One Identity Manager 8.2.1

Administrationshandbuch für One Identity Active Roles Integration

Copyright 2022 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

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

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

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

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

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

Patente

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

Marken

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

Legende

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

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

One Identity Manager Administrationshandbuch für One Identity Active Roles Integration
Aktualisiert - 27. April 2022, 01:40 Uhr
Version - 8.2.1

Inhalt

1

Integration mit One Identity Active Roles

Der One Identity Manager unterstützt die Anbindung von Active Directory-Umgebungen über einen integrierten Active Roles Konnektor. Zusätzliche Active Directory relevante Funktionalitäten, wie beispielsweise Microsoft Exchange, Office Communication Services oder Active Directory Lightweight Directory Service (AD LDS) werden über diesen Konnektor nicht unterstützt.

Der One Identity Manager ist in der Standardkonfiguration der Prozesse und des Synchronisationsverhaltens das primäre System und arbeitet ohne die Ansteuerung von Active Roles Arbeitsabläufen. Für das Standardverhalten wird ein administratives Benutzerkonto benötigt. Der integrierte Active Roles Konnektor erlaubt jedoch auch die Ansteuerung von Active Roles Arbeitsabläufen. Für diese Funktionalität müssen Sie gegebenenfalls die Prozesse im One Identity Manager benutzerdefiniert anpassen.

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

HINWEIS: Dieses Handbuch geht nur auf die Besonderheiten bei der Verwendung des Active Roles Konnektors ein. Ausführliche Informationen zur Verwaltung einer Active Directory-Umgebung mit dem One Identity Manager finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung*.

Ausführliche Informationen zum Einsatz, Administration und Konfiguration eines Active Roles Servers entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.

Architekturüberblick

Für die Verwaltung einer Active Directory-Umgebung mittels One Identity Manager und Active Roles spielen folgende Server eine Rolle:

- Active Roles Server

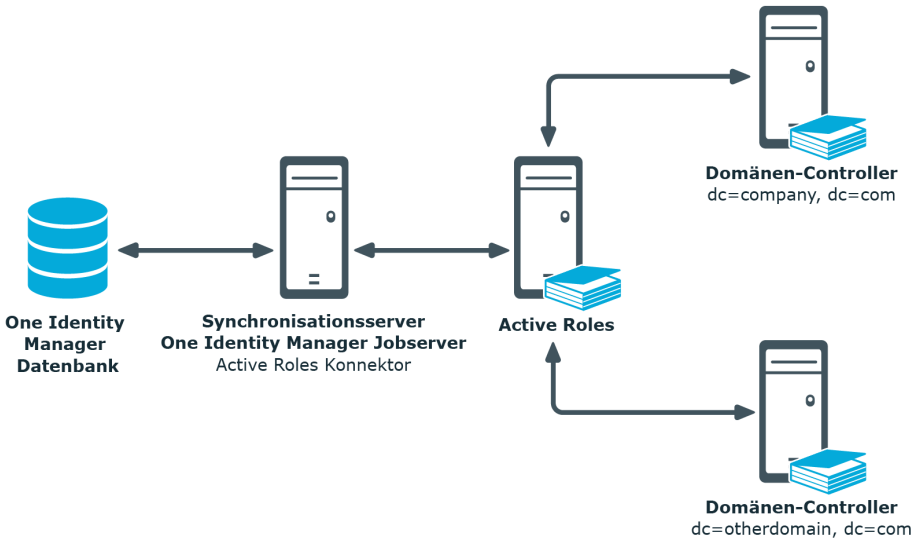
  Active Roles Server, der die Verbindung zum Active Directory Domänen-Controller herstellt. Der Synchronisationsserver verbindet sich gegen diesen Active Roles Server.

- Synchronisationsserver

  Vom Synchronisationsserver wird die Kommunikation des One Identity Manager Service mit Active Roles ausgeführt. Auf diesem Server ist der One Identity Manager Service mit dem Active Roles Konnektor installiert. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Der Synchronisationsserver verbindet sich gegen den Active Roles Server.

