One Identity Manager 9.2

Administrationshandbuch für die Integration mit OneLogin Cloud Directory

Legende

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

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

One Identity Manager Administrationshandbuch für die Integration mit OneLogin Cloud Directory
Aktualisiert - 29. September 2023, 04:54 Uhr

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

Inhalt

Integration mit OneLogin Cloud Directory

Der One Identity Manager bietet eine vereinfachte Administration der Benutzerkonten des OneLogin Cloud Directory durch Synchronisierung mit den OneLogin Domänen der Kunden. Der One Identity Manager konzentriert sich auf die Einrichtung und Bearbeitung von Benutzerkonten und die Versorgung mit den benötigten Berechtigungen für den Zugriff auf Anwendungen und für die Authentifizierung und Autorisierung.

Um die Benutzer mit den benötigten Berechtigungen auszustatten, werden OneLogin Rollen und OneLogin Anwendungen im One Identity Manager abgebildet. Damit ist es möglich, die Identity und Access Governance Prozesse wie Attestierung, Identity Audit, Management von Benutzerkonten und Systemberechtigungen, IT Shop oder Berichtsabonnements für OneLogin Domänen zu nutzen.

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

Durch die Datensynchronisation werden zusätzliche Informationen zu den OneLogin Domänen in die One Identity Manager-Datenbank eingelesen. Aufgrund der komplexen Zusammenhänge und weitreichenden Auswirkungen von Änderungen ist die Anpassung dieser Informationen im One Identity Manager nur in geringem Maße möglich.

Ausführliche Informationen zu OneLogin erhalten Sie in der OneLogin Dokumentation.

HINWEIS: Voraussetzung für die Verwaltung von OneLogin Domänen im One Identity Manager ist die Installation des OneLogin Moduls. Ausführliche Informationen zur Installation finden Sie im *One Identity Manager Installationshandbuch.*

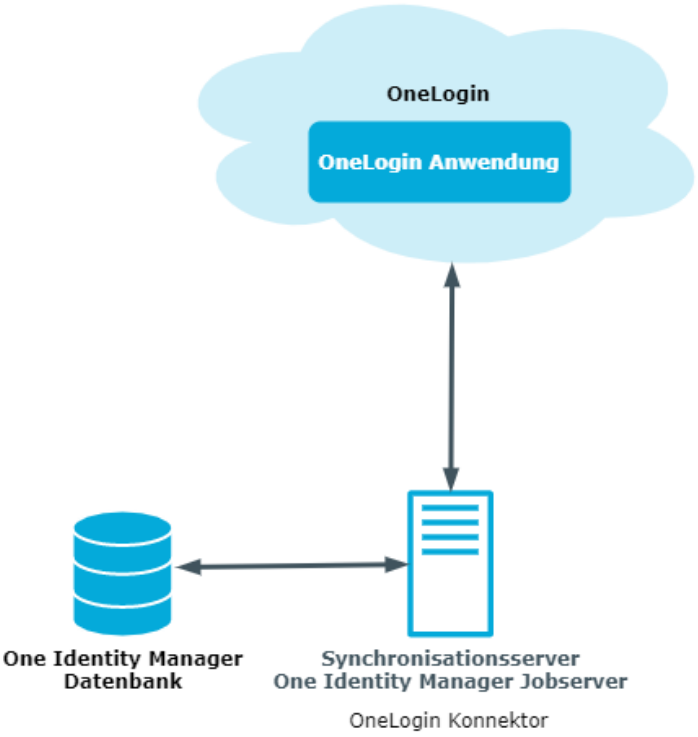
Architekturüberblick

Um auf die Daten einer OneLogin Domäne zuzugreifen, wird auf einem Synchronisationsserver der OneLogin Konnektor installiert. Der Synchronisationsserver sorgt für den Abgleich der Daten zwischen der One Identity Manager-Datenbank und

OneLogin. Der OneLogin Konnektor ist Bestandteil des OneLogin Moduls. Der Zugriff auf die OneLogin Daten erfolgt über die OneLogin API.

HINWEIS: Unter Umständen werden bestimmte Endpunkte der OneLogin API nur auf Nachfrage beim Support aktiviert. Ausführliche Informationen zur OneLogin API finden Sie unter https://developers.onelogin.com/api-docs/1/getting-started/dev-overview und https://developers.onelogin.com/api-docs/2/getting-started/dev-overview.

Abbildung 1: Architektur für die Synchronisation



One Identity Manager Benutzer für die Verwaltung einer OneLogin Domäne

In die Einrichtung und Verwaltung einer OneLogin Domäne sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein.

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

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

Benutzer	Aufgaben
	Benutzer mit dieser Anwendungsrolle: • Weisen Systemberechtigungen an Geschäftsrollen zu.

Konfigurationsparameter für die Verwaltung von OneLogin-Umgebungen

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

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

Weitere Informationen finden Sie unter Konfigurationsparameter für die Verwaltung von OneLogin Domänen auf Seite 168.

2

Synchronisieren einer OneLogin Domäne

Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und OneLogin sorgt der One Identity Manager Service.

Informieren Sie sich hier:

- wie Sie die Synchronisation einrichten, um initial Daten aus einer OneLogin Domäne in die One Identity Manager-Datenbank einzulesen,
- wie Sie eine Synchronisationskonfiguration anpassen, beispielsweise um verschiedene OneLogin Domänen mit ein und demselben Synchronisationsprojekt zu synchronisieren,
- wie Sie die Synchronisation starten und deaktivieren,
- wie Sie die Synchronisationsergebnisse auswerten.

TIPP: Bevor Sie die Synchronisation mit einer OneLogin Domäne einrichten, machen Sie sich mit dem Synchronization Editor vertraut. Ausführliche Informationen über dieses Werkzeug finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Einrichten der Initialsynchronisation mit einer OneLogin Domäne auf Seite 14
- Anpassen der Synchronisationskonfiguration auf Seite 30
- Ausführen einer Synchronisation auf Seite 41
- Aufgaben nach einer Synchronisation auf Seite 44
- Fehleranalyse auf Seite 48

Einrichten der Initialsynchronisation mit einer OneLogin Domäne

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

Um die Objekte einer OneLogin Domäne initial in die One Identity Manager-Datenbank einzulesen

1. Stellen Sie in der OneLogin Domäne ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von OneLogin Domänen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | OneLogin** aktiviert ist.
    - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.

      HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
    - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Verwandte Themen

- Benutzer und Berechtigungen für die Synchronisation mit einer OneLogin Domäne auf Seite 15
- Einrichten eines Synchronisationsservers für OneLogin Domänen auf Seite 16
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer OneLogin Domäne auf Seite 20

- Konfigurationsparameter für die Verwaltung von OneLogin Domänen auf Seite 168
- Standardprojektvorlage für OneLogin Domänen auf Seite 171

Benutzer und Berechtigungen für die Synchronisation mit einer OneLogin Domäne

Bei der Synchronisation mit einer OneLogin Domäne spielen folgende Benutzer eine Rolle.

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Sicherheitstoken oder Benutzer für den Zugriff auf die OneLogin Domäne	Base64-kodierter Sicherheitstoken oder eine Kombination aus Benutzername und Kennwort. Für ausreichende Berechtigungen wird der Scope **Manage All** vorausgesetzt.
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Berechtigungen für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Berechtigungen für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter:

Benutzer	Berechtigungen
	• `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen)
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

Einrichten eines Synchronisationsservers für OneLogin Domänen

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

Auf dem Synchronisationsserver muss der One Identity Manager Service mit der Maschinenrolle **OneLogin** installiert sein. Die Maschinenrolle **OneLogin** enthält den OneLogin Konnektor. Der OneLogin Konnektor wird für die Synchronisation und Provisionierung der Objekte der OneLogin Domänen eingesetzt.

Detaillierte Informationen zum Thema

- Systemvoraussetzungen für den OneLogin Synchronisationsserver auf Seite 16
- One Identity Manager Service mit OneLogin Konnektor installieren auf Seite 17

Systemvoraussetzungen für den OneLogin Synchronisationsserver

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

- Windows Betriebssystem

  Unterstützt werden die Versionen:

  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016

- Windows Server 2012 R2
- Windows Server 2012

- Microsoft .NET Framework Version 4.8 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.

One Identity Manager Service mit OneLogin Konnektor installieren

Auf dem Synchronisationsserver wird der One Identity Manager Service mit der Maschinenrolle **OneLogin** installiert. Die Maschinenrolle **OneLogin** enthält den OneLogin Konnektor. Der OneLogin Konnektor wird für die Synchronisation und Provisionierung der Objekte der OneLogin Domänen eingesetzt.

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

Tabelle 3: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	OneLogin Konnektor
Maschinenrolle	Server | Job Server | OneLogin

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

Um einen Jobserver einzurichten, führen Sie folgende Schritte aus.

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

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

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

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

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

2. Wenn Sie mit einer verschlüsselten One Identity Manager-Datenbank arbeiten, geben Sie dem One Identity Manager Service den Datenbankschlüssel bekannt. Ausführliche Informationen zum Arbeiten mit einer verschlüsselten One Identity Manager-Datenbank finden Sie im *One Identity Manager Installationshandbuch*.
3. Für die Generierung von Prozessen für die Jobserver werden der Provider, Verbindungsparameter und die Authentifizierungsdaten benötigt. Diese Informationen werden im Standardfall aus den Verbindungsdaten der Datenbank ermittelt. Arbeitet der Jobserver über einen Anwendungsserver müssen Sie zusätzliche Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Erfassen der Verbindungsinformationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

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

1. Starten Sie das Programm Server Installer.

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

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

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

3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.
   a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.

      - ODER -

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

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

- **Vollständiger Servername**: Vollständiger Servername gemäß DNS-Syntax.

  Syntax:

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

HINWEIS: Über die Option **Erweitert** können Sie weitere Eigenschaften für den Jobserver bearbeiten. Sie können die Eigenschaften auch zu einem späteren Zeitpunkt mit dem Designer bearbeiten.

4. Auf der Seite **Maschinenrollen** wählen Sie **OneLogin**.
5. Auf der Seite **Serverfunktionen** wählen Sie **OneLogin Konnektor**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

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

   Für eine direkte Verbindung zu Datenbank:

   a. Wählen Sie in der Modulliste **Prozessabholung > sqlprovider**.
   b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
   c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
   d. Klicken Sie **OK**.

   Für eine Verbindung zum Anwendungsserver:

   a. Wählen Sie in der Modulliste den Eintrag **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen**.
   b. Wählen Sie **AppServerJobProvider** und klicken Sie **OK**.
   c. Wählen Sie in der Modulliste **Prozessabholung > AppServerJobProvider**.
   d. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
   e. Erfassen Sie die Adresse (URL) zum Anwendungsserver und klicken Sie **OK**.
   f. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
   g. Wählen Sie unter **Authentifizierungsverfahren** das Authentifizierungsmodul für die Anmeldung. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager-Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
   h. Klicken Sie **OK**.
7. Zur Konfiguration der Installation, klicken Sie **Weiter**.

8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Wählen Sie den Server über die Auswahlliste oder erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.

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

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

    Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.
11. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

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

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

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer OneLogin Domäne

HINWEIS: Unter Umständen werden bestimmte Endpunkte der OneLogin API nur auf Nachfrage beim Support aktiviert. Ausführliche Informationen zur OneLogin API finden Sie unter https://developers.onelogin.com/api-docs/1/getting-started/dev-overview und https://developers.onelogin.com/api-docs/2/getting-started/dev-overview.

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und einer OneLogin Domäne 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.

Ausführliche Informationen zur Einrichtung der Synchronisation finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Detaillierte Informationen zum Thema

- Benötigte Informationen für die Erstellung eines Synchronisationsprojektes auf Seite 21
- Initiales Synchronisationsprojekt für eine OneLogin Domäne erstellen auf Seite 24
- Synchronisationsprojekt für OneLogin Privilegien anpassen auf Seite 31
- Standardprojektvorlage für OneLogin Domänen auf Seite 171
- Einstellungen des OneLogin Konnektors auf Seite 175

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

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

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Domäne	Vollständiger Name der OneLogin Domäne. Beispiel: <your domain>.onelogin.com
URI der API	URI , unter welchem die API erreichbar ist. Es wird nur der Teil der URL benötigt, der von allen aufzurufenden Endpunkten gemeinsam verwendet wird. Wenn die komplette URL https://my-identities.onelogin.com/api/2 lautet, dann ist hier als URI **api** einzugeben. Der Versionsanteil und der Objekttypen-Anteil wird in der Ressourcenkonfiguration angegeben.
Authentifizierungsendpunkt	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, wird die

Angaben	Erläuterungen
	vollständige URL benötigt. Wenn der komplette URI https://my-identities.onelogin.com/api/auth/oauth2/token lautet, dann ist hier **auth/oauth2/token** einzugeben. Wenn die Basis-URL oder der Server verschieden zur Ressourcen-URL ist, dann ist hier die komplette URL anzugeben, beispielsweise **https://api.us.onelogin.com/auth/oauth2/v2/token**.
Sicherheitstoken oder Benutzerkonto und Kennwort zur Anmeldung	Base64-kodierter Sicherheitstoken oder eine Kombination aus Benutzername und Kennwort für die Anmeldung. Das Sicherheitstoken erhalten Sie bei der Registrierung Ihrer Anwendung bei OneLogin. Ausführliche Informationen zu OneLogin erhalten Sie in der OneLogin Dokumentation. Sind beide Anmeldeinformationen vorhanden, wird vorzugsweise der Sicherheitstoken verwendet.
Applikations-/Client-ID	Client-ID für die Anwendung. Die Client-ID erhalten Sie bei der Registrierung Ihrer Anwendung bei OneLogin. Ausführliche Informationen zu OneLogin erhalten Sie in der OneLogin Dokumentation.
Synchronisationsserver für die OneLogin Domäne	Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem OneLogin Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. • Serverfunktion: **OneLogin Konnektor** • Maschinenrolle: **Server | Job Server | OneLogin**
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Name der Datenbank • SQL Server-Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung

Angaben	Erläuterungen
	verwendet wird Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
Remoteverbindungsserver	Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen. Konfiguration des Remoteverbindungsservers: • One Identity Manager Service ist gestartet • **RemoteConnectPlugin** ist installiert 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*.

Verwandte Themen

- Benutzer und Berechtigungen für die Synchronisation mit einer OneLogin Domäne auf Seite 15
- Einrichten eines Synchronisationsservers für OneLogin Domänen auf Seite 16

Initiales Synchronisationsprojekt für eine OneLogin Domäne erstellen

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

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

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

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

Um ein initiales Synchronisationsprojekt für ein OneLogin-basiertes Zielsystem 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 OneLogin** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors wird gestartet.

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

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

5. Auf der Seite **Verbindungsdaten** erfassen Sie Verbindungsinformationen zur Anmeldung an der OneLogin Domäne.
   - **OneLogin Domäne**: Erfassen Sie den vollständiger Namen der OneLogin Domäne, beispielsweise **<your domain>.onelogin.com**.
   - **URI der API ohne Version**: Erfassen Sie den URI, unter welchem die API erreichbar ist. Es wird nur der Teil der URL benötigt, der von allen aufzurufenden Endpunkten gemeinsam verwendet wird.

Wenn die komplette URL https://my-identities.onelogin.com/api/2 lautet, dann ist hier als URI **api** einzugeben. Der Versionsanteil und der Objekttypen-Anteil wird in der Ressourcenkonfiguration angegeben.

- **Authentifizierungsendpunkt/URL**: Erfassen Sie den 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.

  Wenn der komplette URI https://my-identities.onelogin.com/api/auth/oauth2/token lautet, dann ist hier **auth/oauth2/token** einzugeben. Wenn die Basis-URL oder der Server verschieden zur Ressourcen-URL ist, dann ist hier die komplette URL anzugeben, beispielsweise **https://api.us.onelogin.com/auth/oauth2/v2/token**.

6. Auf der Seite **OAuth-Authentifizierung** geben Sie die Anmeldedaten an und wählen Sie den Zugangstyp.
   - **Sicherheitstoken**: Sicherheitstoken für die Anmeldung. Wenn der Sicherheitstoken nicht bekannt ist, erfassen Sie Benutzername und Kennwort.
   - **Benutzername** und **Kennwort**: Benutzername und Kennwort für die Anmeldung, wenn der Sicherheitstoken nicht bekannt ist.
   - **Applikations-/Client-ID**: Erfassen Sie die Client-ID, mit der die Anwendung bei OneLogin registriert ist.
   - **Zugangstyp**: Wählen Sie den Zugangstyp für die Anmeldung. Aktivieren Sie **Client-Berechtigung** oder **Kennwort-Berechtigung**.
   - **Scope**: (Optional) Erfassen Sie die Scope-Parameter, die für die Anmeldung am Zielsystem gültig ist. Wenn mehrere Parameter gültig sind, trennen Sie diese durch Leerzeichen.
7. Auf der Seite **Verbindungseinstellungen prüfen** können Sie die erfassten Verbindungsdaten testen. Klicken Sie **Test**.

