



One Identity Manager 8.1.3

Administrationshandbuch für die
Anbindung von Cloud-Anwendungen

Copyright 2020 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

Diese Anleitung enthält urheberrechtlich geschützte Informationen. Die in dieser Anleitung beschriebene Software wird unter einer Softwarelizenz oder einer Geheimhaltungsvereinbarung bereitgestellt. Diese Software darf nur in Übereinstimmung mit den Bestimmungen der geltenden Vereinbarung verwendet oder kopiert werden. Kein Teil dieser Anleitung darf ohne die schriftliche Erlaubnis von One Identity LLC in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch reproduziert oder übertragen werden, einschließlich Fotokopien und Aufzeichnungen für irgendeinen anderen Zweck als den persönlichen Gebrauch des Erwerbers.

Die Informationen in diesem Dokument werden in Verbindung mit One Identity Produkten bereitgestellt. Durch dieses Dokument oder im Zusammenhang mit dem Verkauf von One Identity LLC Produkten wird keine Lizenz, weder ausdrücklich oder stillschweigend, noch durch Duldung oder anderweitig, an jeglichem geistigen Eigentumsrecht eingeräumt. MIT AUSNAHME DER IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT GENANNTEN BEDINGUNGEN ÜBERNIMMT ONE IDENTITY KEINERLEI HAFTUNG UND SCHLIESST JEDLICHE AUSDRÜCKLICHE, IMPLIZIERTE ODER GESETZLICHE GEWÄHRLEISTUNG ODER GARANTIE IN BEZUG AUF IHRE PRODUKTE AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GEWÄHRLEISTUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ONE IDENTITY FÜR JEDLICHE DIREKTE, INDIREKTE, FOLGE-, STÖRUNGS-, SPEZIELLE ODER ZUFÄLLIGE SCHÄDEN (EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, SCHÄDEN FÜR VERLUST VON GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER VERLUST VON INFORMATIONEN), DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS RESULTIEREN, SELBST WENN ONE IDENTITY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN HAT. One Identity übernimmt keinerlei Zusicherungen oder Garantien hinsichtlich der Richtigkeit und Vollständigkeit des Inhalts dieses Dokuments und behält sich das Recht vor, Änderungen an Spezifikationen und Produktbeschreibungen jederzeit ohne vorherige Ankündigung vorzunehmen. One Identity verpflichtet sich nicht, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Wenn Sie Fragen zu Ihrer potenziellen Nutzung dieses Materials haben, wenden Sie sich bitte an:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Besuchen Sie unsere Website (<http://www.OneIdentity.com>) für regionale und internationale Büro-Adressen.



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

One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC. in den USA und anderen Ländern. Für eine vollständige Liste der One Identity Marken besuchen Sie bitte unsere Website unter www.OneIdentity.com/legal. Alle anderen Marken sind Eigentum der jeweiligen Besitzer.

Legende

-  **WARNUNG:** Das Symbol **WARNUNG** weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.
-  **VORSICHT:** Das Symbol **VORSICHT** weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

Inhalt

| | |
|--|-----------|
| Synchronisation von Cloud-Anwendungen über das Universal Cloud Interface | 6 |
| Architekturüberblick | 7 |
| One Identity Manager Benutzer für die Verwaltung von Cloud-Anwendungen | 9 |
| Einrichten der Synchronisation mit einer Cloud-Anwendung | 12 |
| Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung | 12 |
| Einrichten eines Synchronisationservers | 14 |
| Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung | 17 |
| Synchronisationsergebnisse anzeigen | 27 |
| Anpassen einer Synchronisationskonfiguration | 28 |
| Synchronisation in die Cloud-Anwendung konfigurieren | 30 |
| Schema aktualisieren | 30 |
| Beschleunigung der Synchronisation durch Revisionsfilterung | 31 |
| Provisionierung von Mitgliedschaften konfigurieren | 32 |
| Beschleunigung der Provisionierung und Einzelobjektsynchronisation | 34 |
| Unterstützung bei der Analyse von Synchronisationsproblemen | 35 |
| Deaktivieren der Synchronisation | 35 |
| Basisdaten für die Verwaltung von Cloud-Anwendungen | 37 |
| Administratoren | 38 |
| Operatoren | 39 |
| Auditoren | 41 |
| Bearbeiten eines Servers | 42 |
| Stammdaten eines Jobservers | 43 |
| Festlegen der Serverfunktionen | 45 |
| Cloud-Anwendungen | 47 |
| Allgemeine Stammdaten einer Cloud-Anwendung | 47 |
| Alternative Spaltenbezeichnungen | 49 |
| Synchronisationsprojekt bearbeiten | 49 |
| Containerstrukturen in einer Cloud-Anwendung | 51 |

| | |
|--|-----------|
| Benutzerkonten in einer Cloud-Anwendung | 53 |
| Allgemeine Stammdaten eines Benutzerkontos | 53 |
| Logindaten eines Benutzerkontos | 54 |
| Angaben zur Identifikation | 55 |
| Kontaktinformationen | 56 |
| Benutzerdefinierte Stammdaten | 56 |
| Zusätzliche Aufgaben für die Verwaltung von Benutzerkonten | 57 |
| Überblick über das Benutzerkonto | 57 |
| Zugewiesene Gruppen | 57 |
| Zugewiesene Berechtigungselemente | 57 |
| Gruppen in einer Cloud-Anwendung | 59 |
| Allgemeine Stammdaten einer Gruppe | 59 |
| Benutzerdefinierte Stammdaten einer Gruppe | 60 |
| Zusätzliche Aufgaben für die Verwaltung von Gruppen | 61 |
| Überblick über die Gruppe | 61 |
| Zugewiesene Benutzerkonten | 61 |
| Zugewiesene Gruppen | 61 |
| Zugewiesene Berechtigungselemente | 62 |
| Berechtigungselemente in einer Cloud-Anwendung | 63 |
| Allgemeine Stammdaten eines Berechtigungselements | 63 |
| Benutzerdefinierte Stammdaten eines Berechtigungselements | 64 |
| Zusätzliche Aufgaben für Berechtigungselemente | 64 |
| Überblick über ein Berechtigungselement | 64 |
| Zugewiesene Benutzerkonten | 65 |
| Zugewiesene Gruppen | 65 |
| Provisionierung von Objektänderungen | 66 |
| Ablauf der Provisionierung | 67 |
| Anstehende Änderungen anzeigen | 67 |
| Aufbewahrungszeitraum für anstehende Änderungen | 68 |
| Manuelle Provisionierung konfigurieren | 69 |
| Verwalten von Provisionierungsvorgängen im Web Portal | 71 |
| Bearbeiten von offenen Provisionierungsvorgängen | 72 |
| Einsehen und Bearbeiten von Provisionierungsvorgängen | 73 |
| Einsehen von allen Provisionierungsvorgängen | 73 |

| | |
|---|-----------|
| Einsehen von Statistiken | 74 |
| Zusätzliche Informationen für Experten | 75 |
| Anhang: Standardprojektvorlage für Cloud-Anwendungen | 78 |
| Über uns | 79 |
| Kontaktieren Sie uns | 79 |
| Technische Supportressourcen | 79 |
| Index | 80 |

Synchronisation von Cloud-Anwendungen über das Universal Cloud Interface

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.

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. Per Synchronisation werden die Daten zwischen den Modulen Universal Cloud Interface und Cloud Systems Management ausgetauscht. Provisionierungsprozesse sorgen dafür, dass Änderungen an den Objekten aus dem Modul Cloud Systems Management in das Modul Universal Cloud Interface übertragen werden.

Für manche Cloud-Anwendungen kann (aus technischen Gründen) oder soll (aufgrund der zu geringen Änderungsmenge) keine automatisierte Schnittstelle zum Provisionieren von Änderungen aus dem Modul Universal Cloud Interface in die Cloud-Anwendung eingesetzt werden. In diesem Fall können die Änderungen manuell provisioniert werden.

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

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

Architekturüberblick

Für den Datenaustausch mit einer Cloud-Anwendung kennt der One Identity Manager zwei Vorgehen.

- Automatische Synchronisation und Provisionierung

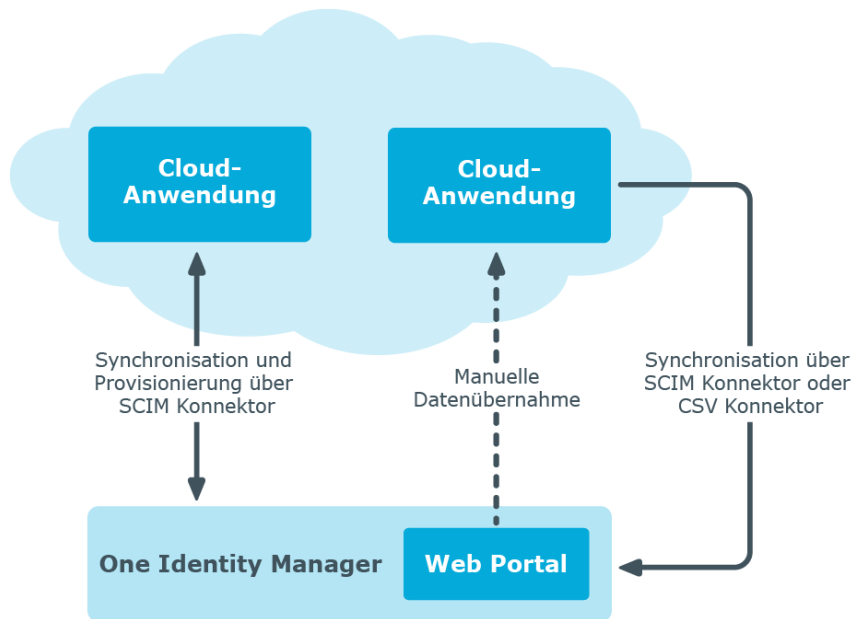
Die Synchronisation einer Cloud-Anwendung mit der One Identity Manager-Datenbank und die Provisionierung von Objektänderungen aus der One Identity Manager-Datenbank in die Cloud-Anwendung übernimmt der SCIM Konnektor des One Identity Manager. Mit diesem Standardvorgehen ist sichergestellt, dass die Daten zwischen Zielsystem und Datenbank regelmäßig abgeglichen und damit konsistent gehalten werden.

