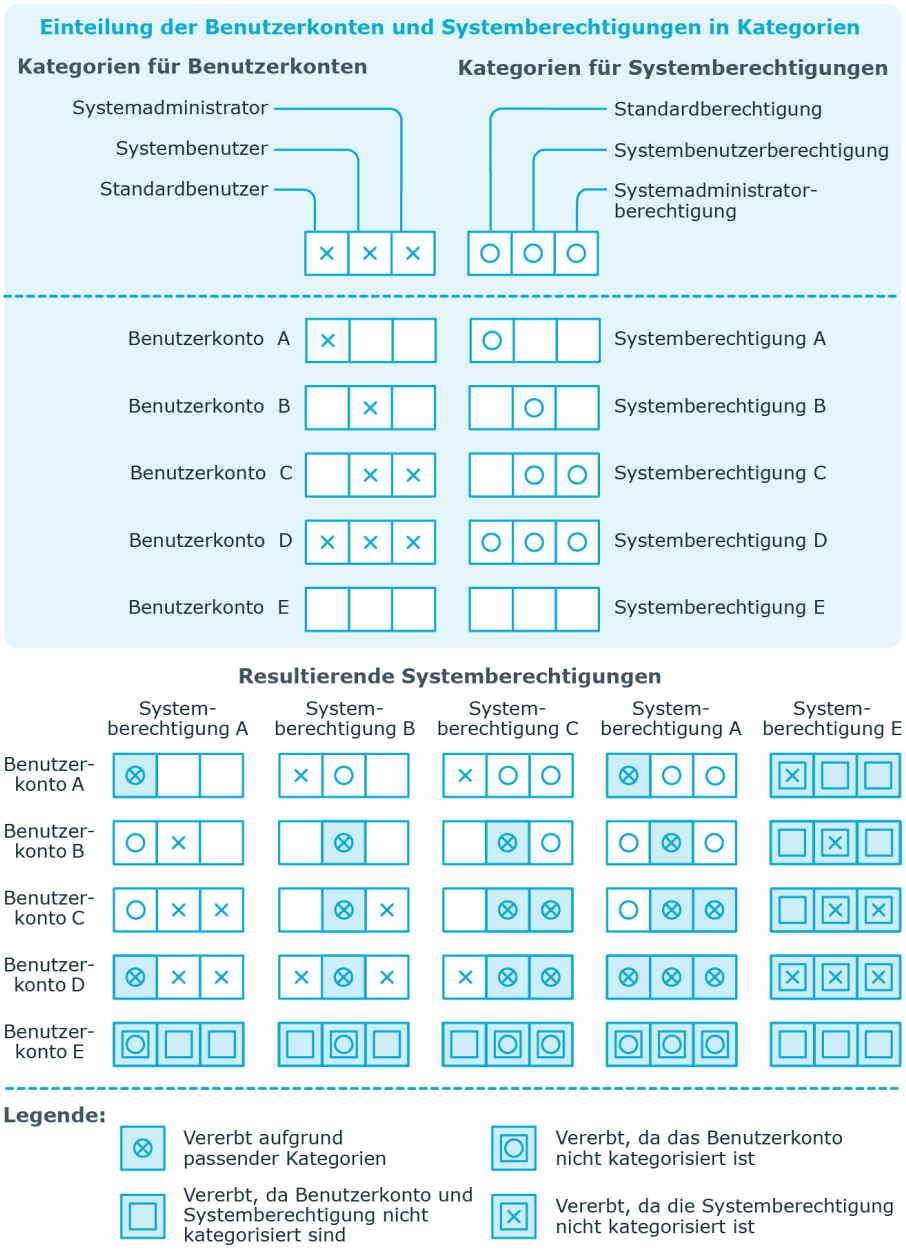
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist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

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

Tabelle 48: Beispiele für Kategorien

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

Abbildung 2: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

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

Verwandte Themen

- Festlegen der Kategorien für die Vererbung von Gruppen auf Seite 80
- Allgemeine Stammdaten eines Benutzerkontos auf Seite 91
- Allgemeine Stammdaten einer Gruppe auf Seite 108

Berechtigungselemente zuweisen

Mit dieser Aufgabe können Sie Berechtigungselemente an Gruppen zuweisen.