   Der One Identity Manager versucht eine Verbindung zur OneLogin Domäne 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.
8. Auf der Seite **Optimierungen** können Sie zusätzliche Einstellungen zur Optimierung der Synchronisationsperformance vornehmen.
   - **Lokalen Cache verwenden**: Legen Sie fest, ob der lokale Cache des OneLogin Konnektors genutzt werden soll.

     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.

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.

- **Max. Anzahl paralleler Anfragen**: Anzahl der Datenanfragen am Zielsystem, die maximal gleichzeitig ausgeführt werden können. Erfassen Sie einen Wert zwischen **1** und **32**.
- **HTTP Keep-Alive nutzen**: Legen Sie fest , ob HTTP-Verbindungen aufrecht erhalten werden sollen. Wenn die Option deaktiviert ist, werden Verbindungen sofort geschlossen und können nicht für weitere Anfragen genutzt werden.

9. Auf der Seite **Anzeigename** erfassen Sie einen eindeutigen Anzeigenamen.

   Über den Anzeigenamen können Sie verschiedene Verbindungskonfigurationen für die OneLogin REST-API unterscheiden.

10. Auf der letzten Seite des Systemverbindungsassistenten können Sie die Verbindungsdaten lokal speichern und die Konfiguration der Systemverbindung abschließen.
    - Aktivieren Sie die Option **Verbindung lokal speichern**, um die Verbindungsdaten zu speichern. Diese können Sie bei der Einrichtung weiterer Synchronisationsprojekte nutzen.
    - Um den Systemverbindungsassistenten zu beenden und zum Projektassistenten zurückzukehren, klicken Sie **Fertig**.

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 Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.

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

Tabelle 5: Zielsystemzugriff festlegen

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

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

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

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

    a. Klicken Sie , um einen neuen Jobserver anzulegen.

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

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

    c. Klicken Sie **OK**.

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

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

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

    Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

    HINWEIS:

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

      Bevor Sie das Synchronisationsprojekt nutzen, prüfen Sie die Fehler. In der Ansicht **Allgemein** auf der Startseite des Synchronization Editor klicken Sie dafür **Projekt prüfen**.
    - Wenn das Synchronisationsprojekt nicht sofort aktiviert werden soll, deaktivieren Sie die Option **Synchronisationsprojekt speichern und sofort aktivieren**. In diesem Fall speichern Sie das Synchronisationsprojekt manuell vor dem Beenden des Synchronization Editor.

Verwandte Themen

- Benötigte Informationen für die Erstellung eines Synchronisationsprojektes auf Seite 21
- Benutzer und Berechtigungen für die Synchronisation mit einer OneLogin Domäne auf Seite 15
- Einrichten eines Synchronisationsservers für OneLogin Domänen auf Seite 16
- Synchronisationsprotokoll konfigurieren auf Seite 28
- Anpassen der Synchronisationskonfiguration auf Seite 30
- Synchronisationsprojekt für OneLogin Privilegien anpassen auf Seite 31
- Aufgaben nach einer Synchronisation auf Seite 44
- Standardprojektvorlage für OneLogin Domänen auf Seite 171
- Einstellungen des OneLogin Konnektors auf Seite 175

Synchronisationsprotokoll konfigurieren

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

Um den Inhalt des Synchronisationsprotokolls für eine Systemverbindung zu konfigurieren

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

   - ODER -

   Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie im Synchronization Editor die Kategorie **Konfiguration > One Identity Manager Verbindung**.
2. Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren**.
3. Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.
4. Aktivieren Sie die zu protokollierenden Daten.

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

Um den Inhalt des Synchronisationsprotokolls für einen Synchronisationsworkflow zu konfigurieren

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

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

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 43

Anpassen der Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation einer OneLogin Domäne eingerichtet. Mit diesem Synchronisationsprojekt können Sie OneLogin Objekte in die One Identity Manager-Datenbank einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in die OneLogin Domäne provisioniert.

Um die Datenbank und die OneLogin Domäne regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als primäres System zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um allgemeingültige Synchronisationskonfigurationen zu erstellen, die erst beim Start der Synchronisation die notwendigen Informationen über die zu synchronisierenden Objekte erhalten, können Variablen eingesetzt werden. Variablen können beispielsweise in den Basisobjekten, den Schemaklassen oder den Verarbeitungsmethoden eingesetzt werden.
- Mit Hilfe von Variablen kann ein Synchronisationsprojekt für die Synchronisation verschiedener Domäne eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an der Domäne als Variablen.
- Um festzulegen, welche OneLogin Objekte und Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschema geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.

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

Detaillierte Informationen zum Thema

- Synchronisationsprojekt für OneLogin Privilegien anpassen auf Seite 31
- Synchronisation in die OneLogin Domäne konfigurieren auf Seite 31
- Synchronisation verschiedener OneLogin Domänen konfigurieren auf Seite 32
- Einstellungen der Systemverbindung zur OneLogin Domäne ändern auf Seite 33
- Schema aktualisieren auf Seite 35

- Beschleunigung der Synchronisation auf Seite 37
- Einzelobjektsynchronisation konfigurieren auf Seite 38
- Beschleunigung der Provisionierung und Einzelobjektsynchronisation auf Seite 39

Synchronisationsprojekt für OneLogin Privilegien anpassen

Die Synchronisation von OneLogin Privilegien ist im Standard deaktiviert. Um die Privilegien zu synchronisieren, muss das Synchronisationsprojekt angepasst werden.

- Aktivieren Sie im Workflow **Initial Synchronization** die Synchronisationsschritt **Privilege** und **UserPrivilege**.
- Aktivieren Sie im Workflow **Provisioning** den Synchronisationsschritt **UserPrivilege**.

Um Synchronisationsschritte zu aktivieren

1. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
2. Wählen Sie die Kategorie **Workflows**.
3. Wählen Sie in der Navigationsansicht einen Workflow.
4. Klicken Sie in der Symbolleiste der Workflowansicht .
5. Entfernen Sie die Option **Deaktivieren** für Synchronisationsschritte, die aktiviert werden sollen.
6. Klicken Sie **OK**.

Verwandte Themen

- OneLogin Privilegien auf Seite 151

Synchronisation in die OneLogin Domäne konfigurieren

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

Um eine Synchronisationskonfiguration für die Synchronisation in die OneLogin Domäne zu erstellen

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

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

Detaillierte Informationen zum Thema

- Synchronisation verschiedener OneLogin Domänen konfigurieren auf Seite 32

Synchronisation verschiedener OneLogin Domänen konfigurieren

Unter bestimmten Voraussetzungen ist es möglich ein Synchronisationsprojekt für die Synchronisation verschiedener OneLogin Domänen zu nutzen.

Voraussetzungen

- Die Zielsystemschemas beider Domänen sind identisch.
- Alle virtuellen Schemaeigenschaften, die im Mapping genutzt werden, müssen in den erweiterten Schemas beider Domänen vorhanden sein.

Um ein Synchronisationsprojekt für die Synchronisation einer weiteren Domäne anzupassen

1. Stellen Sie in der weiteren Domäne ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Öffnen Sie im Synchronization Editor das Synchronisationsprojekt.
3. Erstellen Sie für jede weitere Domäne ein neues Basisobjekt.
   - Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
   - Wählen Sie im Assistenten den OneLogin Konnektor.
   - Geben Sie die Verbindungsparameter bekannt. Die Verbindungsparameter werden in einem spezialisierten Variablenset gespeichert.

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

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

Verwandte Themen

- Synchronisation in die OneLogin Domäne konfigurieren auf Seite 31

Einstellungen der Systemverbindung zur OneLogin Domäne ändern

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

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

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

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

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

Detaillierte Informationen zum Thema

- Verbindungsparameter im Variablenset bearbeiten auf Seite 33
- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 35
- Einstellungen des OneLogin Konnektors auf Seite 175

Verbindungsparameter im Variablenset bearbeiten

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

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

Um die Verbindungsparameter in einem spezialisierten Variablenset anzupassen

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

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

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

    - ODER -

    Klicken Sie , um ein neues Basisobjekt anzulegen.
14. Ordnen Sie im Eingabefeld **Variablenset** das spezialisierte Variablenset zu.
15. Speichern Sie die Änderungen.

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

Verwandte Themen

- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 35

Eigenschaften der Zielsystemverbindung bearbeiten

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

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

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

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

Um die Verbindungsparameter mit dem Systemverbindungsassistenten zu bearbeiten

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

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

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

Verwandte Themen

- Verbindungsparameter im Variablenset bearbeiten auf Seite 33

Schema aktualisieren

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

einem späteren Zeitpunkt wieder in die Synchronisationskonfiguration aufgenommen werden.

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

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

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

Um das Schema einer Systemverbindung zu aktualisieren

1. Wählen Sie die Kategorie **Konfiguration > Zielsystem**.

   - ODER -

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

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

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

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

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

Beschleunigung der Synchronisation

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 OneLogin Konnektor unterstützt die Revisionsfilterung. Als Revisionszähler wird das Änderungsdatum der OneLogin-Objekte aus der OneLogin Änderungshistorie verwendet (Tabelle `OLGEvent`).

Um die Synchronisation zu beschleunigen und die Menge der synchronisierten Einträge in der Änderungshistorie zu verringern, können Sie den Scope für den Schematyp `Event` in Ihrem Synchronisationsprojekt anpassen.

HINWEIS: Um Behavior Driven Governance zu nutzen, müssen jedoch die Ereignisse mit den Typen **5**, **6**, **7**, **8**, **11**, **22**, **29** synchronisiert werden. Ausführliche Informationen zu Behavior Driven Governance finden Sie im *One Identity Manager Administrationshandbuch für Behavior Driven Governance*.

Um den Scope anzupassen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. In der Navigationsansicht wählen Sie **Konfiguration > Zielsystem**.
3. Wählen Sie die Ansicht **Scope**.
4. Klicken Sie **Scope bearbeiten**.
5. Wählen Sie den Schematyp **Event**.
6. Wählen Sie den Tabreiter Systemfilter und erweitern Sie die vorhandene Filterdefinition folgendermaßen:

   ```
   event_type_id=5,6,7,8,11,22,29&since=$olgeventsincefilter$
   ```

7. Speichern Sie die Änderungen.

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 OneLogin-Objekte mit der in der One Identity Manager-Datenbank gespeicherten Revision verglichen. Es werden nur noch die Objekte aus der OneLogin Domäne gelesen, die sich seit diesem Datum verändert haben.

Die optimierte Revisionsfilterung wird unterstützt, da OneLogin über ein eventbasiertes Logging verfügt. Damit ist es möglich, die Information zur letzten Änderung eines Schematyps abzufragen. Wenn die Objekte eines Schematyps weder neu eingefügt noch geändert wurden, kann der Synchronisationsschritt komplett ausgelassen werden. Es müssen keine Objekte für den Abgleich geladen werden. Der OneLogin Konnektor stellt die entsprechenden Informationen bereit.

Um die optimierte Revisionsfilterung zu nutzen

- Aktivieren Sie im Designer den Konfigurationsparameter **Common | TableRevision**.

  Bei jeder Änderung in einer Tabelle wird nun das Revisionsdatum für diese Tabelle aktualisiert. Diese Informationen werden in der Tabelle `QBMTableRevision`, Spalte `RevisionDate` gespeichert. So erkennt One Identity Manager, ob in einer Tabelle Objekte hinzugefügt, geändert oder gelöscht wurden.

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

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

Um die Revisionsfilterung an einem Workflow zuzulassen

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

Um die Revisionsfilterung an einer Startkonfiguration zuzulassen

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

HINWEIS: Wenn der Konfigurationsparameter **Common | TableRevision** deaktiviert wird, werden alle Revisionsdaten in der Tabelle `QBMTableRevision` gelöscht.

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

Einzelobjektsynchronisation konfigurieren

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

Voraussetzungen

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

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

Um den Pfad zum Basisobjekt der Synchronisation für eine Tabelle festzulegen

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **OneLogin**.
3. Wählen Sie die Aufgabe **Synchronisationstabellen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die kundenspezifische Tabelle zu, für die Sie die Einzelobjektsynchronisation nutzen möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifische Tabelle und erfassen Sie den **Pfad zum Basisobjekt**.

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

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

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 44
- Ausstehende Objekte nachbehandeln auf Seite 45

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

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

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

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

Um die Lastverteilung zu konfigurieren

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.
    - Für Jobserver, die an der Lastverteilung teilnehmen, muss die Option **Keine Prozesszuteilung** deaktiviert sein.
    - Weisen Sie diesen Jobservern die Serverfunktion **OneLogin Konnektor** zu.

    Alle Jobserver müssen auf die gleiche OneLogin Domäne zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.
2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

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

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

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

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

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

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Detaillierte Informationen zum Thema

- Jobserver für OneLogin-spezifische Prozessverarbeitung auf Seite 162

Ausführen einer Synchronisation

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

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

Detaillierte Informationen zum Thema

- Synchronisationen starten auf Seite 41
- Synchronisation deaktivieren auf Seite 42
- Synchronisationsergebnisse anzeigen auf Seite 43
- Einzelobjekte synchronisieren auf Seite 44
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 50

Synchronisationen starten

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

Um regelmäßige Synchronisationen auszuführen

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

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

Um die initiale Synchronisation manuell zu starten

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

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

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

Synchronisation deaktivieren

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

Um regelmäßige Synchronisationen zu verhindern

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

   Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer OneLogin Domäne auf Seite 20
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 50

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen

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

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

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

Um das Protokoll einer Provisionierung anzuzeigen

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

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

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

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

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

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 28
- Fehleranalyse auf Seite 48

Einzelobjekte synchronisieren

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

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

Um ein Einzelobjekt zu synchronisieren

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

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

Detaillierte Informationen zum Thema

- Einzelobjektsynchronisation konfigurieren auf Seite 38

Aufgaben nach einer Synchronisation

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

- Ausstehende Objekte nachbehandeln auf Seite 45
- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 47
- OneLogin Benutzerkonten über Kontendefinitionen verwalten auf Seite 47

Ausstehende Objekte nachbehandeln

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

Ausstehende Objekte

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

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

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie im Manager die Kategorie **OneLogin > Zielsystemabgleich: OneLogin**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **OneLogin** als Synchronisationstabellen zugewiesen sind.
2. Öffnen Sie auf dem Formular **Zielsystemabgleich**, in der Spalte **Tabelle/Objekt** den Knoten der Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

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

   - Das Synchronisationsprotokoll wurde bereits gelöscht.

     - ODER -
   - Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.

     Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.
   - Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.

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

   TIPP:

Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

1. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.
2. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.

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

Tabelle 6: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Es wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: • Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen. • Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.
	Zurücksetzen	Die Markierung **Ausstehend** wird für das Objekt entfernt.

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

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

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

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

Um den Fehler zu lokalisieren, muss die Massenverarbeitung der Objekte deaktiviert werden. Die Objekte werden damit nacheinander verarbeitet. Das fehlerhafte Objekt wird

in der Fehlermeldung benannt. Alle Änderungen, die bis zum Auftreten des Fehlers vorgenommen wurden, werden gespeichert.

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularsymbolleiste das Symbol .

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

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

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

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

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

Verwandte Themen

- Ausstehende Objekte nachbehandeln auf Seite 45

OneLogin Benutzerkonten über Kontendefinitionen verwalten

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

verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

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

Um die Benutzerkonten über Kontendefinitionen zu verwalten

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

Verwandte Themen

- Kontendefinitionen für OneLogin Benutzerkonten auf Seite 53

Fehleranalyse

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

- Synchronisation simulieren

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

- Synchronisation analysieren

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

- Meldungen protokollieren

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

- Startinformation zurücksetzen

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

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 43

Datenfehler bei der Synchronisation ignorieren

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

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

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

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

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

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

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

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

Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus)

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

Ob der Offline-Modus für eine Zielsystemverbindung grundsätzlich verfügbar ist, wird am Basisobjekt des jeweiligen Synchronisationsprojekts festgelegt. Sobald ein Zielsystem tatsächlich nicht erreichbar ist, kann diese Zielsystemverbindungen über das Launchpad offline und anschließend wieder online geschaltet werden.

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

Voraussetzungen

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

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

Um den Offline-Modus für ein Basisobjekt zuzulassen

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

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

Die Zahl der nachträglich zu verarbeitenden Prozesse ist abhängig vom Umfang der Änderungen in der One Identity Manager-Datenbank mit Auswirkungen auf das Zielsystem während der Offline-Phase. Um Datenkonsistenz zwischen One Identity Manager-

Datenbank und Zielsystem herzustellen, müssen alle anstehenden Prozesse verarbeitet werden, bevor eine Synchronisation gestartet wird.