- Manuelle Provisionierung

Für manche Cloud-Anwendungen kann oder soll keine automatisierte Schnittstelle zum Provisionieren der Änderungen eingesetzt werden. Für solche Cloud-Anwendungen können die Änderungen manuell provisioniert werden. Für die Datenübernahme aus der Cloud-Anwendung in die One Identity Manager-Datenbank kann die Synchronisation mit dem SCIM Konnektor konfiguriert werden. Wenn der One Identity Manager auch keinen lesenden Zugriff auf die Cloud-Anwendung erhalten kann, können Sie den Datenaustausch beispielsweise über den CSV Konnektor einrichten.

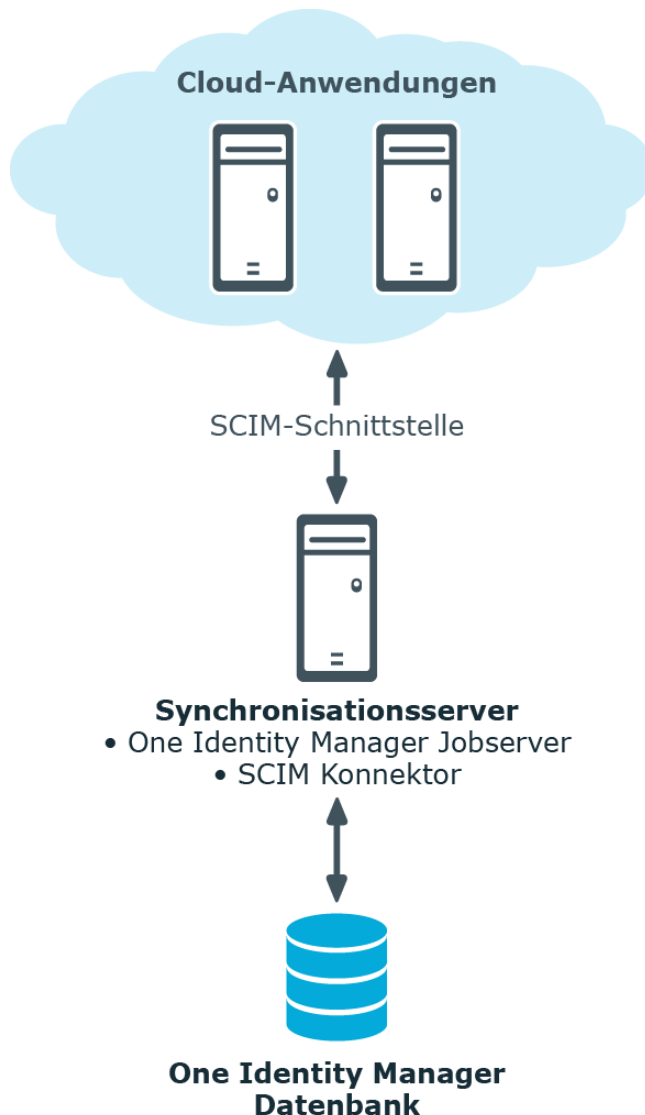
Mit diesem Vorgehen tragen Sie das Risiko von inkonsistenten Daten und Datenverlust, wenn manuelle Prozesse nicht eingehalten werden. Dieses Vorgehen wird daher nicht empfohlen.

Abbildung 1: Architektur für die Synchronisation



Um auf die Cloud-Anwendungen zuzugreifen, wird auf einem Synchronisationsserver der SCIM Konnektor installiert. Der SCIM Konnektor kann mit Cloud-Anwendungen kommunizieren, welche die System for Cross-domain Identity Management (SCIM) Spezifikation verstehen. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und der Cloud-Anwendung.

Abbildung 2: Topologie der Synchronisation



Detaillierte Informationen zum Thema

- [Einrichten der Synchronisation mit einer Cloud-Anwendung](#) auf Seite 12
- [Manuelle Provisionierung konfigurieren](#) auf Seite 69

One Identity Manager Benutzer für die Verwaltung von Cloud-Anwendungen

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

Tabelle 1: Benutzer

| Benutzer | Aufgaben |
|--------------------------------------|--|
| Administratoren | <p>Die Administratoren müssen der Anwendungsrolle Universal Cloud Interface Administratoren oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Administrieren die Anwendungsrollen für das Universal Cloud Interface.• Richten bei Bedarf weitere Anwendungsrollen ein.• Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Cloud-Anwendung und One Identity Manager.• Bearbeiten im Manager die Cloud-Anwendungen.• Bearbeiten offene, manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.• Erhalten im Web Portal und im Manager Informationen über die Cloud-Objekte. |
| Operatoren | <p>Die Operatoren müssen der Anwendungsrolle Universal Cloud Interface Operatoren oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Bearbeiten offene manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken. |
| Auditoren | <p>Die Auditoren müssen der Anwendungsrolle Universal Cloud Interface Auditoren oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Sehen manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken. |
| One Identity Manager Administratoren | <ul style="list-style-type: none">• 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. |

Benutzer

Aufgaben

- Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse.
- Erstellen und konfigurieren bei Bedarf Zeitpläne.
- Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.

Einrichten der Synchronisation mit einer Cloud-Anwendung

Der One Identity Manager unterstützt die Synchronisation mit Cloud-Anwendungen, welche die System for Cross-domain Identity Management (SCIM) Spezifikation in der Version 2.0 verstehen. Der One Identity Manager stellt eine Projektvorlage bereit, mit der Sie die Synchronisation zur Cloud-Anwendung einrichten können.

Um die Objekte einer Cloud-Anwendung initial in die One Identity Manager-Datenbank einzulesen

1. Stellen Sie einen Benutzer für den Zugriff auf die Cloud-Anwendung mit ausreichenden Berechtigungen bereit.
2. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
3. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- [Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung](#) auf Seite 12
- [Einrichten eines Synchronisationsservers](#) auf Seite 14
- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung](#) auf Seite 17

Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung

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

Tabelle 2: Benutzer für die Synchronisation

| Benutzer | Berechtigungen |
|--|--|
| Benutzerkonto des One Identity Manager Service | <p>Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Rechte vergeben, Verzeichnisse und Dateien anlegen und bearbeiten.</p> <p>Das Benutzerkonto muss der Gruppe Domänen-Benutzer angehören.</p> <p>Das Benutzerkonto benötigt das erweiterte Benutzerrecht Anmelden als Dienst.</p> <p>Das Benutzerkonto benötigt Rechte für den internen Webservice.</p> <p>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:</p> <pre>netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis.</p> <p>In der Standardinstallation wird der One Identity Manager installiert unter:</p> <ul style="list-style-type: none">• %ProgramFiles(x86)%\One Identity (auf 32-Bit Betriebssystemen)• %ProgramFiles%\One Identity (auf 64-Bit Betriebssystemen) |
| Sicherheitstoken oder Benutzer für den Zugriff auf die Cloud-Anwendung | Sicherheitstoken oder Benutzername und Kennwort, mit dem die Authentifizierung an der Cloud-Anwendung möglich ist. |
| Benutzer für den Zugriff auf die One Identity Manager-Datenbank | Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer Synchronization bereitgestellt. |

Einrichten eines Synchronisationsservers

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

- Windows Betriebssystem

Unterstützt werden die Versionen:

- Windows Server 2008 R2 (nicht-Itanium 64-Bit) ab Service Pack 1
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016
 - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 oder höher
| **HINWEIS:** Beachten Sie die Empfehlungen des Zielsystemherstellers.
 - Windows Installer
 - One Identity Manager Service, Synchronization Editor, SCIM Konnektor
 - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.
 1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
 2. Wählen Sie die Maschinenrolle **Server | Jobserver | SCIM**.

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

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

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

HINWEIS: Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der

Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Einrichten des Jobservers finden Sie im *One Identity Manager Konfigurationshandbuch*.

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

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

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

1. Starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation.
2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.
 - a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.
- ODER -
Um einen neuen Jobserver zu erstellen, klicken Sie **Hinzufügen**.
 - b. Bearbeiten Sie folgende Informationen für den Jobserver.
 - **Server:** Bezeichnung des Jobservers.
 - **Queue:** Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
 - **Vollständiger Servername:** Vollständiger Servername gemäß DNS Syntax.
Syntax:
<Name des Servers>.<Vollqualifizierter Domänenname>
4. Auf der Seite **Maschinenrollen** wählen Sie **SCIM**.
5. Auf der Seite **Serverfunktionen** wählen Sie **SCIM Konnektor**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und

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.

prüfen Sie die Konfiguration des One Identity Manager Service.

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

- Für eine direkte Verbindung zu Datenbank:
 - a. Wählen Sie **Prozessabholung | sqlprovider**
 - b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
 - c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
 - Für eine Verbindung zum Anwendungsserver:
 - a. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
 - b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
 - c. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
 - d. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
 - e. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
 8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
 9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.
 10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.
- HINWEIS:** Diese Seite wird nur angezeigt, wenn die Datenbank verschlüsselt ist.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
 - **Computer:** Name oder IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
 - **Dienstkonto:** Angaben zum Benutzerkonto des One Identity Manager Service.
 - Um den Dienst unter dem Konto **NT AUTHORITY\SYSTEM** zu starten, aktivieren Sie die Option **Lokales Systemkonto**.
 - Um den Dienst unter einem anderen Konto zu starten, deaktivieren Sie

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

- **Installationskonto:** Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.
 - Um das Benutzerkonto des angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Angemeldeter Benutzer**.
 - Um ein anderes Benutzerkonto zu verwenden, deaktivieren Sie die Option **Angemeldeter Benutzer** und geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.
 - Um das Installationsverzeichnis, den Namen, den Anzeigenamen oder die Beschreibung für den One Identity Manager Service zu ändern, nutzen Sie die weiteren Optionen.
12. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.
Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.
13. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

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

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und Cloud-Anwendung 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.

HINWEIS: Beachten Sie bei der Konfiguration, dass für Teile der URL gegebenenfalls die Groß-/Kleinschreibung beachtet werden muss.