Um Berechtigungselemente an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **Cloud Zielsysteme | <Zielsystem> | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Berechtigungselemente zuweisen**.
4. Doppelklicken Sie im Bereich **Zuordnungen hinzufügen** auf die Berechtigungselemente, die zugewiesen werden sollen.

   - ODER -

   Doppelklicken Sie im Bereich **Zuordnungen entfernen** auf die Berechtigungselemente, deren Zuweisung entfernt werden soll.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Cloud Berechtigungselemente auf Seite 124

Zusatzeigenschaften 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 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.

   - ODER -

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

5. Speichern Sie die Änderungen.

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

Löschen von Gruppen

Um eine Gruppe zu löschen

1. Wählen Sie 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**.

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 Mitgliedschaften von Benutzerkonten in Gruppen gelöscht werden.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 128

Cloud Berechtigungselemente

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

Um Berechtigungselemente zu bearbeiten

1. Wählen Sie 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 eines Berechtigungselements auf Seite 124
- Benutzerdefinierte Stammdaten eines Berechtigungselements auf Seite 125

Allgemeine Stammdaten eines Berechtigungselements

Für ein Berechtigungselement erfassen Sie die folgenden Stammdaten.

Tabelle 49: Stammdaten eines Berechtigungselements

Eigenschaft	Beschreibung
Zielsystem	Cloud Zielsystem, in dem das Berechtigungselement gültig ist.

Eigenschaft	Beschreibung
Berechtigungselement	Bezeichnung des Berechtigungselements.
Berechtigungstyp	Zusätzliche Eigenschaft des Berechtigungselements.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Benutzerdefinierte Stammdaten eines Berechtigungselements

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

Tabelle 50: 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.

Zusätzliche Aufgaben für Berechtigungselemente

Nachdem Sie die Stammdaten erfasst haben, können Sie verschiedene Aufgaben anwenden. Über die Aufgabenansicht stehen verschiedene Formulare zur Verfügung, mit denen Sie folgende Aufgaben ausführen können.

Überblick über ein Berechtigungselement

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

Berechtigungselement an Benutzerkonten zuweisen

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

Um ein Berechtigungselement an Benutzerkonten zuzuweisen

1. Wählen Sie 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.

   - ODER -

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

Berechtigungselement an Gruppen zuweisen

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

Um ein Berechtigungselement an Gruppen zuzuweisen

1. Wählen Sie 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.

- ODER -

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

5. Speichern Sie die Änderungen.

Löschen von Berechtigungselementen

Um ein Berechtigungselement zu löschen

1. Wählen Sie 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**.

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.

Verwandte Themen

- Provisionierung von Objektänderungen auf Seite 128

9

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.