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

Um ein Zielsystem als offline zu kennzeichnen

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

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

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

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

Verwandte Themen

- Synchronisation deaktivieren auf Seite 42

Managen von OneLogin Benutzerkonten und Identitäten

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

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

- Identitäten erhalten ihre Benutzerkonten automatisch über Kontendefinitionen.

  Hat eine Identität noch kein Benutzerkonto in einer OneLogin Domäne, wird durch die Zuweisung der Kontendefinition an eine Identität über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

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

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

Verwandte Themen

- Kontendefinitionen für OneLogin Benutzerkonten auf Seite 53
- Automatische Zuordnung von Identitäten zu OneLogin Benutzerkonten auf Seite 76
- Löschverzögerung für OneLogin Benutzerkonten festlegen auf Seite 88
- Stammdaten von OneLogin Benutzerkonten bearbeiten auf Seite 128

Kontendefinitionen für OneLogin Benutzerkonten

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

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

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

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

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

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- Erstellen von Kontendefinitionen
- Konfigurieren der Automatisierungsgrade

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

Detaillierte Informationen zum Thema

- Kontendefinitionen erstellen auf Seite 54
- Kontendefinitionen bearbeiten auf Seite 55
- Stammdaten einer Kontendefinition auf Seite 55
- Automatisierungsgrade bearbeiten auf Seite 58
- Automatisierungsgrade erstellen auf Seite 59
- Stammdaten eines Automatisierungsgrades auf Seite 60
- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 61
- IT Betriebsdaten erfassen auf Seite 63
- IT Betriebsdaten ändern auf Seite 64
- Zuweisen der Kontendefinition an Identitäten auf Seite 65
- Kontendefinitionen an OneLogin Domänen zuweisen auf Seite 73
- Kontendefinitionen löschen auf Seite 73

Kontendefinitionen erstellen

Erstellen Sie eine oder mehrere Kontendefinitionen für das Zielsystem.

Um eine Kontendefinition zu erstellen

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

Detaillierte Informationen zum Thema

- Stammdaten einer Kontendefinition auf Seite 55

Kontendefinitionen bearbeiten

Sie können die Stammdaten der Kontendefinitionen bearbeiten.

Um eine Kontendefinition zu bearbeiten

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Kontendefinition.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten einer Kontendefinition auf Seite 55
- Kontendefinitionen erstellen auf Seite 54
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 59

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 7: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet. Für OneLogin Benutzerkonten wählen Sie **OLGUser**.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Angabe der vorausgesetzten Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch zugeordnet. Für eine OneLogin Domäne lassen Sie die Angabe leer.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.

Eigenschaft	Beschreibung
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Identitäten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Gibt an, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Identitäten und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.
Automatische Zuweisung zu Identitäten	Gibt an, ob die Kontendefinition automatisch an alle internen Identitäten zugewiesen werden soll. Um die Kontendefinition automatisch an alle internen Identitäten zuzuweisen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Identitäten aktivieren**. Die Kontendefinition wird an jede Identität zugewiesen, die nicht als extern markiert ist. Sobald eine neue interne Identität erstellt wird, erhält diese Identität ebenfalls automatisch diese Kontendefinition. Um die automatische Zuweisung der Kontendefinition von allen Identitäten zu entfernen, verwenden Sie die Aufgabe **Automatische Zuweisung zu Identitäten deaktivieren**. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Identitäten zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.

Eigenschaft	Beschreibung
	Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei verzögertem Löschen beibehalten	Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei Sicherheitsgefährdung beibehalten	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Identitäten. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: (Standard) Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Ressourcentyp	Ressourcentyp zur Gruppierung von Kontendefinitionen.
Freies Feld 01- Freies Feld 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.
Rollen erbbar	Gibt an, ob das Benutzerkonto OneLogin Rollen über die verbundene Identität erben darf. Ist die Option aktiviert, werden die Rollen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.

Automatisierungsgrade bearbeiten

One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

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

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

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

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

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

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

Verwandte Themen

- Stammdaten eines Automatisierungsgrades auf Seite 60
- Automatisierungsgrade erstellen auf Seite 59
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 59

Automatisierungsgrade erstellen

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

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

Um einen Automatisierungsgrad zu erstellen

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

Verwandte Themen

- Stammdaten eines Automatisierungsgrades auf Seite 60
- Kontendefinitionen bearbeiten auf Seite 55
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 59

Automatisierungsgrade an Kontendefinitionen zuweisen

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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 8: Stammdaten eines Automatisierungsgrades

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

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

Abbildungsvorschriften für IT Betriebsdaten erstellen

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

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

- Rollen erbbar
- Identität
- Privilegiertes Benutzerkonto
- Lizenzierungsstatus
- OneLogin Gruppe

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Abbildungsvorschrift bearbeiten.**
4. Klicken Sie **Hinzufügen** und erfassen Sie folgende Informationen.
    - **Spalte**: Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
    - **Quelle**: Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen:
        - Primäre Abteilung
        - Primärer Standort
        - Primäre Kostenstelle
        - Primäre Geschäftsrolle

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

          Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen.
    - **Standardwert**: Standardwert der Eigenschaft für das Benutzerkonto einer Identität, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
    - **Immer Standardwert verwenden**: Gibt an, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.
    - **Benachrichtigung bei Verwendung des Standards**: Gibt an, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Identität - Erstellung neues Benutzerkontos mit Standardwerten** verwendet.

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

Verwandte Themen

- IT Betriebsdaten erfassen auf Seite 63

IT Betriebsdaten erfassen

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

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

Beispiel:

In der Regel erhält jede Identität der Abteilung A ein Standardbenutzerkonto in der Domäne A. Zusätzlich erhalten einige Identitäten der Abteilung A administrative Benutzerkonten in der Domäne A.

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

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.
3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.
    - **Wirksam für**: Legen Sie den Anwendungsbereich der IT Betriebsdaten fest. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.

Um den Anwendungsbereich festzulegen

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

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

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

d. Klicken Sie **OK**.

- **Spalte**: Wählen Sie die Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.

  In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

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

4. Speichern Sie die Änderungen.

Verwandte Themen

- Abbildungsvorschriften für IT Betriebsdaten erstellen auf Seite 61

IT Betriebsdaten ändern

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

Voraussetzungen

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

  - ODER -

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

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

Um die Bildungsregeln auszuführen

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Bildungsregeln ausführen**.

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

   - **Alter Wert**: Wert der Objekteigenschaft vor der Änderung der IT Betriebsdaten.
   - **Neuer Wert**: Wert der Objekteigenschaft nach der Änderung der IT Betriebsdaten.
   - **Auswahl**: Gibt an, ob der neue Wert für das Benutzerkonto übernommen werden soll.
4. Markieren Sie in der Spalte **Auswahl** alle Objekteigenschaften, für die der neue Wert übernommen werden soll.
5. Klicken Sie **Übernehmen**.

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinition an Identitäten

Kontendefinitionen werden an die Identitäten des Unternehmens zugewiesen.

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

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

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

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Identitäten

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

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

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

   - ODER -

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

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

Detaillierte Informationen zum Thema

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 67
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 67
- Kontendefinition an alle Identitäten zuweisen auf Seite 68
- Kontendefinition direkt an Identitäten zuweisen auf Seite 69
- Kontendefinition an Systemrollen zuweisen auf Seite 70
- Kontendefinition in den IT Shop aufnehmen auf Seite 70

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

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

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

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

    Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinition an Geschäftsrollen zuweisen auf Seite 67
- Kontendefinition an alle Identitäten zuweisen auf Seite 68
- Kontendefinition direkt an Identitäten zuweisen auf Seite 69
- Kontendefinition an Systemrollen zuweisen auf Seite 70
- Kontendefinition in den IT Shop aufnehmen auf Seite 70

Kontendefinition an Geschäftsrollen zuweisen

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

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

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 67
- Kontendefinition an alle Identitäten zuweisen auf Seite 68
- Kontendefinition direkt an Identitäten zuweisen auf Seite 69
- Kontendefinition an Systemrollen zuweisen auf Seite 70
- Kontendefinition in den IT Shop aufnehmen auf Seite 70

Kontendefinition an alle Identitäten zuweisen

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

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

Um eine Kontendefinition an alle Identitäten zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Automatische Zuweisung zu Identitäten aktivieren**.

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

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 67
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 67
- Kontendefinition direkt an Identitäten zuweisen auf Seite 69
- Kontendefinition an Systemrollen zuweisen auf Seite 70
- Kontendefinition in den IT Shop aufnehmen auf Seite 70

Kontendefinition direkt an Identitäten zuweisen

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

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

Um eine Kontendefinition direkt an Identitäten zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 67
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 67

- Kontendefinition an alle Identitäten zuweisen auf Seite 68
- Kontendefinition an Systemrollen zuweisen auf Seite 70
- Kontendefinition in den IT Shop aufnehmen auf Seite 70

Kontendefinition an Systemrollen zuweisen

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

Mit dieser Aufgabe nehmen Sie eine Kontendefinition in Systemrollen auf.

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 67
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 67
- Kontendefinition an alle Identitäten zuweisen auf Seite 68
- Kontendefinition direkt an Identitäten zuweisen auf Seite 69
- Kontendefinition in den IT Shop aufnehmen auf Seite 70

Kontendefinition in den IT Shop aufnehmen

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

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

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

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

Um eine Kontendefinition in den IT Shop aufzunehmen (bei rollenbasierter Anmeldung)

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

Um eine Kontendefinition in den IT Shop aufzunehmen (bei nicht-rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontendefinition an die IT Shop Regale zu.
5. Speichern Sie die Änderungen.

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

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

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

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Kontendefinition aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

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

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

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

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

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.
3. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Klicken Sie **OK**.

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

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

Verwandte Themen

- Stammdaten einer Kontendefinition auf Seite 55
- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 67
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 67
- Kontendefinition an alle Identitäten zuweisen auf Seite 68

- Kontendefinition direkt an Identitäten zuweisen auf Seite 69
- Kontendefinition an Systemrollen zuweisen auf Seite 70

Kontendefinitionen an OneLogin Domänen zuweisen

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **OneLogin > Domänen** die Domäne.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Automatische Zuordnung von Identitäten zu OneLogin Benutzerkonten auf Seite 76

Kontendefinitionen löschen

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

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Identitäten.
    a. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

d. Wählen Sie die Aufgabe **Automatische Zuweisung zu Identitäten deaktivieren**.

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

f. Speichern Sie die Änderungen.

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

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

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

   e. Speichern Sie die Änderungen.

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

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

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

   d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Abteilungen, Kostenstellen und Standorte.

   e. Speichern Sie die Änderungen.

4. Entfernen Sie die Zuordnung der Kontendefinition zu Geschäftsrollen.

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

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

   e. Speichern Sie die Änderungen.

5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden.

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

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

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

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

e. Klicken Sie **OK**.

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

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

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

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

e. Klicken Sie **OK**.

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

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

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

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

e. Speichern Sie die Änderungen.

7. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.

a. Wählen Sie im Manager in der Kategorie **OneLogin > Domänen** die Domäne.

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

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

d. Speichern Sie die Änderungen.

8. Löschen Sie die Kontendefinition.

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

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Klicken Sie , um die Kontendefinition zu löschen.

Automatische Zuordnung von Identitäten zu OneLogin Benutzerkonten

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

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

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

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

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

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

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

zu Identitäten erfolgen soll.

Beispiel:

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

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

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

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

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

   Jeder Eintrag in der Liste wird als Teil eines regulären Ausdrucks behandelt. Metazeichen für reguläre Ausdrücke können verwendet werden.
5. Um einen Eintrag zu löschen, wählen Sie den Eintrag und klicken Sie **Löschen**.
6. Klicken Sie **OK**.

- Legen Sie über den Konfigurationsparameter **TargetSystem | OneLogin | PersonAutoDisabledAccounts** fest, ob an deaktivierte Benutzerkonten automatisch Identitäten zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
- Weisen Sie der Domäne eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Identitätenzuordnung in der Domäne.

HINWEIS:

Für die Synchronisation gilt:

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

Außerhalb der Synchronisation gilt:

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

HINWEIS:

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

Identitäten verbunden. Es wird jedoch noch keine Kontendefinition zugewiesen. Die Benutzerkonten sind somit im Zustand **Linked** (verbunden).

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

Weitere Informationen finden Sie unter OneLogin Benutzerkonten über Kontendefinitionen verwalten auf Seite 47.

Verwandte Themen

- Kontendefinitionen erstellen auf Seite 54
- Kontendefinitionen an OneLogin Domänen zuweisen auf Seite 73
- Automatisierungsgrade für OneLogin Benutzerkonten ändern auf Seite 81
- Suchkriterien für die automatische Identitätenzuordnung bearbeiten auf Seite 78

Suchkriterien für die automatische Identitätenzuordnung bearbeiten

HINWEIS: Es wird zunächst versucht ein Active Directory Benutzerkonto zu ermitteln und dessen zugeordnete Identität dem OneLogin Benutzerkonto zuzuweisen. Wird kein passendes Active Directory Benutzerkonto gefunden, werden die Suchkriterien verwendet, um eine Identität zu ermitteln.

Sollen andere Verzeichnisdienste, wie beispielsweise LDAP, verwendet werden, um ein Benutzerkonto und dessen zugeordnete Identität zu ermitteln, passen Sie im Designer das Skript `OLG_PersonAuto_Mapping_OLGUser` an.

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

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

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

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

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

Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um Kriterien für die Identitätenzuordnung festzulegen

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

   Tabelle 9: Standardsuchkriterien für Benutzerkonten

Anwenden auf	Spalte an Identität	Spalte am Benutzerkonto
OneLogin Benutzerkonten	Standard-E-Mail-Adresse (`DefaultEmailAddress`)	E-Mail-Adresse (`EMail`)

5. Speichern Sie die Änderungen.

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

Verwandte Themen

- Identitäten suchen und direkt an Benutzerkonten zuordnen auf Seite 79
- Automatische Zuordnung von Identitäten zu OneLogin Benutzerkonten auf Seite 76

Identitäten suchen und direkt an Benutzerkonten zuordnen

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

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

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

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

Um Suchkriterien auf die Benutzerkonten anzuwenden

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Suchkriterien für die Identitätenzuordnung definieren**.
4. Im unteren Bereich des Formulars klicken Sie **Neu laden**.

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

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

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

Um Identitäten direkt an Benutzerkonten zuzuordnen

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

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

  - ODER -

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

4. Klicken Sie **Ausgewählte zuweisen**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

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

Um Zuordnungen zu entfernen

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

     Von den ausgewählten Benutzerkonten werden die zugeordneten Identitäten entfernt.

Automatisierungsgrade für OneLogin Benutzerkonten ändern

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

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

1. Wählen Sie in der Ergebnisliste das Benutzerkonto.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von OneLogin Benutzerkonten bearbeiten auf Seite 128

Unterstützte Typen von Benutzerkonten

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

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identitätstyp

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

  Tabelle 10: Identitätstypen von Benutzerkonten

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

- Privilegiertes Benutzerkonto

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

Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 83
- Administrative Benutzerkonten auf Seite 84
- Administrative Benutzerkonten für eine Identität bereitstellen auf Seite 84
- Administrative Benutzerkonten für mehrere Identitäten bereitstellen auf Seite 85
- Privilegierte Benutzerkonten auf Seite 86

Standardbenutzerkonten

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

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

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

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

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

   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IsGroupAccount_Role` den Standardwert **1** und aktivieren Sie die Option **Immer Standardwert verwenden**.
   - Verwenden Sie in der Abbildungsvorschrift für die Spalte `IdentityType` den Standardwert **Primary** und aktivieren Sie die Option **Immer Standardwert verwenden**.
4. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem. Wählen Sie unter **Wirksam für** das konkrete Zielsystem.

   Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.
5. Weisen Sie die Kontendefinition an die Identitäten zu.

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

Verwandte Themen

- Kontendefinitionen für OneLogin Benutzerkonten auf Seite 53

Administrative Benutzerkonten

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

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

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

Verwandte Themen

- Administrative Benutzerkonten für eine Identität bereitstellen auf Seite 84
- Administrative Benutzerkonten für mehrere Identitäten bereitstellen auf Seite 85

Administrative Benutzerkonten für eine Identität bereitstellen

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

Voraussetzungen

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

Um ein administratives Benutzerkonto für eine Identität bereitzustellen

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

a. Wählen Sie im Manager die Kategorie **OneLogin > Benutzerkonten**.
b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** die Identität, die dieses administrative Benutzerkonto nutzt.