Der Active Roles Konnektor des One Identity Manager verwendet das Active Roles ADSI Interface für die Kommunikation mit einer Active Roles Instanz. Der Active Roles Konnektor wird für die Synchronisation und Provisionierung der Active Directory-Umgebung eingesetzt. Der Active Roles Konnektor verbindet sich zu einer Active Roles Instanz, die dann die Verbindung zum Active Directory Domänen-Controller herstellt.

Abbildung 1: Architektur für die Synchronisation



Datenmigration zwischen One Identity Manager und One Identity Active Roles

Szenario

Eine mit Active Roles verwaltete Active Directory Domäne soll mit dem One Identity Manager verwaltet werden. Active Roles Self-Service Manager wird nicht eingesetzt.

Bei der Installation der One Identity Manager-Datenbank wählen Sie eine der folgenden Editionen:

- One Identity Manager Active Directory Edition
- One Identity Manager

Die initiale Synchronisation der Active Directory Domäne mit dem One Identity Manager muss mit dem Active Roles Konnektor erfolgen. Alle weiteren Synchronisationen erfolgen ebenfalls mit dem Active Roles Konnektor.

- Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt unter Verwendung der Standardprojektvorlage für Active Roles.

Szenario

Eine mit Active Roles verwaltete Active Directory Domäne soll mit dem One Identity Manager verwaltet werden. Active Roles Self-Service Manager wird eingesetzt. Die Funktionalität soll in den IT Shop des One Identity Manager überführt werden.

Bei der Installation der One Identity Manager-Datenbank wählen Sie eine der folgenden Editionen:

- One Identity Manager Active Directory Edition
- One Identity Manager

Mit der **One Identity Manager Active Directory Edition** wird die Überführung der Funktionalität von Active Roles Self-Service Manager in den IT Shop des One Identity Manager direkt unterstützt.

Wenn Sie die **One Identity Manager Edition** einsetzen, führen Sie vor der initialen Synchronisation zusätzlich folgende Schritte aus:

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | ADSGroup**.
2. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | ADSGroup | ExcludeList** und legen Sie die Active Directory Gruppen fest, die nicht automatisch in den IT Shop übernommen werden sollen.
3. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | ARS_SSM**.
4. Kompilieren Sie die Datenbank.

Die Synchronisation der Active Directory Domäne mit dem One Identity Manager muss mit dem Active Roles Konnektor erfolgen. Alle weiteren Synchronisationen erfolgen ebenfalls mit dem Active Roles Konnektor.

- Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt unter Verwendung der Standardprojektvorlage für Active Roles.

Szenario

Eine mit dem One Identity Manager verwaltete Active Directory Domäne soll mit Active Roles verwaltet werden. Die Synchronisation der Active Directory Domäne erfolgt bisher

mit dem Active Directory Konnektor.

Um die Active Directory Domäne mit One Identity Active Roles zu verwalten

1. Löschen Sie im Synchronization Editor das bestehende Synchronisationsprojekt.
2. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt unter Verwendung der Standardprojektvorlage für Active Roles.

Detaillierte Informationen zum Thema

- Synchronisieren einer Active Directory-Umgebung über One Identity Active Roles auf Seite 9
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 40

2

Synchronisieren einer Active Directory-Umgebung über One Identity Active Roles

Der One Identity Manager unterstützt die Synchronisation mit Active Roles in den Versionen 7.4.1, 7.4.3, 7.4.4, 7.4.5 und 7.5.