Tabelle 3: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

| Angaben | Erläuterungen |
|--------------------------------|---|
| URL des Servers | URL, über die der Server erreicht werden kann, einschließlich des genutzten Übertragungsprotokolls. |
| Port | Port für den Zugriff auf die Cloud-Anwendung. |
| URI des Dienstes | URI, unter welchem der SCIM-Dienst erreichbar ist. |
| Authentifizierungsendpunkt/URL | URI, unter welchem die Authentifizierung möglich ist. Wird für die Authentifizierung ein anderer Server oder eine andere Basis-URL verwendet, ist hier die vollständige URL anzugeben. |
| Authentifizierungsart | Zulässige Authentifizierungsart für die Anmeldung an der Cloud-Anwendung. |
| Benutzername und Kennwort | Benutzername und Kennwort für die Anmeldung an der Cloud-Anwendung mit den Authentifizierungsarten "Basis-Authentifizierung", "OAuth-Authentifizierung" und "Ausgehandelte Authentifizierung". |
| Sicherheitstoken | Sicherheitstoken für die Anmeldung an der Cloud-Anwendung mit der Authentifizierungsart "OAuth-Authentifizierung". |
| Applikations-/Client-ID | Applikations-/Client-ID mit der die Cloud-Anwendung beim Sicherheitstokendienst registriert ist. Wird für die Anmeldung mit der Authentifizierungsart "OAuth-Authentifizierung" benötigt. |
| SCIM-Endpunkte | URIs oder URLs zu den Endpunkten für den Zugriff auf die Schemainformationen, Ressourceninformationen und Service-Provider-Informationen der Cloud-Anwendung. |
| Synchronisationsserver | <p>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.</p> <p>Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem SCIM Konnektor installiert sein.</p> <p>Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden</p> |

Angaben

Erläuterungen

Eigenschaften.

Tabelle 4: Zusätzliche Eigenschaften für den Jobserver

| Eigenschaft | Wert |
|----------------|-----------------------|
| Serverfunktion | SCIM Konnektor |
| Maschinenrolle | Server/Jobserver/SCIM |

Weitere Informationen finden Sie unter [Einrichten eines Synchronisationsservers](#) auf Seite 14.

Verbindungsdaten zur One Identity Manager-Datenbank

- Datenbankserver
- Datenbank
- SQL Server Anmeldung 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.

Remoteverbindungsserver

Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden.

Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen.

Konfiguration des Remoteverbindungservers:

- One Identity Manager Service ist gestartet
- **RemoteConnectPlugin** ist installiert
- SCIM Konnektor ist installiert

Angaben

Erläuterungen

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 SCIM Schnittstelle** und klicken Sie **Starten**.

Der Projektassistent des Synchronization Editors wird gestartet.

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

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

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

4. Auf der Seite **Verbindungsdaten** erfassen Sie die Verbindungsparameter, die der SCIM Konnektor zur Anmeldung an der Cloud-Anwendung benötigt.

Tabelle 5: Serverparameter

| Eigenschaft | Beschreibung |
|--------------------|--|
| URL des Servers | URL, über die der Server erreicht werden kann. Geben Sie auch das genutzte Übertragungsprotokoll an. |
| Port | Port für den Zugriff auf die Cloud-Anwendung. Wenn Standardports (HTTP:80, HTTPS:443) verwendet werden, kann dieses Feld frei bleiben. |
| URI des Dienstes | URI, unter welchem der SCIM-Dienst erreichbar ist. Es wird nur der Teil der URL benötigt, der von allen aufzurufenden Endpunkten gemeinsam verwendet wird. Der SCIM Konnektor setzt die URL aus der Server-URL, dem Port und dem URI zusammen. Beispiel: Wenn die komplette URL "https://identities.example.net:8080/scim/v2" lautet, dann ist hier als URI "scim/v2" einzugeben. |

Tabelle 6: Authentifizierungsart

| Eigenschaft | Beschreibung |
|---|---|
| Basis-Authentifizierung | Authentifizierung über Benutzername und Kennwort. |
| OAuth-Authentifizierung | Authentifizierung über das OAuth-Protokoll 2.0. |
| Ausgehandelte Authentifizierung (NTLM/Kerberos) | Authentifizierung mittels Windows Authentifizierungsmethoden wie NTLM oder Kerberos. |
| Authentifizierungsendpunkt/URL | URI, unter welchem die Authentifizierung möglich ist. Es wird nur der Teil der URL benötigt, der dem gemeinsamen Teil hinzuzufügen ist, um den Authentifizierungsendpunkt zu erreichen. Wird für die Authentifizierung ein anderer Server oder eine andere Basis-URL verwendet, ist hier die vollständige URL anzugeben. Beispiel: Wenn der komplette URI "https://identities.example.net:8080/scim/v2/auth/token" lautet, dann ist hier "auth/token" einzugeben. Wenn die Basis-URL oder der Server verschieden zur Ressourcen-URL ist, dann ist hier die komplette URL anzugeben, beispielsweise "https://authserver.example.net/token". |

- Auf der Seite **Basis-Authentifizierung** erfassen Sie Benutzername und Kennwort für die Authentifizierungsart "Basis-Authentifizierung".
- Auf der Seite **OAuth-Authentifizierung** geben Sie den Sicherheitstoken für die Authentifizierungsart "OAuth-Authentifizierung" an und wählen Sie den

Zugangstyp.

Tabelle 7: Eigenschaften der OAuth-Authentifizierung

| Eigenschaft | Beschreibung |
|---------------------------|---|
| Sicherheitstoken | Sicherheitstoken für die Anmeldung an der Cloud-Anwendung. Wenn der Sicherheitstoken nicht bekannt ist, erfassen Sie Benutzernamen und Kennwort. |
| Benutzername und Kennwort | Benutzername und Kennwort für die Anmeldung an der Cloud-Anwendung, wenn der Sicherheitstoken nicht bekannt ist. |
| Applikations-/Client-ID | Applikations-/Client-ID mit der die Cloud-Anwendung beim Sicherheitstokendienst registriert ist. |
| Zugangstyp | Zugangstyp für die Anmeldung an der Cloud-Anwendung mit der Authentifizierungsart "OAuth-Authentifizierung". Aktivieren Sie Client-Berechtigung oder Kennwort-Berechtigung . |
| Scope | Scope-Parameter, der für die Anmeldung am Zielsystem gültig ist. Wenn mehrere Parameter gültig sind, trennen Sie diese durch Leerzeichen. Ob ein Scope für die Anmeldung erforderlich ist und welche Scope-Parameter gültig sind, ist abhängig vom Service-Provider. |

- Auf der Seite **Ausgehandelte Authentifizierung** erfassen Sie Benutzernamen und Kennwort für die Authentifizierungsart "Ausgehandelte Authentifizierung (NTLM/Kerberos)".
- Auf der Seite **Clientzertifikat** wählen Sie das zu nutzende Zertifikat. Zertifikate können aus *.CER oder *.PFX - Dateien in den Zertifikatsspeicher des lokalen Computers importiert werden.

5. Auf der Seite **Verbindungseinstellungen prüfen** können Sie die erfassten Verbindungsdaten testen. Klicken Sie **Test**.

Der One Identity Manager versucht eine Verbindung zur Cloud-Anwendung aufzubauen.

TIPP: Der One Identity Manager speichert das Testergebnis. Wenn die Seite erneut aufgerufen wird und die Verbindungsdaten nicht geändert wurden, wird das gespeicherte Testergebnis angezeigt. War dieser Test erfolgreich, müssen die Verbindungsdaten nicht erneut getestet werden.

6. Auf der Seite **Endpunktkonfiguration** erfassen Sie die URIs zu den SCIM-Endpunkten. Wenn keine URIs angegeben sind, wird der SCIM-Standard verwendet.

Tabelle 8: Endpunktkonfiguration

| Eigenschaft | Beschreibung |
|-------------------------------|---|
| Schema | Endpunkt für den Zugriff auf die Schemainformationen der Cloud-Anwendung. |
| Ressourcen | Endpunkt für den Zugriff auf die Ressourceninformationen der Cloud-Anwendung, beispielsweise Gruppen oder Benutzerkonten. |
| Unterstützte Service-Optionen | Endpunkt für den Zugriff auf die Service-Provider-Informationen der Cloud-Anwendung. |

- Um die Verbindung zu den angegebenen Endpunkten zu testen, klicken Sie **Test**.

TIPP: Der One Identity Manager speichert das Testergebnis. Wenn die Seite erneut aufgerufen wird und die Endpunktkonfiguration nicht geändert wurde, wird das gespeicherte Testergebnis angezeigt.

7. Auf der Seite **Optimierungen** können Sie zusätzliche Einstellungen zur Optimierung der Synchronisationsperformance vornehmen.

Tabelle 9: Lokaler Cache

| Eigenschaft | Beschreibung |
|-------------------------|--|
| Lokalen Cache verwenden | <p>Angabe, ob der lokale Cache des SCIM Konnektors genutzt werden soll.</p> <p>Der lokale Cache wird genutzt, um die Synchronisation zu beschleunigen. Bei einer Vollsynchronisation werden die Zugriffe auf die Cloud-Anwendung minimiert. Bei der Provisionierung wird die Option ignoriert.</p> <p>Die Option ist standardmäßig aktiviert.</p> <p>Bei Synchronisationen mit Revisionsfilterung ist die Verwendung des Cache nicht sinnvoll. Wenn das Zielsystem die Revisionsfilterung unterstützt, deaktivieren Sie die Option nach der initialen Synchronisation.</p> |

8. Auf der Seite **Auswahl des Zielprodukts** kann das Verhalten des SCIM Konnektors auf die Eigenheiten spezieller Zielprodukte angepasst werden, beispielsweise auf HTTP-Request-Formate.

Tabelle 10: Zielprodukte

| Eigenschaft | Beschreibung |
|-------------------------------|--|
| SCIM Core V 2.0 | Produkt für die Synchronisation einer Standard-SCIM-Umgebung. |
| One Identity Starling Connect | Produkt für die Synchronisation einer One Identity Starling Connect-Umgebung |

9. Auf der Seite **Anzeigename** erfassen Sie einen eindeutigen Anzeigenamen für die Cloud-Anwendung.

Über den Anzeigenamen können Sie die Cloud-Anwendungen in den One Identity Manager Werkzeugen unterscheiden. Er kann nachträglich nicht mehr geändert werden.

10. Auf der letzten Seite des Systemverbindungsassistenten können Sie die Verbindungsdaten lokal speichern und die Konfiguration der Systemverbindung abschließen.
 - Aktivieren Sie die Option **Verbindung auf dem Computer 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**.
11. 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.
12. Der Assistent lädt das Zielsystemschemata. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
13. Auf der Seite **Projektvorlage auswählen** wählen Sie eine Projektvorlage, mit der die Synchronisationskonfiguration erstellt werden soll.

Tabelle 11: Standardprojektvorlagen

| Projektvorlage | Beschreibung |
|-----------------------|---|
| SCIM Synchronisation | Verwenden Sie diese Projektvorlage für die initiale Einrichtung des Synchronisationsprojektes für die Synchronisation einer System for Cross-domain Identity Management Umgebung. |
| Synchronisation | Verwenden Sie diese Projektvorlage für die initiale |

| Projektvorlage | Beschreibung |
|--|---|
| einer One Identity Starling Connect-Umgebung | Einrichtung des Synchronisationsprojektes für die Synchronisation einer SCIM-Umgebung über die One Identity Starling Connect Infrastruktur. |

HINWEIS: 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.