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

Verwandte Themen

- Administrative Benutzerkonten für mehrere Identitäten bereitstellen auf Seite 85
- Ausführliche Informationen zur Abbildung von Identitätstypen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administrative Benutzerkonten für mehrere Identitäten bereitstellen

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

Voraussetzung

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

Um ein administratives Benutzerkonto für mehrere Identitäten bereitzustellen

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

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

d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** eine Identität mit dem Typ **Gruppenidentität**.

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

3. Weisen Sie dem Benutzerkonto die Identitäten zu, die dieses administrative Benutzerkonto nutzen sollen.

a. Wählen Sie im Manager die Kategorie **OneLogin > Benutzerkonten**.

b. Wählen Sie in der Ergebnisliste das Benutzerkonto.

c. Wählen Sie die Aufgabe **Identitäten mit Nutzungsberechtigungen zuzuweisen**.

d. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Identitäten zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Identität und doppelklicken Sie .

Verwandte Themen

- Administrative Benutzerkonten für eine Identität bereitstellen auf Seite 84
- Ausführliche Informationen zur Abbildung von Identitätstypen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Privilegierte Benutzerkonten

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

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

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

1. Erstellen Sie eine Kontendefinition. Erstellen Sie einen neuen Automatisierungsgrad für privilegierte Benutzerkonten und weisen Sie diesen Automatisierungsgrad an die Kontendefinition zu.

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

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

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

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

   Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.
6. Weisen Sie die Kontendefinition direkt an die Identitäten zu, die mit privilegierten Benutzerkonten arbeiten sollen.

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

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

Verwandte Themen

- Kontendefinitionen für OneLogin Benutzerkonten auf Seite 53

Löschverzögerung für OneLogin Benutzerkonten festlegen

Über die Löschverzögerung legen Sie fest, wie lange die Benutzerkonten nach dem Auslösen des Löschens in der Datenbank verbleiben, bevor sie endgültig entfernt werden. Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Die Benutzerkonten werden zunächst deaktiviert oder gesperrt. Bis zum Ablauf der Löschverzögerung besteht die Möglichkeit die Benutzerkonten wieder zu aktivieren. Nach Ablauf der Löschverzögerung werden die Benutzerkonten aus der Datenbank gelöscht und ein Wiederherstellen ist nicht mehr möglich.

Sie haben die folgenden Möglichkeiten die Löschverzögerung zu konfigurieren.

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

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

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

  Beispiel:

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

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

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

Managen von Mitgliedschaften in OneLogin Rollen

OneLogin Benutzerkonten können in OneLogin Rollen zusammengefasst werden, mit denen der Zugriff auf OneLogin Anwendungen geregelt werden kann.

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

Detaillierte Informationen zum Thema

Zuweisen von OneLogin Rollen an OneLogin Benutzerkonten

OneLogin Rollen können direkt oder indirekt an OneLogin Benutzerkonten zugewiesen werden.

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

Des Weiteren können OneLogin Rollen im Web Portal bestellt werden. Dazu werden Identitäten als Kunden in einen Shop aufgenommen. Alle OneLogin Rollen, die als Produkte

diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte OneLogin Rollen werden nach erfolgreicher Genehmigung den Identitäten zugewiesen.

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

Um auf Sonderanforderungen schnell zu reagieren, können Sie die OneLogin Rollen auch direkt an OneLogin Benutzerkonten zuweisen.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

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

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von OneLogin Rollen an OneLogin Benutzerkonten auf Seite 90
- OneLogin Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 92
- OneLogin Rollen an Geschäftsrollen zuweisen auf Seite 93
- OneLogin Rollen in Systemrollen aufnehmen auf Seite 94
- OneLogin Rollen in den IT Shop aufnehmen auf Seite 95
- OneLogin Rollen automatisch in den IT Shop aufnehmen auf Seite 97
- OneLogin Benutzerkonten direkt an OneLogin Rollen zuweisen auf Seite 99
- OneLogin Rollen direkt an OneLogin Benutzerkonten zuweisen auf Seite 100

Voraussetzungen für indirekte Zuweisungen von OneLogin Rollen an OneLogin Benutzerkonten

Bei der indirekten Zuweisung werden Identitäten und OneLogin Rollen in hierarchische Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen

eingeordnet. Für die indirekte Zuweisung von OneLogin Rollen prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Identitäten und OneLogin Rollen erlaubt.

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

   Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

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

      - ODER -

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

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

Verwandte Themen

- Stammdaten von OneLogin Benutzerkonten bearbeiten auf Seite 128
- Allgemeine Stammdaten für OneLogin Benutzerkonten auf Seite 128

OneLogin Rollen an Abteilungen, Kostenstellen und Standorte zuweisen

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

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

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

    Um eine Zuweisung zu entfernen

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

Um Rollen an eine Abteilung, eine Kostenstelle oder einen Standort zuzuweisen (bei nicht-rollenbasierter Anmeldung oder bei rollenbasierter Anmeldung)

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

    - ODER -

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

    - ODER -

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

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

    Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von OneLogin Rollen an OneLogin Benutzerkonten auf Seite 90
- OneLogin Rollen an Geschäftsrollen zuweisen auf Seite 93
- OneLogin Rollen in Systemrollen aufnehmen auf Seite 94
- OneLogin Rollen in den IT Shop aufnehmen auf Seite 95
- OneLogin Rollen automatisch in den IT Shop aufnehmen auf Seite 97
- OneLogin Benutzerkonten direkt an OneLogin Rollen zuweisen auf Seite 99
- OneLogin Rollen direkt an OneLogin Benutzerkonten zuweisen auf Seite 100
- One Identity Manager Benutzer für die Verwaltung einer OneLogin Domäne auf Seite 9

OneLogin Rollen an Geschäftsrollen zuweisen

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

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

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

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Wählen Sie im Bereich **Zuordnungen hinzufügen** die Rollenklasse und weisen Sie die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Um Rollen an eine Geschäftsrolle zuzuweisen (bei nicht-rollenbasierter Anmeldung oder bei rollenbasierter Anmeldung)

1. Wählen Sie im Manager die Kategorie **Geschäftsrollen > <Rollenklasse>**.
2. Wählen Sie in der Ergebnisliste die Geschäftsrolle.

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von OneLogin Rollen an OneLogin Benutzerkonten auf Seite 90
- OneLogin Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 92
- OneLogin Rollen in Systemrollen aufnehmen auf Seite 94
- OneLogin Rollen in den IT Shop aufnehmen auf Seite 95
- OneLogin Rollen automatisch in den IT Shop aufnehmen auf Seite 97
- OneLogin Benutzerkonten direkt an OneLogin Rollen zuweisen auf Seite 99
- OneLogin Rollen direkt an OneLogin Benutzerkonten zuweisen auf Seite 100
- One Identity Manager Benutzer für die Verwaltung einer OneLogin Domäne auf Seite 9

OneLogin Rollen in Systemrollen aufnehmen

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

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

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

Um eine Rolle an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.

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

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Systemrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von OneLogin Rollen an OneLogin Benutzerkonten auf Seite 90
- OneLogin Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 92
- OneLogin Rollen an Geschäftsrollen zuweisen auf Seite 93
- OneLogin Rollen in den IT Shop aufnehmen auf Seite 95
- OneLogin Rollen automatisch in den IT Shop aufnehmen auf Seite 97
- OneLogin Benutzerkonten direkt an OneLogin Rollen zuweisen auf Seite 99
- OneLogin Rollen direkt an OneLogin Benutzerkonten zuweisen auf Seite 100

OneLogin Rollen in den IT Shop aufnehmen

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

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

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

Um eine Rolle in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen > OneLogin Rollen** (bei rollenbasierter Anmeldung).

2. Wählen Sie in der Ergebnisliste die Rolle.

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

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von OneLogin Rollen an OneLogin Benutzerkonten auf Seite 90
- Allgemeine Stammdaten für OneLogin Rollen auf Seite 143
- OneLogin Rollen aus einem IT Shop Regal entfernen auf Seite 96
- OneLogin Rollen aus allen IT Shop Regalen entfernen auf Seite 97
- OneLogin Rollen automatisch in den IT Shop aufnehmen auf Seite 97
- One Identity Manager Benutzer für die Verwaltung einer OneLogin Domäne auf Seite 9

OneLogin Rollen aus einem IT Shop Regal entfernen

Um eine Rolle aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

Verwandte Themen

- OneLogin Rollen aus allen IT Shop Regalen entfernen auf Seite 97

OneLogin Rollen aus allen IT Shop Regalen entfernen

Um eine Rolle aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

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

Verwandte Themen

- OneLogin Rollen aus einem IT Shop Regal entfernen auf Seite 96

OneLogin Rollen automatisch in den IT Shop aufnehmen

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

Um OneLogin Rollen automatisch in den IT Shop aufzunehmen

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

   Der Konfigurationsparameter enthält eine Auflistung aller OneLogin Rollen, die nicht automatisch zum IT Shop zugeordnet werden sollen. Bei Bedarf können Sie die Liste erweitern. Erfassen Sie dazu im Wert des Konfigurationsparameters die Namen der

Rollen. Die Namen werden in einer Pipe (|) getrennten Liste angegeben. Reguläre Ausdrücke werden unterstützt.

3. Kompilieren Sie die Datenbank.

Die OneLogin Rollen werden ab diesem Zeitpunkt automatisch in den IT Shop aufgenommen.

Folgende Schritte werden bei der Aufnahme einer OneLogin Rolle in den IT Shop automatisch ausgeführt.

1. Es wird eine Leistungsposition für die OneLogin Rolle ermittelt.

   Für jede OneLogin Rolle wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Bezeichnung der OneLogin Rolle.

   - Für OneLogin Rollen mit Leistungsposition wird die Leistungsposition angepasst.
   - OneLogin Rollen ohne Leitungsposition erhalten eine neue Leistungsposition.

2. Die Leistungsposition wird der Standard-Servicekategorie **OneLogin Rollen** zugeordnet.
3. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet.

   Die Produkteigner können Bestellungen von Mitgliedschaften in diesen OneLogin Rollen genehmigen. Standardmäßig wird der Eigentümer einer OneLogin Rolle als Produkteigner ermittelt.

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

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

4. Die OneLogin Rolle wird mit der Option **IT Shop** gekennzeichnet und dem IT Shop Regal **OneLogin Rollen** im Shop **Identity & Access Lifecycle** zugewiesen.

Anschließend können die Mitgliedschaften in OneLogin Rollen über das Web Portal bestellt werden.

HINWEIS: Wenn eine OneLogin Rolle endgültig aus der One Identity Manager-Datenbank gelöscht wird, wird auch die zugehörige Leistungsposition gelöscht.

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

Verwandte Themen

- OneLogin Rollen in den IT Shop aufnehmen auf Seite 95
- OneLogin Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 92
- OneLogin Rollen an Geschäftsrollen zuweisen auf Seite 93
- OneLogin Rollen in Systemrollen aufnehmen auf Seite 94
- OneLogin Benutzerkonten direkt an OneLogin Rollen zuweisen auf Seite 99

OneLogin Benutzerkonten direkt an OneLogin Rollen zuweisen

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

Um Benutzerkonten direkt an eine Rolle zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- OneLogin Rollen direkt an OneLogin Benutzerkonten zuweisen auf Seite 100
- OneLogin Rollen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 92
- OneLogin Rollen an Geschäftsrollen zuweisen auf Seite 93
- OneLogin Rollen in Systemrollen aufnehmen auf Seite 94
- OneLogin Rollen in den IT Shop aufnehmen auf Seite 95
- OneLogin Rollen automatisch in den IT Shop aufnehmen auf Seite 97

OneLogin Rollen direkt an OneLogin Benutzerkonten zuweisen

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

Um Rollen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Zuweisen von OneLogin Rollen an OneLogin Benutzerkonten auf Seite 89

Wirksamkeit von Mitgliedschaften in OneLogin Rollen

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

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

HINWEIS:

- Ein wechselseitiger Ausschluss zweier Rollen kann nicht definiert werden. Das heißt, die Festlegung "Rolle A schließt Rolle B aus" UND "Rolle B schließt Rolle A aus" ist nicht zulässig.

- Für eine Rolle muss jede auszuschließende Rolle einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.

Die Wirksamkeit der Zuweisungen wird in den Tabellen `OLGUserInOLGRole` über die Spalte `XIsInEffect` abgebildet.

Voraussetzungen

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

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

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

Um Rollen auszuschließen

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen**.
2. Wählen Sie in der Ergebnisliste eine Rolle.
3. Wählen Sie die Aufgabe **Rollen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu, die sich mit der gewählten Rolle ausschließen.

   - ODER -

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

Vererbung von OneLogin Rollen anhand von Kategorien

Im One Identity Manager können Rollen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Rollen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In den übrigen Tabellen geben Sie Ihre Kategorien für die Rollen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 63**.

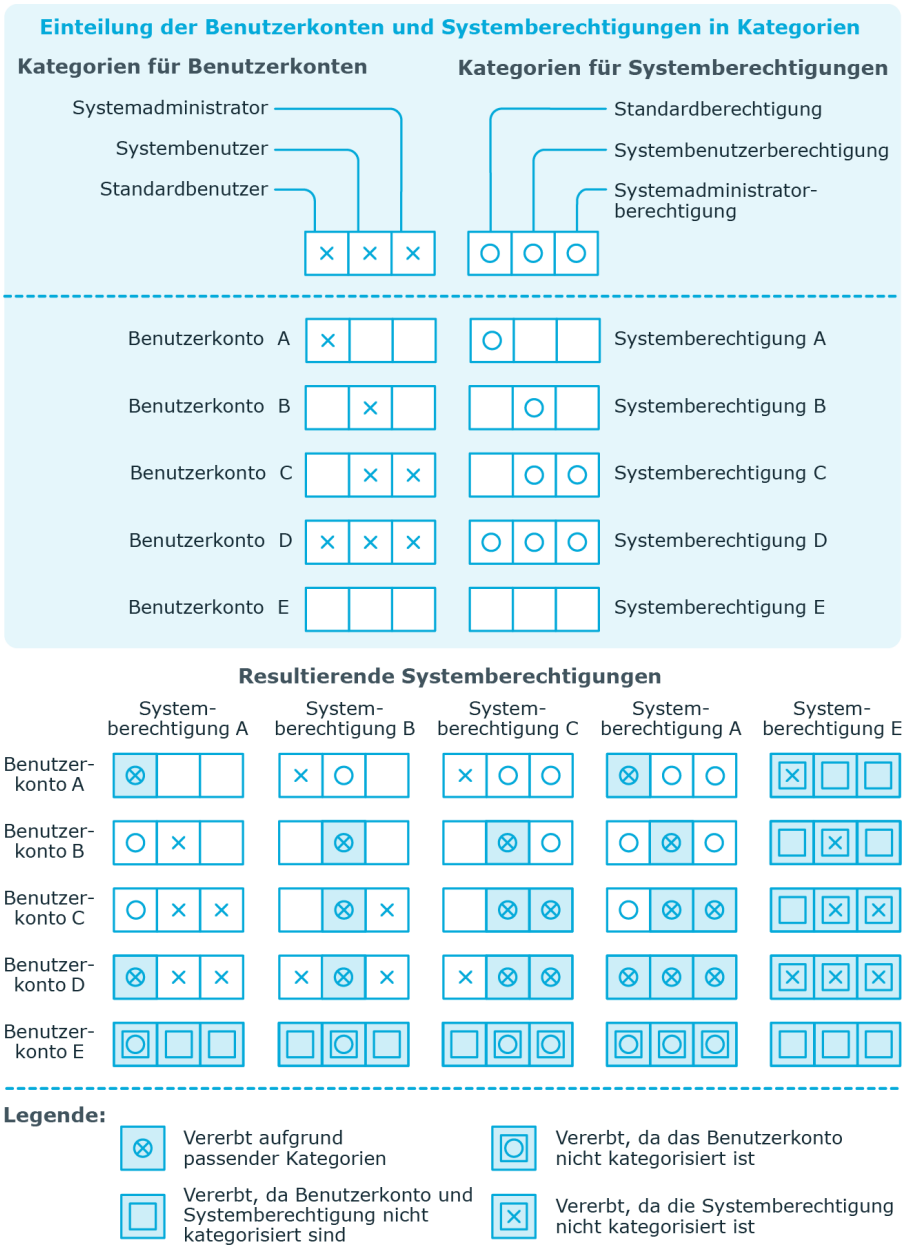
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Rolle kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Rolle überein, wird die Rolle an das Benutzerkonto vererbt. Ist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

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

Tabelle 11: Beispiele für Kategorien

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

Abbildung 2: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

- Definieren Sie im Manager an der OneLogin Domäne die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Rollen über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 125
- Allgemeine Stammdaten für OneLogin Benutzerkonten auf Seite 128
- Allgemeine Stammdaten für OneLogin Rollen auf Seite 143

Übersicht aller Zuweisungen

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

Beispiele:

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

Um detaillierte Informationen über Zuweisungen anzuzeigen

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

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Identitäten befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.