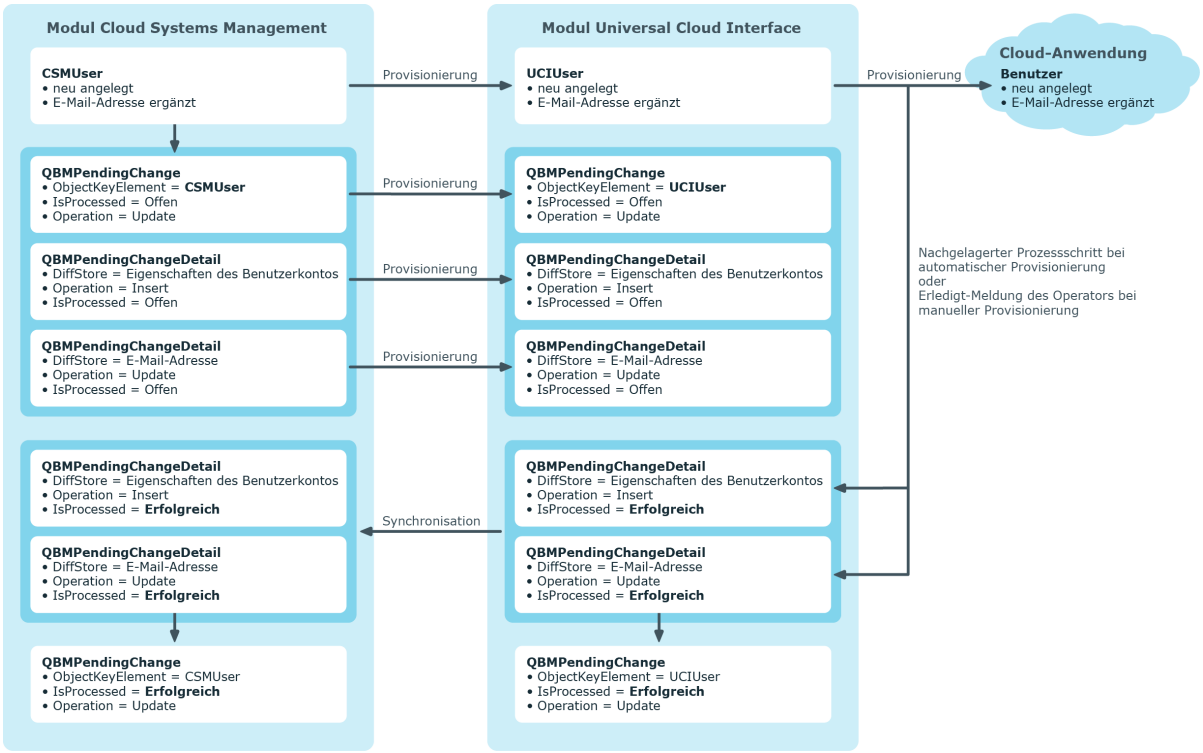
Detaillierte Informationen zum Thema

- Ablauf der Provisionierung auf Seite 128
- Aufbewahrungszeitraum für anstehende Änderungen auf Seite 129

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 3: 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.

Aufbewahrungszeitraum für anstehende Änderungen

Tabelle 51: Konfigurationsparameter für den Aufbewahrungszeitraum von anstehenden Änderungen

Konfigurationsparameter	Wirkung bei Aktivierung
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.

Konfigurationsparameter	Wirkung bei Aktivierung
QBM\PendingChange\LifeTimeSuccess	Der Konfigurationsparameter legt den Aufbewahrungszeitraum (in Tagen) für erfolgreiche Provisionierungsvorgänge fest. Der Standardzeitraum beträgt 2 Tage.

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".
2. Um den Aufbewahrungszeitraum für fehlgeschlagene Provisionierungsvorgänge zu konfigurieren, aktivieren Sie im Designer den Konfigurationsparameter "QBM\PendingChange\LifeTimeError".
3. Um den Aufbewahrungszeitraum für offene Provisionierungsvorgänge zu konfigurieren, aktivieren Sie im Designer den Konfigurationsparameter "QBM\PendingChange\LifeTimeRunning".
4. Geben Sie den Aufbewahrungszeitraum in Tagen an.

10

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 52: Berichte für das Zielsystem

Bericht	Beschreibung
Übersicht aller Zuweisungen (Cloud Zielsystem)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen (Cloud Container)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Container mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen (Cloud Gruppe)	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die die ausgewählte Gruppe besitzen.
Unverbundene Benutzerkonten anzeigen	Der Bericht zeigt alle Benutzerkonten des Zielsystems, denen keine Person zugeordnet ist. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung.
Personen mit mehreren Benutzerkonten anzeigen	Der Bericht zeigt alle Personen, die mehrere Benutzerkonten in dem Zielsystem besitzen. Der Bericht enthält eine Risikoeinschätzung.
Ungenutzte Benutzerkonten anzeigen	Der Bericht enthält alle Benutzerkonten des Zielsystems, die in den letzten Monaten nicht verwendet wurden. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung.
Abweichende	Der Bericht enthält alle Gruppen des Zielsystems, die aus