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

Tabelle 12: Zielsystemzugriff festlegen

| Option | Bedeutung |
|--|--|
| Das Zielsystem soll nur eingelesen werden. | <p>Angabe, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager-Datenbank eingerichtet werden soll.</p> <p>Der Synchronisationsworkflow zeigt folgende Besonderheiten:</p> <ul style="list-style-type: none"> • Die Synchronisationsrichtung ist In den One Identity Manager. • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung In den One Identity Manager definiert. |
| Es sollen auch Änderungen im Zielsystem durchgeführt werden. | <p>Angabe, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll.</p> <p>Der Provisionierungsworkflow zeigt folgende Besonderheiten:</p> <ul style="list-style-type: none"> • 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. |

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

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

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

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

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

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

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

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

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

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

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

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

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

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

6. 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.

7. Klicken Sie **OK**.

Um regelmäßige Synchronisationen auszuführen

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

Um die initiale Synchronisation manuell zu starten

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

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

Verwandte Themen

- [Einrichten eines Synchronisationsservers](#) auf Seite 14
- [Benutzer und Berechtigungen für die Synchronisation mit einer Cloud-Anwendung](#) auf Seite 12
- [Synchronisationsergebnisse anzeigen](#) auf Seite 27
- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 28
- [Beschleunigung der Synchronisation durch Revisionsfilterung](#) auf Seite 31
- [Zusätzliche Informationen für Experten](#) auf Seite 75
- [Standardprojektvorlage für Cloud-Anwendungen](#) auf Seite 78

Synchronisationsergebnisse anzeigen

Die Ergebnisse der Synchronisation werden im Synchronisationsprotokoll zusammengefasst. Der Umfang des Synchronisationsprotokolls kann für jede

Systemverbindung separat festgelegt werden. Der One Identity Manager stellt verschiedene Berichte bereit, in denen die Synchronisationsergebnisse nach verschiedenen Kriterien aufbereitet sind.

Um das Protokoll einer Synchronisation anzuzeigen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht ►.
In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.
Die Auswertung der Synchronisation wird als Bericht angezeigt. Sie können diesen Bericht speichern.

Um das Protokoll einer Provisionierung anzuzeigen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht ⚡.
In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.
Die Auswertung der Provisionierung wird als Bericht angezeigt. Sie können diesen Bericht speichern.

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

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

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation einer Cloud-Anwendung eingerichtet. Mit diesem Synchronisationsprojekt können Sie Objekte aus der Cloud-Anwendung in die One Identity Manager-Datenbank

einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in die Cloud-Anwendung provisioniert.

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

- Um bei der Synchronisation den One Identity Manager als Mastersystem zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um festzulegen, welche Cloud-Objekte und Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.
- 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.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschemata geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.

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

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

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

Detaillierte Informationen zum Thema

- [Synchronisation in die Cloud-Anwendung konfigurieren](#) auf Seite 30
- [Schema aktualisieren](#) auf Seite 30

Synchronisation in die Cloud-Anwendung konfigurieren

Das Synchronisationsprojekt für die initiale Synchronisation stellt je einen Workflow zum initialen Einlesen der Cloud-Objekte/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 Cloud-Anwendung zu erstellen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Prüfen Sie, ob die bestehenden Mappings für die Synchronisation in die Cloud-Anwendung 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.

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 Zielsystemschemata 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 Zielsystemschemata
 - 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 Synchronisation 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 Synchronisation 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 SCIM Konnektor unterstützt die Revisionsfilterung. Als Revisionszähler wird das Datum der letzten Änderung der Cloud-Objekte 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 Cloud-Objekte mit der in der One Identity Manager-Datenbank gespeicherten Revision verglichen. Es werden nur noch die Objekte aus der Cloud-Anwendung gelesen, die sich seit diesem Datum verändert haben.

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

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

Um die Revisionsfilterung an einem Workflow zuzulassen

- Öffnen Sie 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.

Provisionierung von Mitgliedschaften konfigurieren

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

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert (Beispiel: Liste von Benutzerkonten in der Eigenschaft `members~value` einer Cloud-Group).
- Änderungen von Mitgliedschaften sind in beiden verbundenen Systemen zulässig.
- Ein Provisionierungsworkflow und Provisionierungsprozesse sind eingerichtet.

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


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

Um die Einzelprovisionierung von Mitgliedschaften zu ermöglichen

1. Wählen Sie im Manager die Kategorie **Universal Cloud Interface | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
3. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
 - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte XDateSubItem oder CCC_XDateSubItem hat.
 - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden.
4. Klicken Sie **Merge-Modus**.
5. Speichern Sie die Änderungen.

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

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

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

Um die Standardbedingung wiederherzustellen

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

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

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

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

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

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

Um die Lastverteilung zu konfigurieren

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.

- Weisen Sie diesen Jobservern die Serverfunktion **SCIM Konnektor** zu.

Alle Jobserver müssen auf die gleiche Cloud-Anwendung zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.

2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

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

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

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

3. Weisen Sie diese Serverfunktion im Manager an alle Jobserver zu, welche die Prozesse zur Provisionierung und Einzelobjektsynchronisation für das Basisobjekt verarbeiten sollen.

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

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

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Detaillierte Informationen zum Thema

- [Bearbeiten eines Servers](#) auf Seite 42

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

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Startkonfiguration und deaktivieren Sie den hinterlegten Zeitplan.
Synchronisationen können nun nur noch manuell gestartet werden.

Ein aktiviertes Synchronisationsprojekt kann nur eingeschränkt bearbeitet werden. Sind Schemaänderungen notwendig, muss das Schema im Synchronisationsprojekt aktualisiert

werden. Dabei wird das Synchronisationsprojekt deaktiviert und kann erneut bearbeitet werden.

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

Um das Synchronisationsprojekt zu deaktivieren

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

Detaillierte Informationen zum Thema

- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung](#) auf Seite 17

Basisdaten für die Verwaltung von Cloud-Anwendungen

Für die Verwaltung einer Cloud-Anwendung im One Identity Manager sind folgende Basisdaten relevant.

- Administratoren

Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die die Synchronisation dieser Cloud-Anwendung mit dem One Identity Manager konfigurieren können. Im One Identity Manager ist eine Standardanwendungsrolle für die Administratoren vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, Synchronisationen einzurichten und manuelle Provisionierungen durchzuführen. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

Weitere Informationen finden Sie unter [Administratoren](#) auf Seite 38.

- Operatoren

Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die manuelle Provisionierungen durchführen können. Im One Identity Manager ist eine Standardanwendungsrolle für die Operatoren vorhanden. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

Weitere Informationen finden Sie unter [Operatoren](#) auf Seite 39.

- Auditoren

Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die Provisionierungsvorgänge im Web Portal auditieren können. Im One Identity Manager ist eine Standardanwendungsrolle für die Auditoren vorhanden. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

Weitere Informationen finden Sie unter [Auditoren](#) auf Seite 41.

- Server

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

Weitere Informationen finden Sie unter [Bearbeiten eines Servers](#) auf Seite 42.

Administratoren

Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die die Synchronisation dieser Cloud-Anwendung mit dem One Identity Manager konfigurieren können. Im One Identity Manager ist eine Standardanwendungsrolle für die Administratoren vorhanden. Weisen Sie dieser Anwendungsrolle die Personen zu, die berechtigt sind, Synchronisationen einzurichten und manuelle Provisionierungen durchzuführen. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

Tabelle 13: Standardanwendungsrolle für Administratoren


| Benutzer | Aufgaben |
|-----------------|--|
| Administratoren | <p>Die Administratoren müssen der Anwendungsrolle Universal Cloud Interface Administratoren oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Administrieren die Anwendungsrollen für das Universal Cloud Interface.• Richten bei Bedarf weitere Anwendungsrollen ein.• Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Cloud-Anwendung und One Identity Manager.• Bearbeiten im Manager die Cloud-Anwendungen.• Bearbeiten offene, manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.• Erhalten im Web Portal und im Manager Informationen über die Cloud-Objekte. |

Um eine Person initial als Administrator 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 | Universal Cloud Interface | Administratoren**.
3. Wählen Sie die Aufgabe **Personen zuweisen**.
4. Weisen Sie die Person zu und speichern Sie die Änderung.


Um Administratoren zu bearbeiten

1. Wählen Sie die Kategorie **Universal Cloud Interface | Basisdaten zur Konfiguration | Universal Cloud Interface Verantwortliche | Administratoren**.

2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
 - ODER -
 - Wählen Sie in der Ergebnisliste eine Anwendungsrolle. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
 - ODER -
 - Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Anwendungsrolle.
 - Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Universal Cloud Interface | Administratoren** oder eine untergeordnete Anwendungsrolle zu.
4. Speichern Sie die Änderungen.
5. Wählen Sie die Aufgabe **Personen zuweisen**, um Mitglieder in die Anwendungsrolle aufzunehmen.
6. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

Um eine Zuweisung zu entfernen

 - Wählen Sie die Person und doppelklicken Sie .
7. Speichern Sie die Änderungen.

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

Verwandte Themen

- [Einsehen und Bearbeiten von Provisionierungsvorgängen](#) auf Seite 73

Operatoren

Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die manuelle Provisionierungen durchführen können. Im One Identity Manager ist eine Standardanwendungsrolle für die Operatoren vorhanden. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

Tabelle 14: Standardanwendungsrolle für Operatoren

| Benutzer | Aufgaben |
|------------|---|
| Operatoren | Die Operatoren müssen der Anwendungsrolle Universal Cloud Interface Operatoren oder einer untergeordneten Anwendungsrolle zugewiesen sein. |

Benutzer Aufgaben

Benutzer mit dieser Anwendungsrolle:

- Bearbeiten offene manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken.

TIPP: Wenn Sie die Bearbeitungsrechte der Operatoren auf einzelne Cloud-Anwendungen einschränken wollen, definieren Sie untergeordnete Anwendungsrollen für diese Cloud-Anwendungen.

Um Operatoren festzulegen

1. Melden Sie sich mit der Anwendungsrolle **Universal Cloud Interface | Administratoren** am Manager an.
2. Wählen Sie die Kategorie **Universal Cloud Interface | Basisdaten zur Konfiguration | Cloud-Anwendungen**.
3. Wählen Sie in der Ergebnisliste die Cloud-Anwendung.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Operatoren** die Anwendungsrolle.