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

Abbildung 3: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 12: Bedeutung der Symbole in der Symbolleiste des Berichts

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

5

Bereitstellen von Anmeldeinformationen für OneLogin Benutzerkonten

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

Detaillierte Informationen zum Thema

- Kennwortrichtlinien für OneLogin Benutzerkonten auf Seite 106
- Initiales Kennwort für neue OneLogin Benutzerkonten auf Seite 118
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 119

Kennwortrichtlinien für OneLogin Benutzerkonten

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

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

Detaillierte Informationen zum Thema

- Vordefinierte Kennwortrichtlinien auf Seite 107
- Kennwortrichtlinien anwenden auf Seite 108
- Kennwortrichtlinien erstellen auf Seite 110
- Kennwortrichtlinien bearbeiten auf Seite 110
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 114
- Ausschlussliste für Kennwörter auf Seite 117
- Prüfen eines Kennwortes auf Seite 118
- Generieren eines Kennwortes testen auf Seite 118

Vordefinierte Kennwortrichtlinien

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

Kennwortrichtlinie für die Anmeldung am One Identity Manager

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

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

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Identitäten

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

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

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

Kennwortrichtlinien für Benutzerkonten

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

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

Für OneLogin ist die Kennwortrichtlinie **OneLogin Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der OneLogin Benutzerkonten (`OLGUser.UserPassword`) einer OneLogin Domäne anwenden.

Wenn die Kennwortanforderungen der Domänen unterschiedlich sind, wird empfohlen, je Domäne eine eigene Kennwortrichtlinie einzurichten.

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

Kennwortrichtlinien anwenden

Für OneLogin ist die Kennwortrichtlinie **OneLogin Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der OneLogin Benutzerkonten (`OLGUser.UserPassword`) einer OneLogin Domäne anwenden.

Wenn die Kennwortanforderungen der Domänen unterschiedlich sind, wird empfohlen, je Domäne eine eigene Kennwortrichtlinie einzurichten.

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

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

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

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

Um eine Kennwortrichtlinie neu zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Klicken Sie im Bereich **Zuweisungen** die Schaltfläche **Hinzufügen** und erfassen Sie folgende Daten.
    - **Anwenden auf**: Anwendungsbereich der Kennwortrichtlinie.

      Um den Anwendungsbereich festzulegen

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

Um die Zuweisung einer Kennwortrichtlinie zu ändern

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

Kennwortrichtlinien erstellen

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

Um eine Kennwortrichtlinie zu erstellen

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Auf dem Stammdatenformular erfassen Sie die Stammdaten der Kennwortrichtlinie.
3. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 111
- Richtlinieneinstellungen auf Seite 113
- Zeichenklassen für Kennwörter auf Seite 111
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 114
- Kennwortrichtlinien bearbeiten auf Seite 110

Kennwortrichtlinien bearbeiten

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

Um eine Kennwortrichtlinie zu bearbeiten

1. Wählen Sie im Manager die Kategorie **OneLogin > Basisdaten zur Konfiguration > Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten der Kennwortrichtlinie.
5. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 111
- Richtlinieneinstellungen auf Seite 113
- Zeichenklassen für Kennwörter auf Seite 111

- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 114
- Kennwortrichtlinien erstellen auf Seite 110

Allgemeine Stammdaten für Kennwortrichtlinien

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 13: Stammdaten einer Kennwortrichtlinie

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

Zeichenklassen für Kennwörter

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

Tabelle 14: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Erforderliche Anzahl von Zeichenklassen	Anzahl der Regeln für Zeichenklassen, die erfüllt sein müssen, damit ein Kennwort der Kennwortrichtlinie entspricht. Berücksichtigt werden die Regeln für **Min. Anzahl Buchstaben**, **Min.**

Eigenschaft	Bedeutung
	Anzahl Kleinbuchstaben, **Min. Anzahl Großbuchstaben**, **Min. Anzahl Ziffern** und **Min. Anzahl Sonderzeichen**. Es bedeuten: • Wert **0**: Es müssen alle Zeichenklassenregeln erfüllt sein. • Wert **> 0**: Anzahl der Zeichenklassenregeln, die mindestens erfüllt sein müssen. Der Wert kann maximal der Anzahl der Regeln entsprechend, deren Wert **> 0** ist. HINWEIS: Die Prüfung erfolgt nicht für generierte Kennwörter.
Min. Anzahl Buchstaben	Gibt an, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss.
Min. Anzahl Kleinbuchstaben	Gibt an, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Großbuchstaben	Gibt an, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Ziffern	Gibt an, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Gibt an, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.
Zulässige Sonderzeichen	Liste zulässiger Sonderzeichen.
Max. identische Zeichen insgesamt	Maximale Anzahl identischer Zeichen, die insgesamt im Kennwort vorkommen dürfen.
Max. identische Zeichen aufeinanderfolgend	Maximale Anzahl identischer Zeichen, die nacheinander wiederholt werden können.
Unzulässige Sonderzeichen	Liste unzulässiger Sonderzeichen.
Keine Klein-buchstaben erzeugen	Gibt an, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keinen Großbuch-staben erzeugen	Gibt an, ob ein generiertes Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Ziffern erzeugen	Gibt an, ob ein generiertes Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.

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

Richtlinieneinstellungen

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

Tabelle 15: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wenn beim Erstellen eines Benutzerkontos kein Kennwort angegeben wird oder kein Zufallskennwort generiert wird, dann wird das initiale Kennwort benutzt.
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben muss. Ist der Wert **0**, ist kein Kennwort erforderlich.
Max. Länge	Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann. Der maximal zulässige Wert ist **256**.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Die Anzahl der Fehlanmeldungen wird nur bei der Anmeldung am One Identity Manager berücksichtigt. Ist der Wert **0**, dann wird die Anzahl der Fehlanmeldungen nicht berücksichtigt. Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder identitätenbasierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen überschritten, kann sich die Identität oder der Systembenutzer nicht mehr am One Identity Manager anmelden. Kennwörter gesperrter Identitäten und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.

Eigenschaft	Bedeutung
Max. Tage gültig	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird. Ist der Wert **0**, dann läuft das Kennwort nicht ab.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert. Ist der Wert **0**, dann werden keine Kennwörter in der Kennwortchronik gespeichert.
Min. Kennwortstärke	Gibt an, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert **0** wird die Kennwortstärke nicht geprüft. Die Werte **1**, **2**, **3** und **4** geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert **1** die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert **4** fordert die höchste Komplexität.
Namensbestandteile unzulässig	Gibt an, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die Option **Enthält Namensbestandteile für die Kennwortprüfung** aktiviert ist. Die Option passen Sie im Designer an der Spaltendefinition an. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Kundenspezifische Skripte für Kennwortanforderungen

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

Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 115
- Skript zum Generieren eines Kennwortes auf Seite 116

Skript zum Prüfen eines Kennwortes

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

Syntax für Prüfskripte

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

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Kennwort, das zu prüfen ist

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

Beispiel: Skript zum Prüfen eines Kennwortes

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

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

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

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

Verwandte Themen

- Skript zum Generieren eines Kennwortes auf Seite 116

Skript zum Generieren eines Kennwortes

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

Syntax für Generierungsskripte

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

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Generiertes Kennwort

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

Beispiel: Skript zum Generieren eines Kennwortes

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

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

```
      ' replace invalid characters at first position
      If pwd.Length>0
           If pwd(0)="?" Or pwd(0)="!"
                spwd.SetAt(0, CChar("_"))
           End If
      End If
End Sub
```

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

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

Verwandte Themen

- Skript zum Prüfen eines Kennwortes auf Seite 115

Ausschlussliste für Kennwörter

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

HINWEIS: Die Ausschlussliste ist global für alle Kennwortrichtlinien gültig.

Um einen Begriff in die Ausschlussliste aufzunehmen

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

Prüfen eines Kennwortes

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

Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht

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

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

Generieren eines Kennwortes testen

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

Um ein Kennwort zu generieren, das der Kennwortrichtlinie entspricht

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

   Das generierte Kennwort wird angezeigt.

Initiales Kennwort für neue OneLogin Benutzerkonten

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

- Tragen Sie beim Erstellen des Benutzerkontos in den Stammdaten ein Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.
    - Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | OneLogin | Accounts | InitialRandomPassword**.
    - Verwenden Sie zielsystemspezifische Kennwortrichtlinien und definieren Sie in den Kennwortrichtlinien die Zeichenklassen, die das Kennwort enthalten muss.
    - Legen Sie fest, an welche Identität das initiale Kennwort per E-Mail versendet wird.

Verwandte Themen

- Kennwortrichtlinien für OneLogin Benutzerkonten auf Seite 106
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 119

E-Mail-Benachrichtigungen über Anmeldeinformationen

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

Um Benachrichtigungen zu nutzen, sind folgende Voraussetzungen zu erfüllen:

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

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

Um die initialen Anmeldeinformationen per E-Mail zu versenden

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

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

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

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

Abbildung von OneLogin Objekten im One Identity Manager

Im One Identity Manager werden die Benutzerkonten, Rollen und Anwendungen einer OneLogin Domäne abgebildet. Diese Objekte werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Ihre Eigenschaften können im Manager angezeigt oder bearbeitet werden.

Detaillierte Informationen zum Thema

OneLogin Domänen

Als Basisobjekte der Synchronisation werden OneLogin Domänen im One Identity Manager angelegt. Eine Domäne bildet das Zielsystem der Synchronisation mit OneLogin. Sie werden genutzt, um Provisionierungsprozesse, die automatische Zuordnung von Identitäten zu Benutzerkonten und die Vererbung von OneLogin Rollen und OneLogin Anwendungen an Benutzerkonten zu konfigurieren.

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

Verwandte Themen

- OneLogin Domänen erstellen auf Seite 122
- Stammdaten von OneLogin Domänen bearbeiten auf Seite 122
- Allgemeine Stammdaten für OneLogin Domänen auf Seite 123
- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 125
- Synchronisationsprojekt für eine OneLogin Domäne bearbeiten auf Seite 125
- Überblick über OneLogin Domänen anzeigen auf Seite 126
- Einzelobjekte synchronisieren auf Seite 44

OneLogin Domänen erstellen

HINWEIS: Die Einrichtung der Domänen in der One Identity Manager-Datenbank übernimmt der Synchronization Editor bei Verwendung einer Standardprojektvorlage. Falls erforderlich, können Domänen auch im Manager erstellt werden.

Um eine OneLogin Domäne zu erstellen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten für die Domäne.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von OneLogin Domänen bearbeiten auf Seite 122
- Allgemeine Stammdaten für OneLogin Domänen auf Seite 123
- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 125

Stammdaten von OneLogin Domänen bearbeiten

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

Um die Stammdaten einer OneLogin Domäne zu bearbeiten

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für eine Domäne.
5. Speichern Sie die Änderungen.

Verwandte Themen

- OneLogin Domänen erstellen auf Seite 122
- Allgemeine Stammdaten für OneLogin Domänen auf Seite 123
- Kategorien für die Vererbung von Berechtigungen definieren auf Seite 125

Allgemeine Stammdaten für OneLogin Domänen

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 16: Allgemeine Stammdaten einer Domäne

Eigenschaft	Beschreibung
Domäne	Bezeichnung der OneLogin Domäne. Dies entspricht dem `<subdomain>`-Anteil des DNS Namens.
Anzeigename	Name zur Anzeige der Domäne in der Benutzeroberfläche. Initial wird die Bezeichnung der Domäne übernommen; den Anzeigenamen können Sie jedoch ändern.
DNS Name	Vollständiger DNS Name. Beispiel: `<subdomain>.onelogin.com`
Kontendefinition (initial)	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diese Domäne die automatische Zuordnung von Identitäten zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet. Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Identität verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen

Eigenschaft	Beschreibung
	Synchronisation der Fall.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen der Domäne festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte der Domäne, der sie zugeordnet sind. Jeder Domäne können somit andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle, deren Mitglieder verantwortlich für die Administration dieser Domäne sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Synchronisiert durch	Art der Synchronisation, über welche die Daten zwischen der Domäne und dem One Identity Manager synchronisiert werden. Sobald Objekte für diese Domäne im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden. Beim Erstellen einer Domäne mit dem Synchronization Editor wird **One Identity Manager** verwendet. **Tabelle 17: Zulässige Werte** **Wert** / **Synchronisation durch** / **Provisionierung durch** One Identity Manager / OneLogin Konnektor / OneLogin Konnektor Keine Synchronisation / keine / keine HINWEIS: Wenn Sie **Keine Synchronisation** festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- Automatische Zuordnung von Identitäten zu OneLogin Benutzerkonten auf Seite 76
- Zielsystemverantwortliche für OneLogin auf Seite 159

Kategorien für die Vererbung von Berechtigungen definieren

Im One Identity Manager können Rollen selektiv an die Benutzerkonten vererbt werden. Dazu werden die Rollen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält verschiedene Tabellen. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In der übrigen Tabelle geben Sie Ihre Kategorien für die Rollen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 63**.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **OneLogin > Domänen** die Domäne.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wechseln Sie auf den Tabreiter **Abbildungsvorschrift Kategorien**.
4. Erweitern Sie den jeweiligen Basisknoten einer Tabelle.
5. Aktivieren Sie die Kategorie per Maus-Doppelklick auf das Symbol .
6. Tragen Sie eine beliebige Benennung der Kategorie für Benutzerkonten und Berechtigungen in der verwendeten Anmeldesprache ein.
7. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbung von OneLogin Rollen anhand von Kategorien auf Seite 101

Synchronisationsprojekt für eine OneLogin Domäne bearbeiten

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

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

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten**.

Verwandte Themen

- Anpassen der Synchronisationskonfiguration auf Seite 30

Überblick über OneLogin Domänen anzeigen

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

Um einen Überblick über eine Domäne zu erhalten

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Überblick über die OneLogin Domäne**.

OneLogin Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Benutzerkonten einer OneLogin Domäne. Ein Benutzer kann sich mit seinem Benutzerkonto an der Domäne anmelden und erhält über seine Rollenmitgliedschaften und Berechtigungen Zugriff auf die Anwendungen.

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

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

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

Detaillierte Informationen zum Thema

- Managen von OneLogin Benutzerkonten und Identitäten auf Seite 52
- Managen von Mitgliedschaften in OneLogin Rollen auf Seite 89
- OneLogin Benutzerkonten erstellen auf Seite 127
- Stammdaten von OneLogin Benutzerkonten bearbeiten auf Seite 128
- Allgemeine Stammdaten für OneLogin Benutzerkonten auf Seite 128
- Anmeldeinformationen für OneLogin Benutzerkonten auf Seite 132
- Informationen zum Verzeichnis für OneLogin Benutzerkonten auf Seite 133
- Informationen zur Firma von OneLogin Benutzerkonten auf Seite 134
- Benutzerdefinierte Felder für OneLogin Benutzerkonten ändern auf Seite 134
- Administratoren für OneLogin Rollen festlegen auf Seite 135
- Authentifizierungsmethoden an OneLogin Benutzerkonten zuweisen auf Seite 135
- Privilegien an OneLogin Benutzerkonten zuweisen auf Seite 136
- Zusatzeigenschaften an OneLogin Benutzerkonten zuweisen auf Seite 137
- OneLogin Benutzerkonten löschen und wiederherstellen auf Seite 137
- Überblick über OneLogin Benutzerkonten anzeigen auf Seite 138
- Einzelobjekte synchronisieren auf Seite 44

OneLogin Benutzerkonten erstellen

Benutzerkonten werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können neue Benutzerkonten im One Identity Manager einrichten.

Um ein Benutzerkonto zu erstellen

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

Verwandte Themen

- Allgemeine Stammdaten für OneLogin Benutzerkonten auf Seite 128
- Anmeldeinformationen für OneLogin Benutzerkonten auf Seite 132
- Informationen zum Verzeichnis für OneLogin Benutzerkonten auf Seite 133
- Informationen zur Firma von OneLogin Benutzerkonten auf Seite 134
- Stammdaten von OneLogin Benutzerkonten bearbeiten auf Seite 128

Stammdaten von OneLogin Benutzerkonten bearbeiten

Sie können vorhandene Benutzerkonten im One Identity Manager bearbeiten.