Um die Objekte einer Active Directory-Umgebung initial in die One Identity Manager-Datenbank einzulesen

1. Stellen Sie ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von Active Directory-Umgebungen sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | ADS** aktiviert ist. Die Bestandteile für die Unterstützung von Active Roles sind verfügbar, wenn der Konfigurationsparameter **TargetSystem | ADS | ARS** aktiviert ist.
    - Prüfen Sie im Designer, ob die Konfigurationsparameter aktiviert sind. Anderenfalls aktivieren Sie die 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 der Module 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. Mit der **One Identity Manager Active Directory Edition** wird die Überführung der Funktionalität von Active Roles Self-Service Manager in den IT Shop des One

Identity Manager direkt unterstützt.

Wenn Sie die **One Identity Manager Edition** einsetzen, führen Sie vor der initialen Synchronisation zusätzlich folgende Schritte aus:

a. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | ADSGroup**.

   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*.

b. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | ADSGroup | ExcludeList** und legen Sie die Active Directory Gruppen fest, die nicht automatisch in den IT Shop übernommen werden sollen.

   Beispiel:

   ```
   .*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS
   ```

c. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | ARS_SSM**.

d. Kompilieren Sie die Datenbank.

5. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

TIPP: Bevor Sie die Synchronisation mit einer Active Directory 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

- Datenmigration zwischen One Identity Manager und One Identity Active Roles auf Seite 6
- Benötigte Berechtigungen für die Synchronisation über One Identity Active Roles auf Seite 11
- Einrichten des Synchronisationsservers auf Seite 11
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Active Directory Domäne über One Identity Active Roles auf Seite 16
- Ausführen einer Synchronisation auf Seite 24
- Anpassen einer Synchronisationskonfiguration auf Seite 22
- Aufgaben nach einer Synchronisation auf Seite 28
- Fehleranalyse auf Seite 31
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 40
- Konfigurationsparameter für die Verwaltung einer Active Directory-Umgebung auf Seite 52

Benötigte Berechtigungen für die Synchronisation über One Identity Active Roles

Für die Verbindung zu einer Active Directory-Umgebung über Active Roles wird die Einrichtung eines eigenen Benutzerkontos empfohlen. Zur Einrichtung verwenden Sie die Active Roles Zugriffsvorlagen. Über Zugriffsvorlagen delegieren Sie administrationsrelevante Berechtigungen an ein Active Directory Benutzerkonto ohne jedoch diese Berechtigungen direkt im Active Directory zu erteilen. Weitere Informationen zu Active Roles Zugriffsvorlagen entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.

Folgende Zugriffsvorlagen werden für das Delegieren der Berechtigungen vorgeschlagen:

- All Objects - Read All Properties
- All Objects - Full Control

Der One Identity Manager arbeitet ohne die Ansteuerung von Active Roles Arbeitsabläufen. Um eventuell vorhandene Active Roles Arbeitsabläufe zu umgehen, müssen Sie das Benutzerkonto in die Gruppe der **Active Roles Administratoren** aufnehmen.

Bearbeiten Sie die Active Roles Admins im Active Roles Configuration Center. Sollte es der Fall sein, dass im Active Roles Configuration Center ein Benutzerkonto als Active Roles Admin eingetragen ist, muss dieses Benutzerkonto verwendet werden. Ausführliche Informationen zum Bearbeiten der Gruppe oder des Benutzerkontos für den administrativen Zugriff entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.

Verwandte Themen

- Interaktion mit Active Roles Arbeitsabläufen auf Seite 34

Einrichten des Synchronisationsservers

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

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

Detaillierte Informationen zum Thema

- Systemanforderungen für den Synchronisationsserver auf Seite 12
- One Identity Manager Service mit Active Roles Konnektor installieren auf Seite 13

Systemanforderungen für den Synchronisationsserver

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

- Windows Betriebssystem

  Unterstützt werden die Versionen:

  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- Microsoft .NET Framework Version 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- One Identity Active Roles Management Shell for Active Directory (x64)

  Auf 32-Bit Betriebssystemen ist das Active Roles Management Shell for Active Directory (x86) Paket zu verwenden.