- ODER -

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

- Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Universal Cloud Interface | Operatoren** zu.
 - Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
6. Speichern Sie die Änderungen.
 7. Weisen Sie die Anwendungsrolle an die Personen zu, die berechtigt sind, die Cloud-Anwendung im One Identity Manager zu bearbeiten.

HINWEIS: Sie können Operatoren auch für einzelne Container festlegen. Die Operatoren eines Container sind berechtigt, die manuellen Provisionierungsvorgänge dieses Containers zu bearbeiten. Operatoren für Container legen Sie in der Kategorie **Universal Cloud Interface | <Cloud-Anwendung> | Containerstruktur** fest.

Um Personen in eine Anwendungsrolle aufzunehmen

1. Melden Sie sich mit der Anwendungsrolle **Universal Cloud Interface | Administratoren** am Manager an.
2. Wählen Sie die Aufgabe **Personen zuweisen**.
3. Weisen Sie die Personen zu und speichern Sie die Änderungen.

Verwandte Themen

- [Allgemeine Stammdaten einer Cloud-Anwendung](#) auf Seite 47
- [Containerstrukturen in einer Cloud-Anwendung](#) auf Seite 51
- [Bearbeiten von offenen Provisionierungsvorgängen](#) auf Seite 72
- Ausführliche Informationen zum Bearbeiten von Anwendungsrollen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Auditoren

Im One Identity Manager können Sie jeder Cloud-Anwendung Personen zuweisen, die Provisionierungsvorgänge im Web Portal auditieren können. Im One Identity Manager ist eine Standardanwendungsrolle für die Auditoren vorhanden. Bei Bedarf erstellen Sie weitere Anwendungsrollen.

Tabelle 15: Standardanwendungsrolle für Auditoren

| Benutzer | Aufgaben |
|-----------|---|
| Auditoren | Die Auditoren müssen der Anwendungsrolle Universal Cloud Interface Auditoren oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: <ul style="list-style-type: none">• Sehen manuelle Provisionierungsvorgänge im Web Portal und erhalten Statistiken. |


Um Auditoren festzulegen

1. Melden Sie sich mit der Anwendungsrolle **Universal Cloud Interface | Administratoren** am Manager an.
2. Wählen Sie die Kategorie **Universal Cloud Interface | Basisdaten zur Konfiguration | Universal Cloud Interface Verantwortliche | Auditoren**.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
- ODER -
Wählen Sie in der Ergebnisliste eine Anwendungsrolle. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
- ODER -
Klicken Sie in der Ergebnisliste .
4. Bearbeiten Sie die Stammdaten der Anwendungsrolle.
 - Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Universal Cloud Interface | Auditoren** oder eine untergeordnete Anwendungsrolle zu.
5. Speichern Sie die Änderungen.

6. Wählen Sie die Aufgabe **Personen zuweisen**, um Mitglieder in die Anwendungsrolle aufzunehmen.
7. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Person und doppelklicken Sie .

8. Speichern Sie die Änderungen.

Verwandte Themen

- [Einsehen von allen Provisionierungsvorgängen](#) auf Seite 73

Bearbeiten eines Servers

Für die Verarbeitung der cloud-spezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein. Um die Funktion eines Servers zu definieren, haben Sie mehrere Möglichkeiten:

- Erstellen Sie im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** einen Eintrag für den Jobserver. Ausführliche Informationen dazu finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Wählen Sie im Manager in der Kategorie **Universal Cloud Interface | 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 **Universal Cloud Interface | 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 43
- [Festlegen der Serverfunktionen](#) auf Seite 45

Verwandte Themen

- [Einrichten eines Synchronisationsservers](#) auf Seite 14

Stammdaten eines Jobservers

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

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

Tabelle 16: Eigenschaften eines Jobservers

| Eigenschaft | Bedeutung |
|-------------------------------|--|
| Server | Bezeichnung des Jobservers. |
| Vollständiger Servername | Vollständiger Servername gemäß DNS Syntax. 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. 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 |

| Eigenschaft | Bedeutung |
|------------------------------|--|
| Kopierverfahren (Zielserver) | dem Programm Robocopy und zwischen Servern mit einem Linux Betriebssystem mit dem Programm rsync. Unterscheiden sich die Betriebssysteme des Quellserver 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. |
| Codierung | Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden. |
| Übergeordneter Jobserver | Bezeichnung des übergeordneten Jobserver. |
| Ausführender Server | <p>Bezeichnung des ausführenden Servers. Eingegeben wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden.</p> <p>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.</p> |
| 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. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen. |

| Eigenschaft | Bedeutung |
|--|--|
| One Identity Manager Service installiert | <p>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.</p> <p>Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.</p> |
| Stopp One Identity Manager Service | <p>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.</p> <p>Den Dienst können Sie mit entsprechenden administrativen Rechten im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im <i>One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche</i>.</p> |
| Kein automatisches Softwareupdate | <p>Angabe, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist.</p> <p>HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.</p> |
| Softwareupdate läuft | Angabe, ob gerade eine Softwareaktualisierung ausgeführt wird. |
| Letzter Abrufzeitpunkt | Zeitpunkt der letzten Prozessabholung. |
| Letzte Timeout Prüfung | Zeitpunkt der letzten Prüfung für geladene Prozessschritte, deren Auslieferung den Wert im Konfigurationsparameter Common Jobservice LoadedJobsTimeOut überschreitet. |
| Serverfunktion | Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt. |

Verwandte Themen

- [Festlegen der Serverfunktionen](#) auf Seite 45

Festlegen der Serverfunktionen

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

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

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

Tabelle 17: Zulässige Serverfunktionen

| Serverfunktion | Anmerkungen |
|--|---|
| Aktualisierungsserver | <p>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.</p> <p>Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.</p> |
| SQL Ausführungsserver | <p>Der Server kann SQL Aufträge ausführen. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.</p> |
| CSV Skriptserver | <p>Der Server kann CSV-Dateien per Prozesskomponente ScriptComponent verarbeiten.</p> |
| One Identity Manager Service installiert | <p>Server, auf dem ein One Identity Manager Service installiert werden soll.</p> |
| SMTP Host | <p>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.</p> |
| Standard Berichtserver | <p>Server, auf dem die Berichte generiert werden.</p> |
| SCIM Konnektor | <p>Der Server kann sich mit einer Cloud-Anwendung verbinden.</p> |

Verwandte Themen

- [Stammdaten eines Jobservers](#) auf Seite 43

Cloud-Anwendungen

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

Die Stammdaten einer Cloud-Anwendung werden im Manager angezeigt. Neue Cloud-Anwendungen werden standardmäßig über den Synchronization Editor eingerichtet. Bei Bedarf kann eine Cloud-Anwendung auch im Manager neu angelegt werden. Für bestehende Cloud-Anwendungen werden die Eigenschaften im Modul Cloud Systems Management an den Cloud Zielsystemen gepflegt und durch die Provisionierung in das Modul Universal Cloud Interface übernommen. Die Operatoren müssen auch für bestehende Cloud-Anwendungen im Manager zugeordnet werden.

Um die Stammdaten einer Cloud-Anwendung zu bearbeiten

1. Wählen Sie die Kategorie **Universal Cloud Interface | Basisdaten zur Konfiguration | Cloud-Anwendungen**.
2. Wählen Sie in der Ergebnisliste eine Cloud-Anwendung. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Bearbeiten Sie die Stammdaten der Cloud-Anwendung.
4. Speichern Sie die Änderungen.

TIPP: Die Eigenschaften einer Cloud-Anwendung können Sie auch in der Kategorie **Universal Cloud Interface | <Cloud-Anwendung>** anzeigen.


Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten einer Cloud-Anwendung](#) auf Seite 47
- [Alternative Spaltenbezeichnungen](#) auf Seite 49

Allgemeine Stammdaten einer Cloud-Anwendung

Für eine Cloud-Anwendung erfassen Sie die folgenden Stammdaten.

Tabelle 18: Stammdaten einer Cloud-Anwendung

| Eigenschaft | Beschreibung |
|--------------------------------------|--|
| Cloud-Anwendung | Bezeichnung der Cloud-Anwendung. |
| Kanonischer Name | Vollständiger Name der Cloud-Anwendung. Der kanonische Name setzt sich zusammen aus dem DNS-Namen des Servers beziehungsweise dessen URL, dem Port und der URI des Dienstes. Beispiel: identities.example.net:8080/scim/v2 |
| Definierter Name | Definierter Name der Cloud-Anwendung. Der definierte Name wird zur Bildung der definierten Namen untergeordneter Objekte verwendet. Syntaxbeispiel: DC = <Kanonischer Name> |
| Anzeigename | Bezeichnung, unter der die Cloud-Anwendung in den Werkzeugen des One Identity Manager angezeigt wird. |
| Operatoren | Anwendungsrolle, in der die Operatoren festgelegt sind. Die Operatoren bearbeiten manuelle Provisionierungsvorgänge für die Cloud-Anwendung, der sie zugewiesen sind. Jeder Cloud-Anwendung können andere Operatoren zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle, deren Mitglieder manuelle Provisionierungsvorgänge bearbeiten dürfen. Über die Schaltfläche  neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |
| Manuelle Provisionierung | Angabe, ob Änderungen an Cloud-Objekten 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. WICHTIG: Wenn Sie die Option aktivieren, stellen Sie durch regelmäßige und häufige Synchronisationen sicher, dass die Daten zwischen der One Identity Manager-Datenbank und der Cloud-Anwendung konsistent gehalten werden! |
| Benutzerkonten löschen nicht erlaubt | Angabe, ob Benutzerkonten in der Cloud-Anwendung gelöscht werden dürfen. Wenn die Option aktiviert ist, können die Benutzerkonten lediglich deaktiviert werden. |

Verwandte Themen

- [Manuelle Provisionierung konfigurieren](#) auf Seite 69
- [Verwalten von Provisionierungsvorgängen im Web Portal](#) auf Seite 71

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 **Universal Cloud Interface | Basisdaten zur Konfiguration | Cloud-Anwendungen**.
2. Wählen Sie in der Ergebnisliste eine Cloud-Anwendung. 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 eine Cloud-Anwendung 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 **Universal Cloud Interface | Basisdaten zur Konfiguration | Cloud-Anwendungen**.
2. Wählen Sie in der Ergebnisliste die Cloud-Anwendung. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten....**

Verwandte Themen

- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 28

Containerstrukturen in einer Cloud-Anwendung

Die Containerstruktur repräsentiert die Strukturelemente einer Cloud-Anwendung. Container werden in einer hierarchischen Baumstruktur dargestellt.