Bericht	Beschreibung
Systemberechtigungen anzeigen	manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen anzeigen	Der Bericht enthält alle Benutzerkonten des Zielsystems, die eine überdurchschnittliche Anzahl an Gruppenmitgliedschaften besitzen.
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 132

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 erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Gruppe besitzen.
- Wird der Bericht für eine Complianceregel erstellt, werden alle Rollen ermittelt, in denen sich Personen befinden, die diese Complianceregel verletzten.
- 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 (Abteilung, Kostenstelle, Standort, Geschäftsrolle oder IT Shop Struktur), 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 53: Bedeutung der Symbole in der Symbolleiste des Berichts

Symbol	Bedeutung
	Anzeigen der Legende mit der Bedeutung der Steuerelemente des Berichts.
	Speichern der aktuellen Ansicht des Berichts als Bild.
	Auswählen der Rollenklasse, über die der Bericht erstellt werden soll.
	Anzeige aller Rollen oder Anzeige der betroffenen Rolle.

Anhang: Konfigurationsparameter für die Verwaltung von Cloud Zielsystemen

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

Tabelle 54: 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.
TargetSystem\CSM\Accounts	Der Konfigurationsparameter erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem\CSM\Accounts\InitialRandomPassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.
TargetSystem\CSM\Accounts\InitialRandomPassword\SendTo	Der Konfigurationsparameter enthält die Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der

Konfigurationsparameter	Bedeutung
	Kostenstelle/Abteilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder XUserInserted). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter "TargetSystem\CSM\DefaultAddress" hinterlegte Adresse versandt.
TargetSystem\CSM\Accounts\ InitialRandomPassword\SendTo\ MailTemplateAccountName	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den initialen Anmeldeinformationen (Name des Benutzerkontos) zu versorgen. Es wird die Mailvorlage "Person - Erstellung neues Benutzerkonto" verwendet.
TargetSystem\CSM\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den initialen Anmeldeinformationen (initiales Kennwort) zu versorgen. Es wird die Mailvorlage "Person - Initiales Kennwort für neues Benutzerkonto" verwendet.
TargetSystem\CSM\Accounts\MailTemplateDefaultValues	Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage "Person - Erstellung neues Benutzerkonto mit Standardwerten" verwendet.
TargetSystem\CSM\Accounts\ PrivilegedAccount	Der Konfigurationsparameter erlaubt die Konfiguration der Einstellungen für privilegierte Benutzerkonten.
TargetSystem\CSM\Accounts\ PrivilegedAccount\ SAMAccountName_Postfix	Der Konfigurationsparameter enthält den Postfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem\CSM\Accounts\ PrivilegedAccount\	Der Konfigurationsparameter enthält den Präfix zur Bildung des

Konfigurationsparameter	Bedeutung
SAMAccountName_Prefix	Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem\CSM\DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem\CSM\ MaxFullsyncDuration	Der Konfigurationsparameter enthält die maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.
TargetSystem\CSM\PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\CSM\PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem\CSM\PersonAutoFullSync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem\CSM\PersonExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird.

Anhang: 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 Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 55: 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
UCIItem	CSMItem
UCIUser	CSMUser
UCIUserInGroup	CSMUserInGroup
UCIUserHasItem	CSMUserHasItem
QBMPendingChange	QBMPendingChange
QBMPendingChangeDetail	QBMPendingChangeDetail

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen besuchen Sie https://www.oneidentity.com/company/contact-us.aspx oder rufen Sie + 1-800-306-9329 an.

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 Selbsthilfetools, 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

G

I

J

K

O

P

R

S

V

Z