  Die Anleitung zur Installation entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.
- Folgende Pakete müssen vom Active Roles Installationsmedium nachinstalliert werden:

  Auf 32-Bit Betriebssystemen:

  - `<source>\Redistributables\vc_redist.x86.exe`
  - `<source>\Components\ActiveRoles ADSI Provider\ADSI_x86.msi`

  Auf 64-Bit Betriebssystemen:

  - `<source>\Redistributables\vc_redist.x64.exe`
  - `<source>\Components\ActiveRoles ADSI Provider\ADSI_x64.msi`

Weiterhin ist es notwendig, dass vom Jobserver aus Verbindungen über Port **15172** (TCP) zum Active Roles Server möglich sind. Gegebenenfalls muss eine entsprechende Firewall-Regel auf dem Active Roles Server eingerichtet werden.

One Identity Manager Service mit Active Roles Konnektor installieren

HINWEIS: Für bestehende Active Roles Installationen:

Der One Identity Manager Service kann auf einem Server mit Active Roles installiert werden.

Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Active Roles Konnektor installiert sein. Außerdem muss der Synchronisationsserver im One Identity Manager als Jobserver bekannt sein.

Tabelle 1: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	Active Roles Konnektor
Maschinenrolle	Server | Jobserver | Active Directory

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

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

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

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

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

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

Verbindungsinformationen im Designer konfigurieren. Ausführliche Informationen zum Einrichten des Jobservers finden Sie im *One Identity Manager Konfigurationshandbuch*.

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

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

      - ODER -

      Um einen neuen Jobserver zur erstellen, klicken Sie **Hinzufügen**.
   b. Bearbeiten Sie folgende Informationen für den Jobserver.
      - **Server**: Bezeichnung des Jobservers.
      - **Queue**: Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder Jobserver innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
      - **Vollständiger Servername**: Vollständiger Servername gemäß DNS Syntax.

        Syntax:

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

   HINWEIS: Über die Option **Erweitert** können Sie weitere Eigenschaften für den Jobserver bearbeiten. Sie können die Eigenschaften auch zu einem späteren Zeitpunkt mit dem Designer bearbeiten.
4. Auf der Seite **Maschinenrollen** wählen Sie **Active Directory**.
5. Auf der Seite **Serverfunktionen** wählen Sie **Active Roles Konnektor**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

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

- Für eine direkte Verbindung zu Datenbank:
    1. Wählen Sie **Prozessabholung > sqlprovider**
    2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
    3. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
- Für eine Verbindung zum Anwendungsserver:
    1. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
    2. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
    3. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.
    4. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
    5. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Wenn die Datenbank verschlüsselt ist, wählen Sie auf der Seite **Datenbankschlüsseldatei auswählen** die Datei mit dem privaten Schlüssel.
11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
    - **Dienstkonto**: Erfassen Sie die Angaben zum Benutzerkonto unter dem der One Identity Manager Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

    Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen. Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.
12. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

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

13. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

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

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Active Directory Domäne über One Identity Active Roles

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und Active Directory-Umgebung einzurichten. Nachfolgend sind die Schritte für die initiale Einrichtung eines Synchronisationsprojektes beschrieben. Ausführliche Informationen zur Einrichtung der Synchronisation finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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

Verwandte Themen

- Benötigte Informationen für die Erstellung eines Synchronisationsprojektes auf Seite 17
- Initiales Synchronisationsprojekt für eine Active Directory Domäne erstellen auf Seite 19