Um die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie im Manager die Kategorie **OneLogin > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Benutzerkontos.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für OneLogin Benutzerkonten auf Seite 128
- Anmeldeinformationen für OneLogin Benutzerkonten auf Seite 132
- Informationen zum Verzeichnis für OneLogin Benutzerkonten auf Seite 133
- Informationen zur Firma von OneLogin Benutzerkonten auf Seite 134
- OneLogin Benutzerkonten erstellen auf Seite 127

Allgemeine Stammdaten für OneLogin Benutzerkonten

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 18: Allgemeine Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Domäne	Domäne des Benutzerkontos.
Identität	Identität, die das Benutzerkonto verwendet. • Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Identität bereits eingetragen. • Wenn Sie die automatische Identitätenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Identität gesucht und in das Benutzerkonto übernommen. • Wenn Sie das Benutzerkonto manuell erstellen, können

Eigenschaft	Beschreibung
	Sie die Identität aus der Auswahlliste wählen. In der Auswahlliste werden im Standard aktivierte und deaktivierte Identitäten angezeigt. Um deaktivierte Identitäten nicht in der Auswahlliste anzuzeigen, aktivieren Sie den Konfigurationsparameter **QER | Person| HideDeactivatedIdentities**. HINWEIS: Wenn Sie eine deaktivierte Identität an ein Benutzerkonto zuordnen, wird das Benutzerkonto, abhängig von der Konfiguration, unter Umständen gesperrt oder gelöscht. Für ein Benutzerkonto mit einer Identität vom Typ **Organisatorische Identität**, **Persönliche Administratoridentität**, **Zusatzidentität**, **Gruppenidentität** oder **Dienstidentität** können Sie eine neue Identität erstellen. Klicken Sie dafür neben dem Eingabefeld und erfassen Sie die erforderlichen Identitätenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp.
Keine Verbindung mit einer Identität erforderlich	Gibt an, ob dem Benutzerkonto absichtlich keine Identität zugeordnet ist. Die Option wird automatisch aktiviert, wenn ein Benutzerkonto in der Ausschlussliste für die automatische Identitätenzuordnung enthalten ist oder eine entsprechende Attestierung erfolgt ist. Sie können die Option manuell setzen. Aktivieren Sie die Option, falls das Benutzerkonto mit keiner Identität verbunden werden muss (beispielsweise, wenn mehrere Identitäten das Benutzerkonto verwenden). Wenn durch die Attestierung diese Benutzerkonten genehmigt werden, werden diese Benutzerkonten künftig nicht mehr zur Attestierung vorgelegt. Im Web Portal können Benutzerkonten, die nicht mit einer Identität verbunden sind, nach verschiedenen Kriterien gefiltert werden.
Nicht mit einer Identität verbunden	Zeigt an, warum für das Benutzerkonto die Option **Keine Verbindung mit einer Identität erforderlich** aktiviert ist. Mögliche Werte sind: • **durch Administrator**: Die Option wurde manuell durch den Administrator aktiviert. • **durch Attestierung**: Das Benutzerkonto wurde attestiert. • **durch Ausschlusskriterium**: Das Benutzerkonto wird aufgrund eines Ausschlusskriteriums nicht mit einer Identität verbunden. Das Benutzerkonto ist beispielsweise in der Ausschlussliste für die automatische

Eigenschaft	Beschreibung
	Identitätenzuordnung enthalten (Konfigurationsparameter **PersonExcludeList**).
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Identität und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden. HINWEIS: Über die Aufgabe **Entferne Kontendefinition** am Benutzerkonto können Sie das Benutzerkonto wieder in den Zustand **Linked** zurücksetzen. Dabei wird die Kontendefinition vom Benutzerkonto und von der Identität entfernt. Das Benutzerkonto bleibt über diese Aufgabe erhalten, wird aber nicht mehr über die Kontendefinition verwaltet. Die Aufgabe entfernt nur Kontendefinitionen, die direkt zugewiesen sind (`XOrigin=1`).
Automatisierungsgrad	Automatisierungsgrad des Benutzerkontos. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
Vorname	Vorname des Benutzers.
Nachname	Nachname des Benutzers.
Titel	Akademischer Titel des Benutzers.
Benutzername	Name des Benutzerkontos zur Anmeldung an einer OneLogin Domäne.
E-Mail-Adresse	E-Mail-Adresse des Benutzerkontos.
Telefon	Telefonnummer.
Eindeutige Kennung	Unikale ID, unter der das Benutzerkonto durch OneLogin verwaltet wird.
Externe ID	ID des Benutzers in einem externen Verzeichnis.
Vertrauenswürdiger IdP	ID des vertrauenswürdigen IdP (Identitätsanbieter) in OneLogin, dem der Benutzer zugewiesen ist.

Eigenschaft	Beschreibung
Aktivierungszustand	Zustand der Aktivierung eines Benutzerkontos in OneLogin. Zulässige Werte sind **Nicht aktiviert**, **Aktiv**, **Ausgesetzt**, **Gesperrt**, **Kennwort abgelaufen**, **Kennwort ausstehend**, **Warten auf Kennwortrücksetzung** und **Sicherheitsfragen erforderlich**.
Lizenzierungsstatus	Status der Lizenzierung eines Benutzerkontos in OneLogin. Zulässige Werte sind **Lizenziert**, **Nicht lizenziert**, **Abgelehnt** und **Genehmigt**.
Gruppe	OneLogin Gruppe, zu der der Benutzer gehört.
Kontomanager	Verantwortlicher für das Benutzerkonto.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten . Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Kommentar	Freitextfeld für zusätzliche Erläuterungen.
Identitätstyp	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Identität. • **Organisatorische Identität**: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Identität genutzt wird. • **Zusatzidentität**: Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Identitäten genutzt wird. Weisen Sie alle Identitäten zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.

Eigenschaft	Beschreibung
Rollen erbbar	Gibt an, ob das Benutzerkonto OneLogin Rollen über die verbundene Identität erben darf. Ist die Option aktiviert, werden die Rollen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt.
Privilegiertes Benutzerkonto	Gibt an, ob es sich um ein privilegiertes Benutzerkonto handelt.

Verwandte Themen

- Kontendefinitionen für OneLogin Benutzerkonten auf Seite 53
- Automatische Zuordnung von Identitäten zu OneLogin Benutzerkonten auf Seite 76
- Vererbung von OneLogin Rollen anhand von Kategorien auf Seite 101
- Unterstützte Typen von Benutzerkonten auf Seite 81
- Anmeldeinformationen für OneLogin Benutzerkonten auf Seite 132
- Informationen zum Verzeichnis für OneLogin Benutzerkonten auf Seite 133
- Informationen zur Firma von OneLogin Benutzerkonten auf Seite 134
- Allgemeine Stammdaten für OneLogin Domänen auf Seite 123
- Voraussetzungen für indirekte Zuweisungen von OneLogin Rollen an OneLogin Benutzerkonten auf Seite 90

Anmeldeinformationen für OneLogin Benutzerkonten

Es werden die folgenden Anmeldeinformationen abgebildet.

Tabelle 19: Anmeldeinformationen

Eigenschaft	Beschreibung
Angelegt am	Gibt an, wann das Benutzerkonto erstellt wurde.
Datum der Einladung	Gibt an, wann das Benutzerkonto eingeladen wurde.
Datum der Aktivierung	Gibt an, wann das Benutzerkonto aktiviert wurde.
Kennwort	Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Identität kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Identität finden Sie im *One Identity Manager Administrationshandbuch für das*

Eigenschaft	Beschreibung
	Identity Management Basismodul. Wenn Sie ein zufällig generiertes initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen. Das Kennwort wird nach dem Publizieren in das Zielsystem aus der Datenbank gelöscht. HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien beachtet. Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die Anforderungen des Zielsystems verstößt.
Kennwortbestätigung	Kennwortwiederholung.
Letzte Kennwor-tänderung	Datum der letzten Kennwortänderung.
Letzte Anmeldung	Datum der letzten Anmeldung.
Anzahl fehlerhafter Anmeldungen	Anzahl der aufeinanderfolgenden ungültigen Anmeldeversuche des Benutzers.
Gesperrt bis	Gibt an, bis zu welchem Zeitpunkt das Benutzerkonto gesperrt ist.

Verwandte Themen

- Kennwortrichtlinien für OneLogin Benutzerkonten auf Seite 106
- Initiales Kennwort für neue OneLogin Benutzerkonten auf Seite 118
- Allgemeine Stammdaten für OneLogin Benutzerkonten auf Seite 128
- Informationen zum Verzeichnis für OneLogin Benutzerkonten auf Seite 133
- Informationen zur Firma von OneLogin Benutzerkonten auf Seite 134

Informationen zum Verzeichnis für OneLogin Benutzerkonten

Es werden folgende Informationen zum angeschlossenen Verzeichnisdienst, zum Beispiel Active Directory oder LDAP, abgebildet.

Tabelle 20: Angaben zum Verzeichnis

Eigenschaft	Beschreibung
Definierter Name	Definierter Name des Benutzerkontos im angeschlossenen

Eigenschaft	Beschreibung
	Verzeichnis.
Manager	Definierter Name des Managers im angeschlossenen Verzeichnis.
Benutzeranmeldename	Anmeldename des Benutzerkontos im angeschlossenen Verzeichnis.
Anmeldename (pre Win2000)	Anmeldename des Active Directory Benutzerkontos für die Vorgängerversion von Active Directory.

Verwandte Themen

- Allgemeine Stammdaten für OneLogin Benutzerkonten auf Seite 128
- Anmeldeinformationen für OneLogin Benutzerkonten auf Seite 132
- Informationen zur Firma von OneLogin Benutzerkonten auf Seite 134

Informationen zur Firma von OneLogin Benutzerkonten

Erfassen Sie die folgenden Stammdaten.

Tabelle 21: Stammdaten zur Identifikation

Eigenschaft	Beschreibung
Firma	Firma der Identität.
Abteilung	Abteilung der Identität.

Verwandte Themen

- Allgemeine Stammdaten für OneLogin Benutzerkonten auf Seite 128
- Anmeldeinformationen für OneLogin Benutzerkonten auf Seite 132
- Informationen zum Verzeichnis für OneLogin Benutzerkonten auf Seite 133

Benutzerdefinierte Felder für OneLogin Benutzerkonten ändern

Mit dieser Aufgabe können Sie die Werte der benutzerdefinierten Felder für ein Benutzerkonto ändern.

Um die benutzerdefinierten Felder für ein Benutzerkonto zu ändern

1. Wählen Sie im Manager die Kategorie **OneLogin > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **OneLogin benutzerdefinierte Felder**.
5. Wählen Sie das benutzerdefinierte Feld und erfassen Sie in der Spalte **Wert** den neuen Wert der Eigenschaft.
6. Speichern Sie die Änderungen.

Verwandte Themen

- OneLogin benutzerdefinierte Felder auf Seite 152

Administratoren für OneLogin Rollen festlegen

Für die Verwaltung von Rollen können Sie Administratoren festlegen.

Um einen Administrator für Rollen festzulegen

1. Wählen Sie im Manager die Kategorie **OneLogin > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Administration von Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Rollenadministratoren festlegen auf Seite 144

Authentifizierungsmethoden an OneLogin Benutzerkonten zuweisen

Sie können Authentifizierungsmethoden an Benutzerkonten zuweisen.

Um Authentifizierungsmethoden an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Authentifizierungsmethoden zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Authentifizierungsmethoden zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- OneLogin Authentifizierungsmethoden auf Seite 146
- OneLogin Benutzerkonten an Authentifizierungsmethoden zuweisen auf Seite 146

Privilegien an OneLogin Benutzerkonten zuweisen

Privilegien definieren, worauf ein Benutzer in seiner OneLogin-Instanz zugreifen kann. Sie können Privilegien an Benutzerkonten zuweisen.

Um Privilegien an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Privilegien zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Privilegien zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- OneLogin Privilegien auf Seite 151
- OneLogin Benutzerkonten an Privilegien zuweisen auf Seite 151

Zusatzeigenschaften an OneLogin Benutzerkonten zuweisen

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

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

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

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

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

   Um eine Zuweisung zu entfernen

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

OneLogin Benutzerkonten löschen und wiederherstellen

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

Ein Benutzerkonto, das nicht über eine Kontendefinition entstanden ist, löschen Sie im Manager über die Ergebnisliste oder über die Menüleiste. Nach Bestätigung der Sicherheitsabfrage wird das Benutzerkonto im One Identity Manager zunächst zum Löschen markiert. Das Benutzerkonto wird im One Identity Manager gesperrt und je nach Einstellung der Löschverzögerung endgültig aus der One Identity Manager-Datenbank und aus dem Zielsystem gelöscht.

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

Um ein Benutzerkonto zu löschen, das nicht über eine Kontendefinition verwaltet wird

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

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie im Manager die Kategorie **OneLogin > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste .

Verwandte Themen

- Löschverzögerung für OneLogin Benutzerkonten festlegen auf Seite 88

Überblick über OneLogin Benutzerkonten anzeigen

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

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie im Manager die Kategorie **OneLogin > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das OneLogin Benutzerkonto**.

OneLogin Anwendungen

Anwendungen darf ein Benutzer verwenden, wenn er über eine Rollenmitgliedschaft die Erlaubnis dazu zugeordnet bekommen hat. Anwendungen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können einzelne Stammdaten der Anwendungen bearbeiten. Neue Anwendungen können Sie im One Identity Manager nicht erstellen.

Detaillierte Informationen zum Thema

- Stammdaten für OneLogin Anwendungen bearbeiten auf Seite 139
- Allgemeine Stammdaten für OneLogin Anwendungen auf Seite 139

- OneLogin Rollen an OneLogin Anwendungen zuweisen auf Seite 140
- Zusatzeigenschaften an OneLogin Anwendungen zuweisen auf Seite 141
- Überblick über OneLogin Anwendungen anzeigen auf Seite 141
- Einzelobjekte synchronisieren auf Seite 44

Stammdaten für OneLogin Anwendungen bearbeiten

Anwendungen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können vorhandene Anwendungen im One Identity Manager bearbeiten.

Um die Stammdaten einer Anwendung zu bearbeiten

1. Wählen Sie im Manager die Kategorie **OneLogin > Anwendungen**.
2. Wählen Sie in der Ergebnisliste die Anwendung.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Anwendung.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für OneLogin Anwendungen auf Seite 139

Allgemeine Stammdaten für OneLogin Anwendungen

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 22: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Anzeigename	Name zur Anzeige der Anwendung in der Benutzeroberfläche der One Identity Manager-Werkzeuge.
Authentifizierungsmethode	Authentifizierungsmethode der Anwendung.
Eindeutige Kennung	Unikale ID, unter der die Anwendung durch OneLogin verwaltet wird.
Domäne	Domäne der Anwendung.

Eigenschaft	Beschreibung
Richtlinie	Zulässige Richtlinie für die Anwendung.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Anwendung an Benutzerkonten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Notizen	Freitextfeld für zusätzliche Erläuterungen.
Sichtbar	Gibt an, ob die Anwendung im OneLogin-Portal sichtbar ist.
Provisionierung aktiviert	Gibt an, ob für diese Anwendung die Provisionierung aktiviert ist.

Verwandte Themen

- OneLogin Richtlinien auf Seite 149

OneLogin Rollen an OneLogin Anwendungen zuweisen

Weisen Sie Rollen an Anwendungen zu. Damit erhalten die Benutzerkonten dieser Rollen die Berechtigung, die Anwendungen zu nutzen.

Um Rollen an eine Anwendung zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Anwendungen**.
2. Wählen Sie in der Ergebnisliste die Anwendung.
3. Wählen Sie die Aufgabe **Rollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Rollen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- OneLogin Anwendungen an OneLogin Rollen zuweisen auf Seite 144

Zusatzeigenschaften an OneLogin Anwendungen zuweisen

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

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

Um Zusatzeigenschaften für eine Anwendung festzulegen

1. Wählen Sie im Manager die Kategorie **OneLogin > Anwendungen**.
2. Wählen Sie in der Ergebnisliste die Anwendung.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

Überblick über OneLogin Anwendungen anzeigen

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

Um einen Überblick über eine Anwendung zu erhalten

1. Wählen Sie im Manager die Kategorie **OneLogin > Anwendungen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die OneLogin Anwendungen**.

OneLogin Rollen

In einer OneLogin Domäne können Benutzerkonten in Rollen zusammengefasst werden, mit denen der Zugriff auf OneLogin Anwendungen geregelt werden kann. Rollen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie können einzelne Stammdaten der Rollen bearbeiten. Neue Rollen können Sie im One Identity Manager nicht erstellen.