Um die Stammdaten eines Containers anzuzeigen


1. Wählen Sie die Kategorie **Universal Cloud Interface | <Cloud-Anwendung> | Containerstruktur**.
2. Wählen Sie in der Ergebnisliste den Container.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Zu einem Container erhalten Sie die folgenden Stammdaten.

Tabelle 19: 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-Anwendung | Cloud-Anwendung des Containers. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |
| Kontomanager | Verantwortlicher für den Container. |
| Operatoren | Anwendungsrolle, in der die Operatoren festgelegt sind. Die Operatoren bearbeiten manuelle Provisionierungsvorgänge für den Container, dem sie zugewiesen sind. Jedem Container können andere Operatoren zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle, deren |

| Eigenschaft | Beschreibung |
|--------------------|---------------------|
|--------------------|---------------------|

Mitglieder manuelle Provisionierungsvorgänge bearbeiten dürfen. Über die Schaltfläche  neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.

Verwandte Themen

- [Operatoren](#) auf Seite 39

Benutzerkonten in einer Cloud-Anwendung

Die Benutzerkonten repräsentieren die Authentifizierungsobjekte einer Cloud-Anwendung. Ein Benutzerkonto erhält über seine Mitgliedschaften in Gruppen und Berechtigungselementen die nötigen Rechte zum Zugriff auf die Cloud-Ressourcen.

Um die Stammdaten eines Benutzerkontos anzuzeigen

1. Wählen Sie die Kategorie **Universal Cloud Interface** | **<Cloud-Anwendung>** | **Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Verwandte Themen

- [Allgemeine Stammdaten eines Benutzerkontos](#) auf Seite 53
- [Logindaten eines Benutzerkontos](#) auf Seite 54
- [Angaben zur Identifikation](#) auf Seite 55
- [Kontaktinformationen](#) auf Seite 56
- [Benutzerdefinierte Stammdaten](#) auf Seite 56

Allgemeine Stammdaten eines Benutzerkontos

Zu einem Benutzerkonto erhalten Sie die folgenden allgemeinen Stammdaten.

Tabelle 20: Allgemeine Stammdaten eines Benutzerkontos

| Eigenschaft | Beschreibung |
|-------------------------------|---|
| Cloud-Anwendung | Cloud-Anwendung des Benutzerkontos. |
| Anrede | Anrede des Benutzers. |
| Vorname | Vorname des Benutzers. |
| Nachname | Nachname des Benutzers. |
| Vollständiger Name | Vollständiger Name des Benutzers. |
| Initialen | Initialen des Benutzers. |
| Berufsbezeichnung | Berufsbezeichnung des Benutzers. |
| 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. |
| Container | Container des Benutzerkontos. |
| Erste primäre Gruppe | Primäre Gruppe des Benutzerkontos. |
| Zweite primäre Gruppe | Zusätzliche primäre Gruppe des Benutzerkontos. Wenn es in der Cloud-Anwendung Gruppen mit unterschiedlichen Gruppentypen gibt, kann hier eine weitere primäre Gruppe zugeordnet sein. |
| 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. |
| Ressourcentyp | Typ der Ressource, beispielsweise User. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |
| Anmeldename | Name, mit dem sich der Benutzer an der Cloud-Anwendung anmeldet. |
| Benutzerkonto ist deaktiviert | Angabe, ob das Benutzerkonto gesperrt ist. |

Logindaten eines Benutzerkontos

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

Tabelle 21: Logindaten eines Benutzerkontos

| Eigenschaft | Beschreibung |
|------------------------------|---|
| Kennwort/Kennwortbestätigung | Kennwort für das Benutzerkonto. |
| Letzte Kennwortänderung | Datum der letzten Änderung des Kennwortes. |
| Letzte Anmeldung | Datum und Uhrzeit der letzten Anmeldung an der Cloud-Anwendung. |

Angaben zur Identifikation

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

Tabelle 22: Identifikationsdaten eines Benutzerkontos

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

Kontaktinformationen

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

Tabelle 23: 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 24: 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

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 **Universal Cloud Interface | <Cloud-Anwendung> | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das Benutzerkonto**.

Zugewiesene Gruppen

Über diese Aufgabe sehen Sie alle Gruppen, die dem Benutzerkonto zugewiesen sind.

Um zugewiesene Gruppen anzuzeigen

1. Wählen Sie die Kategorie **Universal Cloud Interface | <Cloud-Anwendung> | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.

Verwandte Themen

- [Gruppen in einer Cloud-Anwendung](#) auf Seite 59

Zugewiesene Berechtigungselemente

Über diese Aufgabe sehen Sie alle Berechtigungselemente, die dem Benutzerkonto zugewiesen sind.

Um zugewiesene Berechtigungselemente anzuzeigen

1. Wählen Sie die Kategorie **Universal Cloud Interface** | **<Cloud-Anwendung>** | **Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Berechtigungselemente zuweisen**.

Verwandte Themen

- [Berechtigungselemente in einer Cloud-Anwendung](#) auf Seite 63

Gruppen in einer Cloud-Anwendung

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 anzuzeigen

1. Wählen Sie die Kategorie **Universal Cloud Interface** | **<Cloud-Anwendung>** | **Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten einer Gruppe](#) auf Seite 59
- [Benutzerdefinierte Stammdaten einer Gruppe](#) auf Seite 60

Allgemeine Stammdaten einer Gruppe

Zu einer Gruppe erhalten Sie die folgenden allgemeinen Stammdaten.

Tabelle 25: Allgemeine Stammdaten einer Gruppe

| Eigenschaft | Beschreibung |
|------------------|------------------------------|
| Bezeichnung | Bezeichnung der Gruppe. |
| Container | Container der Gruppe. |
| Cloud-Anwendung | Cloud-Anwendung der Gruppe. |
| Definierter Name | Definierter Name der Gruppe. |

| Eigenschaft | Beschreibung |
|--------------------|--|
| 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. |
| Beschreibung | Freitextfeld für zusätzliche Erläuterungen. |
| Gruppentyp | Name des Gruppentyps. |
| Ressourcentyp | Typ der Ressource, beispielsweise Group. |

Benutzerdefinierte Stammdaten einer Gruppe

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

Tabelle 26: 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. |

Zusätzliche Aufgaben für die Verwaltung von Gruppen

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 **Universal Cloud Interface | <Cloud-Anwendung> | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die Gruppe**.

Zugewiesene Benutzerkonten

Über diese Aufgabe sehen Sie alle Benutzerkonten, die der Gruppe zugewiesen sind.

Um zugewiesene Benutzerkonten anzuzeigen

1. Wählen Sie die Kategorie **Universal Cloud Interface | <Cloud-Anwendung> | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.

Verwandte Themen

- [Benutzerkonten in einer Cloud-Anwendung](#) auf Seite 53

Zugewiesene Gruppen

Über diese Aufgabe sehen Sie alle Gruppen, die der Gruppe zugewiesen sind.

Um zugewiesene Gruppen anzuzeigen

1. Wählen Sie die Kategorie **Universal Cloud Interface | <Cloud-Anwendung> | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.

Zugewiesene Berechtigungselemente

Über diese Aufgabe sehen Sie alle Berechtigungselemente, die der Gruppe zugewiesen sind.

Um zugewiesene Berechtigungselemente anzuzeigen

1. Wählen Sie die Kategorie **Universal Cloud Interface | <Cloud-Anwendung> | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Berechtigungselemente zuweisen**.

Verwandte Themen

- [Berechtigungselemente in einer Cloud-Anwendung](#) auf Seite 63

Berechtigungselemente in einer Cloud-Anwendung

Berechtigungselemente bilden beliebige weitere Objekte der Cloud-Anwendung ab.

Um die Stammdaten eines Berechtigungselements anzuzeigen

1. Wählen Sie die Kategorie **Universal Cloud Interface | <Cloud-Anwendung> | Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten eines Berechtigungselements](#) auf Seite 63
- [Benutzerdefinierte Stammdaten eines Berechtigungselements](#) auf Seite 64

Allgemeine Stammdaten eines Berechtigungselements

Für ein Berechtigungselement erhalten Sie die folgenden Stammdaten.

Tabelle 27: Allgemeine Stammdaten eines Berechtigungselements

| Eigenschaft | Beschreibung |
|----------------------|--|
| Cloud-Anwendung | Cloud-Anwendung, in der das Berechtigungselement gültig ist. |
| 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 28: 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

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 **Universal Cloud Interface** | **<Cloud-Anwendung>** | **Berechtigungselemente**.

2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Überblick über das Berechtigungselement**.

Zugewiesene Benutzerkonten

Über diese Aufgabe sehen Sie alle Benutzerkonten, die dem Berechtigungselement zugewiesen sind.

Um zugewiesene Benutzerkonten anzuzeigen

1. Wählen Sie die Kategorie **Universal Cloud Interface | <Cloud-Anwendung> | Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.

Verwandte Themen

- [Benutzerkonten in einer Cloud-Anwendung](#) auf Seite 53

Zugewiesene Gruppen

Über diese Aufgabe sehen Sie alle Gruppen, die dem Berechtigungselement zugewiesen sind.

Um zugewiesene Gruppen anzuzeigen

1. Wählen Sie die Kategorie **Universal Cloud Interface | <Cloud-Anwendung> | Berechtigungselemente**.
2. Wählen Sie in der Ergebnisliste das Berechtigungselement.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.

Verwandte Themen

- [Gruppen in einer Cloud-Anwendung](#) auf Seite 59

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. Für manche Cloud-Anwendungen kann oder soll keine automatisierte Schnittstelle zum Provisionieren der Änderungen eingesetzt werden. Für solche Cloud-Anwendungen können die Änderungen manuell provisioniert werden. Über ein Web Portal werden die manuellen Provisionierungsvorgänge angezeigt. Operatoren können anhand dieser Übersicht die anstehenden Änderungen in die Cloud-Anwendungen übertragen.

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. Bei der automatischen Provisionierung werden die anstehenden Änderungen in der Reihenfolge ihrer Erstellung verarbeitet. Für die manuelle Provisionierung werden die anstehenden Änderungen in der Reihenfolge ihrer Erstellung im Web Portal aufgelistet.

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.