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

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

Tabelle 2: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Definierter Name der Domäne	Definierter LDAP Name der Domäne.
Benutzerkonto und Kennwort zur Anmeldung am Active Roles	Benutzerkonto und Kennwort zur Anmeldung am Active Roles. Stellen Sie ein Benutzerkonto mit ausreichend Berechtigungen bereit. Weitere Informationen finden Sie unter Benötigte Berechtigungen für die Synchronisation über One Identity Active Roles auf Seite 11.
DNS Name oder IP Adresse des Active Roles Servers	Vollständiger Name oder IP Adresse des Active Roles Servers, gegen den sich der Synchronisationsserver verbindet. Beispiel: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Synchronisationsserver für das Active Directory	Vom Synchronisationsserver werden alle Aktionen des One Identity Manager Service gegen die Zielsystemumgebung ausgeführt. Die für die Synchronisation und Administration mit der One Identity Manager-Datenbank benötigten Einträge werden vom Synchronisationsserver bearbeitet. Auf dem Synchronisationsserver muss der One Identity Manager Service mit demActive Roles Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. • Serverfunktion: **Active Roles Konnektor** • Maschinenrolle: **Server | Jobserver | Active Directory** Weitere Informationen finden Sie unter Systemanforderungen für den Synchronisationsserver auf Seite 12.
Verbindungsdaten zur One Identity Manager-	• Datenbankserver

Angaben	Erläuterungen
Datenbank	• Name der Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
Remoteverbindungsserver	Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden. Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen. Konfiguration des Remoteverbindungsservers: • One Identity Manager Service ist gestartet • **RemoteConnectPlugin** ist installiert • Active Roles Konnektor ist installiert Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software sowie der Berechtigungen des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie lediglich das **RemoteConnectPlugin** zusätzlich installieren. Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Initiales Synchronisationsprojekt für eine Active Directory 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.

Um ein initiales Synchronisationsprojekt für eine Active Directory Domäne über Active Roles einzurichten

1. Starten Sie den Synchronization Editor und melden Sie sich an der One Identity Manager-Datenbank an.
2. Wählen Sie die Startseite. Klicken Sie **Mit einem neuen Synchronisationsprojekt beginnen**.

   Der Projektassistent wird gestartet.
3. Auf der Willkommensseite klicken Sie **Weiter**.
4. Auf der Seite **Zielsystem auswählen** wählen Sie **Active Roles Konnektor**.
5. 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.
6. Auf der Seite **Zielserver** geben den Active Roles Server an, gegen den Sie sich verbinden möchten. Die möglichen Server werden, wenn möglich, automatisch ermittelt.
   - Wählen Sie unter **Hostname/IP Adresse** den Zielserver aus.
   - Kann der Server nicht automatisch ermittelt werden, tragen Sie unter **Hostname/IP Adresse** den DNS Namen oder die IP Adresse des Servers ein.
7. Auf der Seite **Anmeldeinformationen** geben Sie das Benutzerkonto für den Zugriff auf Active Roles an.

- Um das Benutzerkonto des aktuell angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Aktuelle Anmeldedaten verwenden (aktueller Benutzer/Dienstkonto)**. Im Fall der Synchronisation ist dies das Benutzerkonto, unter dem der One Identity Manager Service läuft.
- Um ein definiertes Benutzerkonto zu verwenden, erfassen Sie das Benutzerkonto und das Kennwort zur Anmeldung am Zielsystem.

HINWEIS: Wenn Sie kein definiertes Benutzerkonto angeben, dann wird während der Konfiguration im Synchronization Editor ebenfalls das Benutzerkonto des aktuell angemeldeten Benutzers verwendet.

Das Benutzerkonto, das für den Synchronization Editor verwendet wird, weicht gegebenenfalls vom Benutzerkonto des One Identity Manager Service ab. In diesem Fall wird empfohlen, das **RemoteConnectPlugin** zu verwenden. Damit ist sichergestellt, dass das gleiche Benutzerkonto während Konfiguration im Synchronization Editor als auch im Dienstkontext verwendet wird.

8. Auf der Seite **Auswahl der Domäne/des Wurzeleintrages** wählen Sie die Domäne, die Sie synchronisieren möchten oder tragen Sie den definierten Namen des Wurzeleintrages ein.
9. Auf der Seite **One Identity Manager Verbindung** überprüfen Sie die Verbindungsdaten zur One Identity Manager-Datenbank. Die Daten werden aus der verbundenen Datenbank geladen. Geben Sie das Kennwort erneut ein.