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

Detaillierte Informationen zum Thema

- Managen von Mitgliedschaften in OneLogin Rollen auf Seite 89
- Stammdaten für OneLogin Rollen bearbeiten auf Seite 142
- Allgemeine Stammdaten für OneLogin Rollen auf Seite 143
- Rollenadministratoren festlegen auf Seite 144
- OneLogin Anwendungen an OneLogin Rollen zuweisen auf Seite 144
- Zusatzeigenschaften an OneLogin Rollen zuweisen auf Seite 145
- Überblick über OneLogin Rollen anzeigen auf Seite 145
- Einzelobjekte synchronisieren auf Seite 44

Stammdaten für OneLogin Rollen bearbeiten

Sie können vorhandene Rollen im One Identity Manager bearbeiten.

Um die Stammdaten einer Rolle zu bearbeiten

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Rolle.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Allgemeine Stammdaten für OneLogin Rollen auf Seite 143

Allgemeine Stammdaten für OneLogin Rollen

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 23: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Anzeigename	Name zur Anzeige der Rolle in der Benutzeroberfläche der One Identity Manager-Werkzeuge.
Eindeutige Kennung	Unikale ID, unter der die Rolle durch OneLogin verwaltet wird.
Domäne	Domäne der Rolle.
IT Shop	Gibt an, ob die Rolle über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Rolle über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Rolle kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Rolle ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Rolle über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Rolle an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Leistungsposition	Leistungsposition, um die Rolle über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Rolle an Benutzerkonten. Stellen Sie einen Wert im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Rollen. Rollen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Rollen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.

Verwandte Themen

- Vererbung von OneLogin Rollen anhand von Kategorien auf Seite 101
- Ausführliche Informationen zur Vorbereitung der Rollen für die Bestellung über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Rollenadministratoren festlegen

Für die Verwaltung von Rollen können Sie Administratoren festlegen.

Um Administratoren für eine Rolle festzulegen

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Administratoren zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Administratoren zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie den Administrator und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- Administratoren für OneLogin Rollen festlegen auf Seite 135

OneLogin Anwendungen an OneLogin Rollen zuweisen

Weisen Sie Rollen an Anwendungen zu. Damit erhalten die Benutzerkonten dieser Rollen die Berechtigung, die Anwendungen zu nutzen.

Um Anwendungen an eine Rolle zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Anwendungen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Anwendungen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- OneLogin Rollen an OneLogin Anwendungen zuweisen auf Seite 140

Zusatzeigenschaften an OneLogin Rollen zuweisen

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

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

Um Zusatzeigenschaften für eine Rolle festzulegen

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen**.
2. Wählen Sie in der Ergebnisliste die Rolle.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

Überblick über OneLogin Rollen anzeigen

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

Um einen Überblick über eine Rolle zu erhalten

1. Wählen Sie im Manager die Kategorie **OneLogin > Rollen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die OneLogin Rollen**.

OneLogin Authentifizierungsmethoden

OneLogin Authentifizierungsmethoden werden durch die Synchronisation in den One Identity Manager eingelesen. OneLogin Authentifizierungsmethoden können Sie im One Identity Manager nicht bearbeiten.

Um Informationen zu einer OneLogin Authentifizierungsmethode anzuzeigen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen > <Ihre Domäne> > Authentifizierungsmethoden**.
2. Wählen Sie in der Ergebnisliste die Authentifizierungsmethode.
3. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über die OneLogin Authentifizierungsmethode**: Sie erhalten einen Überblick über die OneLogin Authentifizierungsmethode und ihre Abhängigkeiten.
    - **Stammdaten bearbeiten**: Es werden die Stammdaten für die OneLogin Authentifizierungsmethode angezeigt. Sie können die Stammdaten nicht bearbeiten.
        - **Anzeigename**: Anzeigename der Authentifizierungsmethode.
        - **Bezeichnung**: Name der Authentifizierungsmethode, wie er den Administratoren in OneLogin angezeigt wird.
        - **Eindeutige Kennung**: Unikale ID, unter der die Authentifizierungsmethode durch OneLogin verwaltet wird.
        - **Domäne**: Domäne, zu der die Authentifizierungsmethode gehört.
    - **Benutzerkonten zuweisen**: Weisen Sie die Authentifizierungsmethode an Benutzerkonten zu.

Verwandte Themen

- OneLogin Benutzerkonten an Authentifizierungsmethoden zuweisen auf Seite 146
- Authentifizierungsmethoden an OneLogin Benutzerkonten zuweisen auf Seite 135
- Einzelobjekte synchronisieren auf Seite 44

OneLogin Benutzerkonten an Authentifizierungsmethoden zuweisen

Sie können Authentifizierungsmethoden an Benutzerkonten zuweisen.

Um Benutzerkonten an eine Authentifizierungsmethode zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen > <Ihre Domäne> > Authentifizierungsmethoden**.
2. Wählen Sie in der Ergebnisliste die Authentifizierungsmethode.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- OneLogin Authentifizierungsmethoden auf Seite 146
- Authentifizierungsmethoden an OneLogin Benutzerkonten zuweisen auf Seite 135

OneLogin Dienstanbieter

OneLogin Dienstanbieter werden durch die Synchronisation in den One Identity Manager eingelesen. OneLogin Dienstanbieter können Sie im One Identity Manager nicht bearbeiten.

Um Informationen zu einer OneLogin Dienstanbieter anzuzeigen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen > <Ihre Domäne> > Dienstanbieter**.
2. Wählen Sie in der Ergebnisliste die Dienstanbieter.
3. Wählen Sie eine der folgenden Aufgaben:
   - **Überblick über die OneLogin Dienstanbieter**: Sie erhalten einen Überblick über den OneLogin Dienstanbieter und seine Abhängigkeiten.
   - **Stammdaten bearbeiten**: Es werden die Stammdaten für den OneLogin Dienstanbieter angezeigt. Sie können die Stammdaten nicht bearbeiten.
     - **Anzeigename**: Anzeigename des Dienstanbieters.
     - **Eindeutige Kennung**: Unikale ID, unter der der Dienstanbieter durch OneLogin verwaltet wird.
     - **Domäne**: Domäne, zu der der Dienstanbieter gehört.

- **URL**: Bezeichner, der es eingehenden Anfragen ermöglicht, auf diesen Dienstanbieter zu verweisen.
- **Ablauf des Zugriffstoken [min]**: Die Anzahl der Minuten bis zum Ablauf des Zugriffstokens.
- **Ablauf des Aktualisierungstoken [min]**: Die Anzahl der Minuten bis zum Ablauf des Aktualisierungstokens.
- **Beschreibung**: Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- OneLogin Clients auf Seite 148
- OneLogin Scopes auf Seite 149
- Einzelobjekte synchronisieren auf Seite 44

OneLogin Clients

OneLogin Clients werden durch die Synchronisation in den One Identity Manager eingelesen. Es handelt sich um OpenID Anwendungen, die über einen OneLogin Dienstanbieter Token erstellen können. OneLogin Clients können Sie im One Identity Manager nicht bearbeiten.

Um Informationen zu einem OneLogin Client anzuzeigen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen > <Ihre Domäne> > Clients**.
2. Wählen Sie in der Ergebnisliste den Client.
3. Wählen Sie eine der folgenden Aufgaben:
   - **Überblick über den OneLogin Client**: Sie erhalten einen Überblick über den OneLogin Client und seine Abhängigkeiten.
   - **Stammdaten bearbeiten**: Es werden die Stammdaten für den OneLogin Client angezeigt. Sie können die Stammdaten nicht bearbeiten.
     - **Anzeigename**: Anzeigename des Clients.
     - **Eindeutige Kennung**: Unikale ID, unter der der Client durch OneLogin verwaltet wird.
     - **Domäne**: Domäne, zu der der Client gehört.
     - **Dienstanbieter**: Dienstanbieter, für den der Client definiert ist.

Verwandte Themen

- OneLogin Dienstanbieter auf Seite 147
- Einzelobjekte synchronisieren auf Seite 44

OneLogin Scopes

Mit Hilfe von Scopes können Administratoren festlegen, welche Aktionen ein Benutzer über einen Dienstanbieter durchführen kann. OneLogin Scopes werden durch die Synchronisation in den One Identity Manager eingelesen. OneLogin Scopes können Sie im One Identity Manager nicht bearbeiten.

Um Informationen zu einem Scope anzuzeigen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen > <Ihre Domäne> > Scopes**.
2. Wählen Sie in der Ergebnisliste den Scope.
3. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über den OneLogin Scope**: Sie erhalten einen Überblick über den OneLogin Scope und seine Abhängigkeiten.
    - **Stammdaten bearbeiten**: Es werden die Stammdaten für den OneLogin Scope angezeigt. Sie können die Stammdaten nicht bearbeiten.
        - **Eindeutige Kennung**: Unikale ID, unter der der Scope durch OneLogin verwaltet wird.
        - **Domäne**: Domäne, zu der der Scope gehört.
        - **Dienstanbieter**: Dienstanbieter, für den der Scope definiert ist.
        - **Scope**: Aktion, die ausgeführt werden kann.
        - **Beschreibung**: Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- OneLogin Dienstanbieter auf Seite 147
- Einzelobjekte synchronisieren auf Seite 44

OneLogin Richtlinien

OneLogin Richtlinien für Benutzer und Anwendungen werden durch die Synchronisation in den One Identity Manager eingelesen. OneLogin Richtlinien können Sie im One Identity Manager nicht bearbeiten.

Um Informationen zu einer OneLogin Richtlinie anzuzeigen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen > <Ihre Domäne> > Richtlinien**.
2. Wählen Sie in der Ergebnisliste die Richtlinie.
3. Wählen Sie eine der folgenden Aufgaben:

- **Überblick über die OneLogin Richtlinie**: Sie erhalten einen Überblick über die OneLogin Richtlinie und ihre Abhängigkeiten.
- **Stammdaten bearbeiten**: Es werden die Stammdaten für die OneLogin Richtlinie angezeigt. Sie können die Stammdaten nicht bearbeiten.
    - **Anzeigename**: Anzeigename der Richtlinie.
    - **Eindeutige Kennung**: Unikale ID, unter der die Richtlinie durch OneLogin verwaltet wird.
    - **Domäne**: Domäne, zu der die Richtlinie gehört.

Verwandte Themen

- Allgemeine Stammdaten für OneLogin Anwendungen auf Seite 139
- OneLogin Gruppen auf Seite 150
- Einzelobjekte synchronisieren auf Seite 44

OneLogin Gruppen

Über OneLogin Gruppen können beispielsweise OneLogin Richtlinien auf die Benutzerkonten der Gruppen angewendet werden. OneLogin Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. OneLogin Gruppen können Sie im One Identity Manager nicht bearbeiten.

Um Informationen zu einer OneLogin Gruppe anzuzeigen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen > <Ihre Domäne> > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über die OneLogin Gruppe**: Sie erhalten einen Überblick über die OneLogin Gruppe und ihre Abhängigkeiten.
    - **Stammdaten bearbeiten**: Es werden die Stammdaten für die OneLogin Gruppe angezeigt. Sie können die Stammdaten nicht bearbeiten.
        - **Anzeigename**: Anzeigename der Gruppe.
        - **Eindeutige Kennung**: Unikale ID, unter der die Gruppe durch OneLogin verwaltet wird.
        - **Domäne**: Domäne, zu der die Gruppe gehört.

Verwandte Themen

- OneLogin Richtlinien auf Seite 149
- Einzelobjekte synchronisieren auf Seite 44

OneLogin Privilegien

Für Privilegien sind zusätzliche Konfigurationen am Synchronisationsprojekt erforderlich. Weitere Informationen finden Sie unter Synchronisationsprojekt für OneLogin Privilegien anpassen auf Seite 31.

Privilegien definieren, worauf ein Benutzer in seiner OneLogin-Instanz zugreifen kann. Im Wesentlichen handelt es sich dabei um die administrative Berechtigungen für einen einzelnen Benutzer. OneLogin Privilegien werden durch die Synchronisation in den One Identity Manager eingelesen. OneLogin Privilegien können Sie im One Identity Manager nicht bearbeiten.

Um Informationen zu einem OneLogin Privileg anzuzeigen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen > <Ihre Domäne> > Privilegien**.
2. Wählen Sie in der Ergebnisliste das Privileg.
3. Wählen Sie eine der folgenden Aufgaben:
    - **Überblick über das OneLogin Privileg**: Sie erhalten einen Überblick über das OneLogin Privileg und seine Abhängigkeiten.
    - **Stammdaten bearbeiten**: Es werden die Stammdaten für das OneLogin Privileg angezeigt. Sie können die Stammdaten nicht bearbeiten.
        - **Anzeigename**: Anzeigename des Privilegs.
        - **Eindeutige Kennung**: Unikale ID, unter der das Privileg durch OneLogin verwaltet wird.
        - **Domäne**: Domäne, zu der das Privileg gehört.
        - **Beschreibung**: Freitextfeld für zusätzliche Erläuterungen.
    - **Benutzerkonten zuweisen**: Weisen Sie das Privileg an Benutzerkonten zu.

Verwandte Themen

- OneLogin Benutzerkonten an Privilegien zuweisen auf Seite 151
- Privilegien an OneLogin Benutzerkonten zuweisen auf Seite 136
- Einzelobjekte synchronisieren auf Seite 44

OneLogin Benutzerkonten an Privilegien zuweisen

Privilegien definieren, worauf ein Benutzer in seiner OneLogin-Instanz zugreifen kann. Sie können Privilegien an Benutzerkonten zuweisen.

Um Benutzerkonten an ein Privileg zuzuweisen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen > <Ihre Domäne> > Privilegien**.
2. Wählen Sie in der Ergebnisliste das Privileg.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- OneLogin Privilegien auf Seite 151
- Privilegien an OneLogin Benutzerkonten zuweisen auf Seite 136

OneLogin benutzerdefinierte Felder

OneLogin benutzerdefinierte Felder werden durch die Synchronisation in den One Identity Manager eingelesen. Benutzerdefinierte Felder können Sie im One Identity Manager erstellen und bearbeiten.

Um Informationen zu einem benutzerdefinierten Feld anzuzeigen

1. Wählen Sie im Manager die Kategorie **OneLogin > Domänen > <Ihre Domäne> > Benutzerdefinierte Felder**.
2. Wählen Sie in der Ergebnisliste das benutzerdefinierte Feld.
3. Wählen Sie eine der folgenden Aufgaben:
   - **Überblick über das OneLogin benutzerdefinierte Feld**: Sie erhalten einen Überblick über das OneLogin benutzerdefinierte Feld und seine Abhängigkeiten.
   - **Stammdaten bearbeiten**: Es werden die Stammdaten für das OneLogin benutzerdefinierte Feld angezeigt. Sie können die Stammdaten nicht bearbeiten.
     - **Bezeichnung**: Bezeichnung des benutzerdefinierten Feldes.
     - **Domäne**: Domäne, zu der das benutzerdefinierte Feld gehört.

Verwandte Themen

- Benutzerdefinierte Felder für OneLogin Benutzerkonten ändern auf Seite 134
- Einzelobjekte synchronisieren auf Seite 44

Berichte über OneLogin Objekte

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

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

Tabelle 24: Berichte zur Datenqualität eines Zielsystems

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Herkunft)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die Herkunft der zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Historie)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Rolle Anwendung	Der Bericht ermittelt alle Rollen, in denen sich Identitäten befinden, welche die ausgewählte Systemberechtigung besitzen.
Übersicht anzeigen	Rolle Anwendung	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre Zuweisungen.
Übersicht anzeigen (inklusive Herkunft)	Rolle Anwendung	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der

Bericht	Bereitgestellt für	Beschreibung
		zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	Rolle Anwendung	Der Bericht zeigt einen Überblick über die Systemberechtigung einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Abweichende Systemberechtigungen anzeigen	Domäne	Der Bericht enthält alle Systemberechtigungen, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten anzeigen (inklusive Historie)	Domäne	Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten mit einer überdurchschnittliche Anzahl an Systemberechtigungen anzeigen	Domäne	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
Identitäten mit mehreren Benutzerkonten anzeigen	Domäne	Der Bericht zeigt alle Identitäten, die mehrere Benutzerkonten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Systemberechtigungen anzeigen (inklusive Historie)	Domäne	Der Bericht zeigt die Systemberechtigungen mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum

Bericht	Bereitgestellt für	Beschreibung
		entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Domäne	Der Bericht ermittelt alle Rollen, in denen sich Identitäten befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.
Ungenutzte Benutzerkonten anzeigen	Domäne	Der Bericht enthält alle Benutzerkonten, die in den letzten Monaten nicht verwendet wurden.
Unverbundene Benutzerkonten anzeigen	Domäne	Der Bericht zeigt alle Benutzerkonten, denen keine Identität zugeordnet ist.

Tabelle 25: Zusätzliche Berichte für das Zielsystem

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

Behandeln von OneLogin Objekten im Web Portal

Der One Identity Manager bietet seinen Benutzern die Möglichkeit, verschiedene Aufgaben unkompliziert über ein Web Portal zu erledigen.