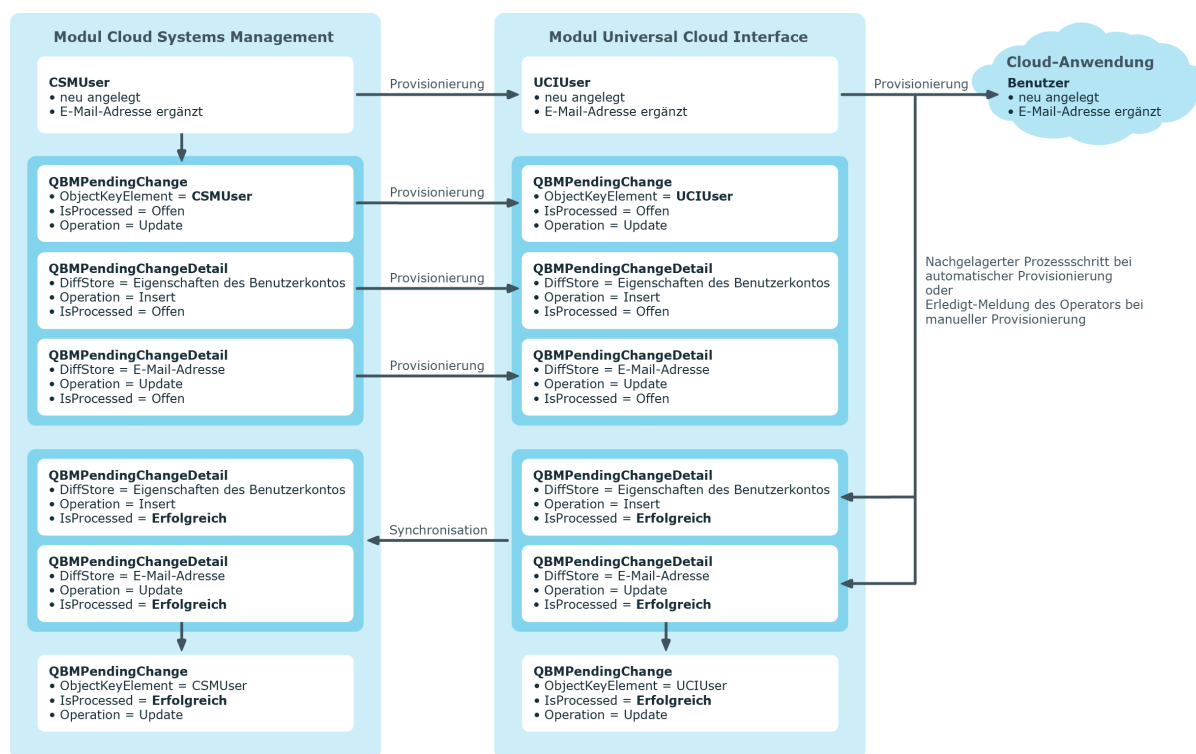
Detaillierte Informationen zum Thema

- [Ablauf der Provisionierung](#) auf Seite 67
- [Manuelle Provisionierung konfigurieren](#) auf Seite 69
- [Aufbewahrungszeitraum für anstehende Änderungen](#) auf Seite 68

Ablauf der Provisionierung

Folgende Grafik zeigt die Provisionierung von Objektänderungen und die zugehörige Verarbeitung der anstehenden Änderungen. Der Ablauf ist für automatische und manuelle Provisionierungsvorgänge identisch und 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 Bearbeitungsstatus für die anstehenden Änderungen zeitnah im Modul Cloud Systems Management bekannt ist.



Anstehende Änderungen anzeigen

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

Um anstehende Änderungen anzuzeigen

- Wählen Sie das Menü **Datenbank | Anstehende Änderungen**.

Tabelle 29: Bedeutung der Einträge in der Symbolleiste

| Symbol | Bedeutung |
|---|-------------------------------|
|  | Ausgewähltes Objekt anzeigen. |
|  | Ansicht aktualisieren. |

Aufbewahrungszeitraum für anstehende Änderungen

Tabelle 30: 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. |
| 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. Die definierten Fristen gelten gleichermaßen für automatische als auch manuelle Provisionierungsvorgänge.

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.

Manuelle Provisionierung konfigurieren

VORSICHT: Datenverlust durch inkonsistente Daten!

Wenn Sie die manuelle Provisionierung wählen, müssen Sie durch geeignete manuelle Prozesse sicherstellen, dass die Änderungen aus der One Identity Manager-Datenbank zeitnah in die Cloud-Anwendung übertragen werden.

Stellen Sie sicher, dass die Daten zwischen Cloud-Anwendung und One Identity Manager-Datenbank regelmäßig und zeitnah abgeglichen werden. Richten Sie dafür die Synchronisation über den SCIM Konnektor ein. Sollte das nicht möglich sein, können Sie die Synchronisation über den CSV Konnektor nutzen.

Ob eine manuelle Provisionierung zulässig ist, wird an den Cloud-Anwendungen konfiguriert. Über ein Web Portal werden die offenen manuellen Provisionierungsvorgänge für diese Cloud-Anwendungen angezeigt. Operatoren können anhand dieser Übersicht die anstehenden Änderungen in die Cloud-Anwendungen übertragen und danach als erledigt kennzeichnen. Auditoren können die offenen und die verarbeiteten Provisionierungsvorgänge im Web Portal prüfen.

Um die manuelle Provisionierung zu konfigurieren

1. Bearbeiten Sie die Stammdaten der Cloud-Anwendung.
 - a. Aktivieren Sie die Option **Manuelle Provisionierung**.
 - b. Ordnen Sie die Operatoren zu, welche die offenen Provisionierungsvorgänge im Web Portal bearbeiten dürfen.

TIPP: Sie können Operatoren auch für einzelne Container festlegen. Weitere Informationen finden Sie unter [Containerstrukturen in einer Cloud-Anwendung](#) auf Seite 51.
2. Legen Sie die Auditoren fest, die manuelle Provisionierungsvorgänge im Web Portal prüfen dürfen.

Detaillierte Informationen zum Thema

- [Cloud-Anwendungen](#) auf Seite 47
- [Allgemeine Stammdaten einer Cloud-Anwendung](#) auf Seite 47
- [Operatoren](#) auf Seite 39
- [Auditoren](#) auf Seite 41
- [Bearbeiten von offenen Provisionierungsvorgängen](#) auf Seite 72

- [Einsehen von allen Provisionierungsvorgängen](#) auf Seite 73
- [Einrichten der Synchronisation mit einer Cloud-Anwendung](#) auf Seite 12

Ausführliche Informationen zum Einrichten der Synchronisation mit dem CSV Konnektor finden Sie im One Identity Manager Anwenderhandbuch für den CSV Konnektor.

Verwalten von Provisionierungsvorgängen im Web Portal

Über das Web Portal werden die offenen manuellen Provisionierungsvorgänge für Cloud-Anwendungen angezeigt. Operatoren können anhand dieser Übersicht die anstehenden Änderungen in die Cloud-Anwendungen übertragen und danach als erledigt kennzeichnen. Auditoren können die offenen und die verarbeiteten Provisionierungsvorgänge im Web Portal prüfen.

Abhängig davon welche Anwendungsrolle der Benutzer besitzt, kann er entsprechend seiner Berechtigungen, Provisionierungsvorgänge im Web Portal einsehen oder verwalten. Weitere Informationen finden Sie unter [One Identity Manager Benutzer für die Verwaltung von Cloud-Anwendungen](#) auf Seite 9.

Um sich im Web Portal anzumelden

1. Öffnen Sie die Web Portal Seite, in dem Sie in der Adressleiste des Webbrowsers die URL-Adresse der Web Portal Seite eingeben.
Standardmäßig lautet die URL `http://<Servername>/Applikationsname/`, wobei `<Servername>` der Name des Servers ist, auf dem die Web Portal Anwendung installiert ist.
2. Erfassen Sie im Textfeld **Anmeldename** Ihren vollständigen Anmeldenamen.
3. Erfassen Sie im Textfeld **Kennwort** Ihr persönliches Kennwort.
4. Klicken Sie **Anmelden**.

Ausführliche Informationen zur Anmeldung am Web Portal finden Sie im One Identity Manager Anwenderhandbuch für das Web Portal.

Detaillierte Informationen zum Thema

- [Provisionierung von Objektänderungen](#) auf Seite 66
- [Bearbeiten von offenen Provisionierungsvorgängen](#) auf Seite 72
- [Einsehen und Bearbeiten von Provisionierungsvorgängen](#) auf Seite 73
- [Einsehen von allen Provisionierungsvorgängen](#) auf Seite 73

Bearbeiten von offenen Provisionierungsvorgängen

Als Operator bearbeiten Sie offene, manuelle Provisionierungsvorgänge im Web Portal. Ein Provisionierungsvorgang ist ein Arbeitsauftrag für den Operator, für die er eine Operation an einem Zielobjekt ausführt. Es gibt folgende Zielobjekte.

Tabelle 31:
Zielobjekte

Benutzerkonto

Gruppe

Zuweisung

HINWEIS: Neben dem Operator kann auch ein Administrator offene Provisionierungsvorgänge bearbeiten.

In der Ansicht **Offene Cloud Operationen** werden Ihnen die Vorgänge absteigend sortiert nach Eingangsdatum mit Objektnamen und Beschreibung der Operation angezeigt. Die Operationsart sehen Sie im Anzeigefeld **Operation** in den Detailinformationen zum markierten Vorgang. Es gibt folgende Operationsarten.

Tabelle 32: Operationsarten

Neues Objekt Erstellen Sie ein neues Objekt.

Änderung Setzen Sie einen Wert im Zielsystem.

Löschung Löschen Sie ein Objekt.

In den Detailinformationen wird zu jeder angeforderten Operation eine ausführliche Anweisung formuliert, die mit **i** gekennzeichnet ist. Sind zu einem Zielobjekt mehrere offene Vorgänge vorhanden, arbeiten Sie die Vorgänge in der Reihenfolge ihres Eintreffens ab. Das heißt, der älteste Vorgang muss zuerst bearbeitet werden.

Um offene Provisionierungsvorgänge zu bearbeiten

1. Öffnen Sie auf der Startseite des Web Portals das Menü **Offene Cloud Operationen**.
2. Markieren Sie in der Ansicht **Offene Cloud Operationen** den gewünschten Provisionierungsvorgang.
HINWEIS: Werden in den Detailinformationen zum markierten offenen Vorgang mehrere Operationen untereinander angezeigt, bearbeiten Sie die erste Operation.
3. Führen Sie die Anweisung aus.