   HINWEIS:
   - Wenn Sie mit einer unverschlüsselten One Identity Manager-Datenbank arbeiten und noch kein Synchronisationsprojekt in der Datenbank gespeichert ist, erfassen Sie alle Verbindungsdaten neu.
   - Wenn bereits ein Synchronisationsprojekt gespeichert ist, wird diese Seite nicht angezeigt.
10. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
11. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

Tabelle 3: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	Gibt an, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager-Datenbank eingerichtet werden soll. Der Synchronisationsworkflow zeigt folgende Besonderheiten: • Die Synchronisationsrichtung ist **In den One Identity Manager**.

Option	Bedeutung
	• 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.

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

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

    a. Klicken Sie , um einen neuen Jobserver anzulegen.

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

    c. Klicken Sie **OK**.

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

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

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

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

    Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

    HINWEIS:

    • Beim Aktivieren wird eine Konsistenzprüfung durchgeführt. Wenn dabei Fehler auftreten, erscheint eine Meldung. Sie können entscheiden, ob das

Synchronisationsprojekt dennoch aktiviert werden soll.

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

- Wenn das Synchronisationsprojekt nicht sofort aktiviert werden soll, deaktivieren Sie die Option **Synchronisationsprojekt speichern und sofort aktivieren**. In diesem Fall speichern Sie das Synchronisationsprojekt manuell vor dem Beenden des Synchronization Editor.
- Die Verbindungsdaten zum Zielsystem werden in einem Variablenset gespeichert und können bei Bedarf im Synchronization Editor in der Kategorie **Konfiguration > Variablen** angepasst werden.

Verwandte Themen

- Benötigte Informationen für die Erstellung eines Synchronisationsprojektes auf Seite 17
- Benötigte Berechtigungen für die Synchronisation über One Identity Active Roles auf Seite 11
- Systemanforderungen für den Synchronisationsserver auf Seite 12
- Standardprojektvorlage für One Identity Active Roles auf Seite 58

Anpassen einer Synchronisationskonfiguration

Ausführliche Informationen zum Anpassen der Synchronisation für eine Active Directory-Umgebung finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung*.

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

Um die Datenbank und die Active Directory-Umgebung regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

- Um bei der Synchronisation den One Identity Manager als primäres System zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um allgemeingültige Synchronisationskonfigurationen zu erstellen, die erst beim Start der Synchronisation die notwendigen Informationen über die zu

synchronisierenden Objekte erhalten, können Variablen eingesetzt werden. Variablen können beispielsweise in den Basisobjekten, den Schemaklassen oder den Verarbeitungsmethoden eingesetzt werden.

- Mit Hilfe von Variablen kann ein Synchronisationsprojekt für die Synchronisation verschiedener Domänen eingerichtet werden. Hinterlegen Sie die Verbindungsparameter zur Anmeldung an den Domänen als Variablen.
- Um festzulegen, welche Active Directory Objekte und Datenbankobjekte bei der Synchronisation behandelt werden, bearbeiten Sie den Scope der Zielsystemverbindung und der One Identity Manager-Datenbankverbindung. Um Dateninkonsistenzen zu vermeiden, definieren Sie in beiden Systemen den gleichen Scope. Ist kein Scope definiert, werden alle Objekte synchronisiert.
- Wenn sich das One Identity Manager Schema oder das Zielsystemschema geändert hat, aktualisieren Sie das Schema im Synchronisationsprojekt. Anschließend können Sie die Änderungen in das Mapping aufnehmen.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.

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

Verwandte Themen

- Beschleunigung der Provisionierung und Einzelobjektsynchronisation auf Seite 23

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 **Active Roles Konnektor** zu.

   Alle Jobserver müssen auf die gleiche Active Directory 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*.