- Managen von Benutzerkonten und Identitäten

  Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann die Kontendefinition von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Identität, beispielsweise einen Manager, wird das Benutzerkonto angelegt.

- Managen von Zuweisungen von Rollen

  Mit der Zuweisung von Rollen an ein IT Shop Regal können diese Produkte von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Identität wird die Rolle zugewiesen.

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

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

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

- Attestierung

  Wenn das Modul Attestierung vorhanden ist, kann die Richtigkeit der Eigenschaften von Zielsystemobjekten und von Berechtigungszuweisungen regelmäßig oder auf Anfrage bescheinigt werden. Dafür werden im Manager Attestierungsrichtlinien konfiguriert. Die Attestierer nutzen das Web Portal, um Attestierungsvorgänge zu entscheiden.

- Governance Administration

  Wenn das Modul Complianceregeln vorhanden ist, können Regeln definiert werden, die unzulässige Berechtigungszuweisungen identifizieren und deren Risiken bewerten. Die Regeln werden regelmäßig und bei Änderungen an den Objekten im One Identity Manager überprüft. Complianceregeln werden im Manager definiert. Verantwortliche nutzen das Web Portal, um Regelverletzungen zu überprüfen, aufzulösen und Ausnahmegenehmigungen zu erteilen.

  Wenn das Modul Unternehmensrichtlinien vorhanden ist, können Unternehmensrichtlinien für die im One Identity Manager abgebildeten Zielsystemobjekte definiert und deren Risiken bewertet werden. Unternehmensrichtlinien werden im Manager definiert. Verantwortliche nutzen das Web Portal, um Richtlinienverletzungen zu überprüfen und Ausnahmegenehmigungen zu erteilen.

- Risikobewertung

  Über den Risikoindex von Rollen und Anwendungen kann das Risiko von Zuweisungen für das Unternehmen bewertet werden. Dafür stellt der One Identity Manager Standard-Berechnungsvorschriften bereit. Im Web Portal können die Berechnungsvorschriften modifiziert werden.

- Berichte und Statistiken

  Das Web Portal stellt verschiedene Berichte und Statistiken über die Identitäten, Benutzerkonten, deren Berechtigungen und Risiken bereit.

Ausführliche Informationen zu den genannten Themen finden Sie unter Managen von OneLogin Benutzerkonten und Identitäten auf Seite 52 und Managen von Mitgliedschaften in OneLogin Rollen auf Seite 89 und in folgenden Handbüchern:

- *One Identity Manager Web Designer Web Portal Anwenderhandbuch*
- *One Identity Manager Administrationshandbuch für Attestierungen*
- *One Identity Manager Administrationshandbuch für Complianceregeln*
- *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien*
- *One Identity Manager Administrationshandbuch für Risikobewertungen*

Basisdaten für OneLogin Domänen

Für die Verwaltung einer OneLogin Domäne im One Identity Manager sind folgende Basisdaten relevant.

- Kontendefinitionen

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

  Weitere Informationen finden Sie unter Kontendefinitionen für OneLogin Benutzerkonten auf Seite 53.

- Kennwortrichtlinien

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

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

  Weitere Informationen finden Sie unter Kennwortrichtlinien für OneLogin Benutzerkonten auf Seite 106.

- Initiales Kennwort für neue Benutzerkonten

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

  Weitere Informationen finden Sie unter Initiales Kennwort für neue OneLogin Benutzerkonten auf Seite 118.

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

  Bei Erstellung eines neuen Benutzerkontos werden die Anmeldeinformationen an definierte Empfänger versendet. Dabei werden zwei Benachrichtigungen versendet,

die den Benutzernamen und das initiale Kennwort enthalten. Zur Erzeugung der Benachrichtigungen werden Mailvorlagen genutzt.

Weitere Informationen finden Sie unter E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 119.

- Zielsystemtypen

  Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können. Es werden Einstellungen für die Provisionierung von Mitgliedschaften und die Einzelobjektsynchronisation vorgenommen. Zusätzlich dient der Zielsystemtyp zur Abbildung der Objekte im Unified Namespace.

  Weitere Informationen finden Sie unter Ausstehende Objekte nachbehandeln auf Seite 45.

- Zielsystemverantwortliche

  Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie der Anwendungsrolle die Identitäten zu, die berechtigt sind, OneLogin Objekte zu bearbeiten.

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

  Weitere Informationen finden Sie unter Zielsystemverantwortliche für OneLogin auf Seite 159.

- Server

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

  Weitere Informationen finden Sie unter Jobserver für OneLogin-spezifische Prozessverarbeitung auf Seite 162.

Zielsystemverantwortliche für OneLogin

Im One Identity Manager ist eine Standardanwendungsrolle für die Zielsystemverantwortlichen vorhanden. Weisen Sie der Anwendungsrolle die Identitäten zu, die berechtigt sind, OneLogin Objekte zu bearbeiten.

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

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

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

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

Tabelle 26: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | OneLogin** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Rollen zur Aufnahme in den IT Shop vor • Können Identitäten anlegen, die nicht den Identitätstyp **Primäre Identität** haben. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Identitäten als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Identitäten als Zielsystemadministrator festzulegen

1. Melden Sie sich als One Identity Manager Administrator (Anwendungsrolle **Basisrollen | Administratoren**) am Manager an.
2. Wählen Sie die Kategorie **One Identity Manager Administration > Zielsysteme > Administratoren**.

3. Wählen Sie die Aufgabe **Identitäten zuweisen**.
4. Weisen Sie die Identität zu und speichern Sie die Änderung.

Um initial Identitäten in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

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

Um als Zielsystemverantwortlicher weitere Identitäten als Zielsystemverantwortliche zu berechtigen

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

Um Zielsystemverantwortliche für einzelne Domänen festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **OneLogin > Domänen**.
3. Wählen Sie in der Ergebnisliste die Domäne.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Zielsystemverantwortliche** die Anwendungsrolle.

   - ODER -

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

   a. Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | OneLogin** zu.

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

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer OneLogin Domäne auf Seite 9
- Allgemeine Stammdaten für OneLogin Domänen auf Seite 123

Jobserver für OneLogin-spezifische Prozessverarbeitung

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

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

- Erstellen Sie im Designer in der Kategorie **Basisdaten > Installationen > Jobserver** einen Eintrag für den Jobserver. Ausführliche Informationen dazu finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Wählen Sie im Manager in der Kategorie **OneLogin > 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 **OneLogin > Basisdaten zur Konfiguration > Server**.
2. Wählen Sie in der Ergebnisliste den Jobserver-Eintrag.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für den Jobserver.
5. Wählen Sie die Aufgabe **Serverfunktionen zuweisen** und legen Sie die Serverfunktionen fest.
6. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Jobservers auf Seite 163
- Serverfunktionen eines Jobservers auf Seite 165

Allgemeine 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 27: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS-Syntax. Syntax: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Zielsystem	Zielsystem des Computerkontos.
Sprache	Sprache des Servers.
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme `Robocopy` und `rsync` unterstützt. Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm `Robocopy` und zwischen Servern mit einem Linux Betriebssystem mit dem Programm `rsync`. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt,

Eigenschaft	Bedeutung
	das beide Server unterstützen.
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Mit dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	Gibt an, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur `QBM_PJobQueueLoad` aktiviert, sobald die Queue das erste Mal angefragt wird.

Eigenschaft	Bedeutung
	Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Gibt an, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Berechtigungen im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Pausiert wegen Nichtverfügbarkeit eines Zielsystems	Gibt an, ob die Verarbeitung von Aufträgen für diese Queue angehalten wurde, weil das Zielsystem, für den dieser Jobserver der Synchronisationsserver ist, vorübergehend nicht erreichbar ist. Sobald das Zielsystem wieder erreichbar ist, wird die Verarbeitung gestartet und alle anstehenden Aufträge werden ausgeführt. Ausführliche Informationen zum Offline-Modus finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
Kein automatisches Softwareupdate	Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Gibt an, ob gerade eine Softwareaktualisierung ausgeführt wird.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Serverfunktionen eines Jobservers auf Seite 165

Serverfunktionen eines Jobservers

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

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

Tabelle 28: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
CSV Konnektor	Server, auf dem der CSV Konnektor für die Synchronisation installiert ist.
Domänen-Controller	Active Directory Domänen-Controller. Server, die nicht als Domänen-Controller gekennzeichnet sind, werden als Memberserver betrachtet.
Druckserver	Server, der als Druckserver arbeitet.
Generischer Server	Server für die generische Synchronisation mit einem kundendefinierten Zielsystem.
Homeserver	Server zur Anlage von Homeverzeichnissen für Benutzerkonten.
Aktualisierungsserver	Der Server führt die automatische Softwareaktualisierung aller anderen Server aus. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Der Server kann SQL Aufträge ausführen. Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten.
Generischer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.
One Identity Manager-Datenbankkonnektor	Server, auf dem der One Identity Manager Konnektor

Serverfunktion	Anmerkungen
	installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Manager aus.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
Primärer Domänen-Controller	Primärer Domänen-Controller.
Profilserver	Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten.
SAM Synchronisationsserver	Server für die Synchronisation mit einem SMB-basierten Zielsystem.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtsserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell Konnektor	Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen.
OneLogin Konnektor	Server, auf dem der OneLogin Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem OneLogin aus.

Verwandte Themen

- Allgemeine Stammdaten eines Jobservers auf Seite 163

Anhang A

Konfigurationsparameter für die Verwaltung von OneLogin Domänen

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

Tabelle 29: Konfigurationsparameter

Konfi-gurationsparameter	Beschreibung
TargetSystem | OneLogin	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung OneLogin-basierter Zielsysteme. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
TargetSystem | OneLogin | Accounts	Erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem | OneLogin | Accounts | InitialRandomPassword	Gibt an, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.
TargetSystem | OneLogin | Accounts | InitialRandomPassword | SendTo	Identität, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Rolle, Verantwortlicher der Identität oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter **TargetSystem | OneLogin | DefaultAddress** hinterlegte Adresse versandt.

Konfi-gurationsparameter	Beschreibung
TargetSystem | OneLogin | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Identität - Erstellung neues Benutzerkonto** verwendet.
TargetSystem | OneLogin | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Identität - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem | OneLogin | Accounts | MailTem-plateDefaultValues	Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Identität - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | OneLogin | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | OneLogin | MaxFullsyncDuration	Maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.
TargetSystem | OneLogin | PersonAutoDefault	Modus für die automatische Identitätenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | OneLogin | PersonAutoDisabledAccounts	Gibt an, ob an deaktivierte Benutzerkonten automatisch Identitäten zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | OneLogin | PersonAutoFullSync	Modus für die automatische Identitätenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem | OneLogin | PersonExcludeList	Auflistung aller Benutzerkonten, für die keine automatische Identitätenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird.

Konfigurationsparameter	Beschreibung
	Beispiel: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $`
QER | ITShop | AutoPublish | OLGRole	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der automatischen Übernahme von OneLogin Rollen in den IT Shop. Ist der Parameter aktiviert, werden alle Rollen automatisch als Produkte dem IT Shop zugewiesen. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
QER | ITShop | AutoPublish | OLGRole| ExcludeList	Auflistung aller OneLogin Rollen, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Jeder Eintrag ist Bestandteil eines regulären Suchmusters und unterstützt die Notation für reguläre Ausdrücke. Beispiel: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`

Anhang B

Standardprojektvorlage für OneLogin Domänen

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

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

Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 30: Abbildung der OneLogin Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im OneLogin	Tabelle im One Identity Manager Schema
APIAuthorization	OLGAPIAuthorization
Application	OLGApplication
AuthFactor	OLGAuthFactor
Client	OLGClient, OLGClientHasOLGScope
CustomAttribute	OLGCustomAttribute
Event	OLGEvent
Group	OLGGroup
Policy	OLGPolicy
Privilege	OLGPrivilege
Role	OLGRole
RoleAdmin	OLGUserInOLGRoleAdmin

Schematyp im OneLogin	Tabelle im One Identity Manager Schema
RoleApplication	OLGRoleApplication
Scope	OLGScope
User	OLGUser
UserApplication	OLGUserHasOLGApplication
UserAuthFactor	OLGUserHasOLGAuthFactor
UserCustomAttribute	OLGUserHasOLGCustomAttribute
UserPrivilege	OLGUserHasOLGPrivilege

Anhang C

Verarbeitung von OneLogin Systemobjekten

Folgende Tabelle beschreibt die zulässigen Verarbeitungsmethoden für die Schematypen von OneLogin und benennt notwendige Einschränkungen bei der Verarbeitung der Systemobjekte.

Tabelle 31: Zulässige Verarbeitungsmethoden für Schematypen

Typ	Lesen	Hinzufügen	Löschen	Aktualisieren
Dienstanbieter (`APIAuthorization`)	Ja	Nein	Nein	Nein
Anwendungen (`Application`)	Ja	Nein	Nein	Nein
Authentifizierungsmethoden (`AuthFactor`)	Ja	Nein	Nein	Nein
Clients (`Client`)	Ja	Nein	Nein	Nein
Benutzerdefinierte Felder (`CustomAttribute`)	Ja	Nein	Nein	Nein
Änderungshistorie (`Event`)	Ja	Nein	Nein	Nein
Gruppen (`Group`)	Ja	Nein	Nein	Nein
Richtlinien (`Policy`)	Ja	Nein	Nein	Nein
Privilegien (`Privilege`)	Ja	Nein	Nein	Nein
Rollen (`Role`)	Ja	Nein	Nein	Nein
Administratoren für Rollen (`RoleAdmin`)	Ja	Ja	Ja	Ja
Zuweisungen von Rollen an Anwendungen (`RoleApplication`)	Ja	Ja	Ja	Ja
Scopes (`Scope`)	Ja	Nein	Nein	Nein

Typ	Lesen	Hinzufügen	Löschen	Aktualisieren
Benutzerkonten (`User`)	Ja	Ja	Ja	Ja
Zuweisungen von Anwendungen an Benutzerkonten (`UserApplication`)	Ja	Nein	Nein	Nein
Zuweisungen von Authentifizierungsmethoden an Benutzerkonten (`UserAuthFactor`)	Ja	Ja	Ja	Ja
Zuweisungen von benutzerdefinierten Feldern an Benutzerkonten (`UserCustomAttribute`)	Ja	Nein	Nein	Ja
Zuweisungen von Privilegien an Benutzerkonten (`UserPrivilege`)	Ja	Ja	Ja	Ja

Anhang D

Einstellungen des OneLogin Konnektors

Für die Systemverbindung mit dem OneLogin Konnektor werden die folgenden Einstellungen konfiguriert.

Tabelle 32: Einstellungen des OneLogin Konnektors

Einstellung	Beschreibung
Authentication-URI	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. Variable: `olgauthendpoint`
Client Secret (OAuth)	Sicherheitstoken für die Anmeldung. Variable: `olgauthoauthclientsecret`
Domain	Vollständiger Namen der OneLogin Domäne, beispielsweise **<your domain>.onelogin.com**. Variable: `olgrootdn`
Grant type (OAuth)	Zugangstyp für die Anmeldung. Variable: `olgauthoauthgranttype`
HTTP KeepAlive	Angabe , ob HTTP-Verbindungen aufrecht erhalten werden sollen. Wenn die Option deaktiviert ist, werden Verbindungen sofort geschlossen und können nicht für weitere Anfragen genutzt werden. Standard: **true** Variable: `olgkeepalive`
Max. Parallel Queries	Anzahl der Datenanfragen am Zielsystem, die maximal gleichzeitig ausgeführt werden können. Erfassen Sie einen Wert zwischen **1** und **32**.

Einstellung	Beschreibung
	Standard: **10** Variable: `olgparallelprocesses`
Password (OAuth)	Kennwort für die Anmeldung, wenn der Sicherheitstoken nicht bekannt ist. Variable: `olgauthoauthpassword`
Read events created since	Verwendet für Revisionsfilterung. Variable: `olgeventsincefilter`
Scope (OAuth)	Scope-Parameter, der für die Anmeldung am Zielsystem gültig ist. Wenn mehrere Parameter gültig sind, trennen Sie diese durch Leerzeichen. Variable: `olgauthoauthscope`
Service-URI	URI der API ohne Version. Standard: **api** Variable: `olgroot`
Use Client Side Cache	Angabe, ob der lokale Cache des OneLogin Konnektors genutzt werden soll. 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. 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. Standard: **true** Variable: `olgusecache`
User Name (OAuth)	Benutzername für die Anmeldung, wenn der Sicherheitstoken nicht bekannt ist. Variable: `olgauthoauthusername`
Application/Client ID	Client-ID für die Anwendung.

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

L

O

P

R

S

V

Z