4. Klicken Sie **Als erledigt markieren**.

Ein ausgeführter Provisionierungsvorgang verschwindet aus der Ansicht **Offene Cloud Operationen**.

Einsehen und Bearbeiten von Provisionierungsvorgängen

Als Administrator können Sie alle Provisionierungsvorgänge einsehen. Das heißt, Sie sehen offene und geschlossene Vorgänge. Offene Vorgänge können Sie bearbeiten. Fehlgeschlagene Provisionierungsvorgänge können nicht bearbeitet werden. Weitere Informationen finden Sie unter [Bearbeiten von offenen Provisionierungsvorgängen](#) auf Seite 72.

Um Provisionierungsvorgänge einzusehen

1. Öffnen Sie das Menü **Cloud Operationen**.

Offene und geschlossene Provisionierungsvorgänge werden absteigend nach Eingangsdatum sortiert angezeigt.

2. Nehmen Sie eine der folgenden Aktionen vor:

- a. Markieren Sie den offenen Vorgang und führen Sie die Anweisung aus. Klicken Sie auf **Als erledigt markieren**.
- b. Markieren Sie den Vorgang und sehen Sie sich die relevanten Informationen in den Detailinformationen an.

Um sich nur offene Provisionierungsvorgänge anzusehen

1. Öffnen Sie das Menü **Offene Cloud Operationen**.

2. Bearbeiten Sie den Vorgang und klicken Sie **Als erledigt markieren**.

Die bearbeiteten Vorgänge werden in die Ansicht **Cloud Operationen** verschoben.

Einsehen von allen Provisionierungsvorgängen

Als Auditor können Sie alle Provisionierungsvorgänge im Web Portal einsehen. Das heißt, Sie können geschlossene und offene Provisionierungsvorgänge einsehen. Offene Provisionierungsvorgänge können Sie nicht bearbeiten.

Um Provisionierungsvorgänge einzusehen

1. Öffnen Sie das Menü **Cloud Operationen**.
Offene und geschlossene Provisionierungsvorgänge werden absteigend nach Eingangsdatum sortiert angezeigt.
2. Markieren Sie den Vorgang und sehen Sie sich die relevanten Informationen in den Detailinformationen an.

Einsehen von Statistiken

Statistiken zu Provisionierungsvorgängen werden auf der Startseite des Web Portals angezeigt und sind für den Adminitstrator, Operator und Auditor sichtbar. In der Statistik wird die Anzahl der offenen Provisionierungsvorgänge in einem Zeitverlauf angezeigt. Der Zeitverlauf besteht aus Punkten, die jeweils ein Datum repräsentieren und angeklickt werden können. Wenn Sie die Maus über einen Punkt im Zeitverlauf bewegen, wird ein kleiner Text angezeigt, der Informationen zu den offenen Vorgängen an diesem Tag liefert.

Um sich die Statistiken anzusehen

1. Doppelklicken Sie in der grafischen Darstellung auf einen Punkt im Zeitverlauf.
Ein Fenster mit einer vergrößerten grafischen Darstellung wird angezeigt. Die Daten zu den einzelnen Punkten im Zeitverlauf sind jetzt sichtbar.
2. Bewegen Sie die Maus an dem Datum über den Punkt, zu dem Sie sich informieren möchten.
Zu dem Datum wird die Anzahl der Vorgänge angezeigt.
3. Lassen Sie sich alle Vorgänge mit Werten chronologisch absteigend anzeigen.
 - a. Klicken Sie auf den Link **Hilfe**.
 - b. Wählen Sie den Tabreiter **Quelldateien anzeigen**.

Zusätzliche Informationen für Experten

Beim Einrichten der Synchronisation mit einer Cloud-Anwendung nutzt der One Identity Manager das SCIM Schema, welches vom Server exportiert wird. Wenn der SCIM Konnektor das Schema nicht ermitteln kann, können Sie ihm die Schemainformationen mittels Überlagerungsdateien übergeben. Die Überlagerungsdateien enthalten eine vollständige Beschreibung des genutzten Schemas. Sie müssen der SCIM Core Schema Spezifikation (RFC 7643) entsprechen.

Um die Synchronisation mit Überlagerungsdateien zu konfigurieren

1. Starten Sie den Synchronization Editor.
2. Aktivieren Sie den Expertenmodus.
3. Erstellen Sie ein initiales Synchronisationsprojekt. Weitere Informationen finden Sie unter [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Cloud-Anwendung](#) auf Seite 17. Es gelten folgende Besonderheiten:
 - a. Auf der Seite **Experteneinstellungen** legen Sie fest, ob Sie zusätzliche Einstellungen vornehmen möchten. Aktivieren Sie **Schemaeinstellungen anzeigen**.
 - b. Auf der Seite **Schemadefinition (manuell)** geben Sie den Pfad zu den Überlagerungsdateien an. Beide Dateien müssen vorhanden sein.

Tabelle 33: Informationen zu den Überlagerungsdateien

| Eigenschaft | Beschreibung |
|--|--|
| Schemaüberlagerungsdatei | Enthält die vollständige Schemadefinition der Cloud-Anwendung. |
| Ressourcenkonfiguration-Überlagerungsdatei | Enthält die vollständige Ressourcendefinition der Cloud-Anwendung. |

- Um die Überlagerungsdateien auf Fehler zu überprüfen, klicken Sie **Prüfen**.

HINWEIS: Wenn in der Synchronisationskonfiguration Überlagerungsdateien angegeben sind, ersetzen diese eine auf dem Server vorhandene Schemadefinition.

Die Schemadefinitionen aus den Überlagerungsdateien werden als Verbindungsparameter (DPRSystemConnection.ConnectionParameter) gespeichert.

Änderungen am SCIM Schema müssen in den Überlagerungsdateien gepflegt werden. Geänderte Überlagerungsdateien müssen erneut in das Synchronisationsprojekt eingelesen werden.

Um Schemaänderungen in das Synchronisationsprojekt zu übernehmen

1. Aktualisieren Sie die Schemadefinition in den Überlagerungsdateien.
2. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
3. Aktivieren Sie den Expertenmodus.
4. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.
5. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Verbindung bearbeiten...**
Der Systemverbindungsassistent wird gestartet.
6. Auf der Seite **Schemadefinition (manuell)** geben Sie den Pfad zu den Überlagerungsdateien an.
7. Beenden Sie den Systemverbindungsassistenten.
Die Verbindungsparameter werden aktualisiert.
8. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
9. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
10. Speichern Sie die Änderungen.

Wenn, beispielsweise durch nachträgliche Anpassungen, der Server eine gültige Schemadefinition bereitstellt, muss die Schemadefinition der Überlagerungsdateien aus den Verbindungsparametern entfernt werden.

Um das Schema der Überlagerungsdateien zu entfernen und die Schemadefinition des Servers zu verwenden

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Aktivieren Sie den Expertenmodus.
3. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.
4. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Verbindung bearbeiten...**
Der Systemverbindungsassistent wird gestartet.
5. Wählen Sie die Seite **Endpunkt Konfiguration** und erfassen Sie die URIs zu den SCIM-Endpunkten. Wenn keine URIs angegeben sind, wird das SCIM Basisschema verwendet.
6. Wählen Sie die Seite **Schemadefinition (manuell)** und klicken Sie **Vorhandene entfernen**, sowohl für die Schemaüberlagerungsdatei als auch für die Ressourcenkonfiguration-Überlagerungsdatei.
7. Beenden Sie den Systemverbindungsassistenten.
8. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.

9. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
10. Speichern Sie die Änderungen.

Standardprojektvorlage für Cloud-Anwendungen

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 34: Abbildung der SCIM Schematypen auf Tabellen im One Identity Manager Schema

| SCIM Schematyp | Tabelle im One Identity Manager Schema |
|-----------------------|---|
| Group | UCIGroup |
| User | UCIUser |

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

A

- Administrator 9, 38
- Anstehende Änderung 66-67
 - Aufbewahrungszeitraum 68
- Anwendungsrolle 9
 - Administrator 38
 - Auditor 41
 - Operator 39
- Auditor 9, 41, 69

B

- Benutzerkonto 53
 - Kontomanager 55
 - zugewiesene
 - Berechtigungselemente 57
 - zugewiesene Gruppen 57
- Berechtigungselement 63
 - Berechtigungstyp 63
 - zugewiesene Benutzerkonten 65
 - zugewiesene Gruppen 65

C

- Cloud-Anwendung 47
 - alternative Spaltenbezeichnung 49
 - Benutzer 9
 - Benutzerkonto löschen 47
 - manuelle Provisionierung 47
 - Operator 47
- Container 51
 - Kontomanager 51
 - Operator 51

E

- Einzelobjektsynchronisation
 - beschleunigen 34

G

- Gruppe 59
 - Container 59
 - Gruppentyp 59
 - Kontomanager 59
 - zugewiesene Benutzerkonten 61
 - Zugewiesene
 - Berechtigungslemente 62
 - zugewiesene Gruppen 61

J

- Jobserver
 - Eigenschaften 43
 - Lastverteilung 34

K

- Kontomanager 55

L

- Lastverteilung 34
- Lokaler Cache 17

M

Mitgliedschaft

Änderung provisionieren 32

O

Operator 9, 39, 69

P

Projektvorlage 78

Provisionierung 66

beschleunigen 34

manuell 69

Mitgliederliste 32

Provisionierungsvorgang 69

anzeigen 67

fehlgeschlagen 67

löschen 68

offen 67

R

Ressourcenkonfiguration 75

Revisionsfilter 31

S

Schema

aktualisieren 30

Änderungen 30

komprimieren 30

Schemadefinition 75

Serverfunktion 45

Synchronisation

Benutzer 12

Berechtigungen 12

beschleunigen 31

Cache nutzen 17

einrichten 12

konfigurieren 17, 28

nur Änderungen 31

Scope 28

starten 17

Synchronisationsprojekt

erstellen 17

Verbindungsparameter 17, 28

verhindern 35

Workflow 17, 30

Synchronisationsanalysebericht 35

Synchronisationskonfiguration

anpassen 28, 30

Synchronisationsprojekt

bearbeiten 49

deaktivieren 35

erstellen 17

Projektvorlage 78

Synchronisationsprotokoll 27

Synchronisationsrichtung

In das Zielsystem 17, 30

In den One Identity Manager 17

Synchronisationsserver 42

installieren 14

konfigurieren 14

Serverfunktion 45

Synchronisationsworkflow

erstellen 17, 30

U

Überlagerungsdatei 75

Z

Zeitplan

deaktivieren 35