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 25
- Synchronisation deaktivieren auf Seite 26
- Synchronisationsergebnisse anzeigen auf Seite 27

Synchronisationen starten

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

Um regelmäßige Synchronisationen auszuführen

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

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

Um die initiale Synchronisation manuell zu starten

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

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

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus **Frozen**. Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.

- Stellen Sie sicher, dass Startkonfigurationen, die in Startfolgen verwendet werden, nicht gleichzeitig einzeln gestartet werden. Weisen Sie den Startfolgen und Startkonfigurationen unterschiedliche Zeitpläne zu.

- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Legen Sie an den Startkonfigurationen fest, wie sich der One Identity Manager in diesem Fall verhalten soll.
  - Stellen Sie über den Zeitplan sicher, dass die Startkonfigurationen nacheinander ausgeführt werden.
  - Gruppieren Sie die Startkonfigurationen mit gleichem Startverhalten.

Synchronisation deaktivieren

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

Um regelmäßige Synchronisationen zu verhindern

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

   Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Verwandte Themen

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Active Directory Domäne über One Identity Active Roles auf Seite 16

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.

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.

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:

- Ausstehender Objekte nachbehandeln auf Seite 28
- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 30
- Active Directory Benutzerkonten und Active Directory Kontakte über Kontendefinitionen verwalten auf Seite 31

Ausstehender 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 **Active Directory > Zielsystemabgleich: Active Directory**.

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

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

   - Das Synchronisationsprotokoll wurde bereits gelöscht.

     - ODER -

   - Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.

Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.

- Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.

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

TIPP:

Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

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

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

Tabelle 4: 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.

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

Verwandte Themen

- Ausstehender Objekte nachbehandeln auf Seite 28

Active Directory Benutzerkonten und Active Directory Kontakte über Kontendefinitionen verwalten

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

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

Um die Benutzerkonten und Kontakte 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 **Active Directory > Benutzerkonten > Verbunden aber nicht konfiguriert > <Domäne>**.

       - ODER -

       Wählen Sie im Manager die Kategorie **Active Directory > Kontakte > 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.

Ausführliche Informationen zu Kontendefinitionen für Active Directory Benutzerkonten und Kontakte finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung*.

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 27

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.

3

Interaktion mit Active Roles Arbeitsabläufen

In der Standardkonfiguration der Prozesse und des Synchronisationsverhaltens arbeitet der integrierte Active Roles Konnektor ohne die Ansteuerung von Active Roles Arbeitsabläufen. Änderungen werden sofort in die Active Directory-Umgebung publiziert. Für das Standardverhalten wird ein administratives Benutzerkonto benötigt, das Mitglied in der Gruppe der Active Roles Administratoren ist.

Der im One Identity Manager integrierte Active Roles Konnektor erlaubt jedoch auch die Ansteuerung von Active Roles Arbeitsabläufen. Das bedeutet, dass für jede Operation, in Active Roles die mit einem Arbeitsablauf verbunden ist, dieser Arbeitsablauf ausgelöst wird.

Wenn der Active Roles Konnektor Arbeitsabläufe auslösen soll, dann müssen Sie gegebenenfalls die Prozesse benutzerdefiniert so anpassen, dass die Prozesse auf die Ausführung der Arbeitsabläufe und somit die Ausführung der erwünschten Änderungen im Active Directory warten. Dies ist erforderlich, da die im One Identity Manager definierten Active Directory Prozesse synchron ausgeführt werden. Um Sie bei der Abfrage der möglichen Status der Arbeitsabläufe zu unterstützen, enthält der Active Roles Konnektor zusätzliche Funktionen.

Ob Arbeitsabläufe angesteuert werden, ist abhängig der Konfiguration der Domäne und den Berechtigungen des One Identity Manager Service Benutzerkontos.

> HINWEIS: Ist das Benutzerkonto des One Identity Manager Services Mitglied in der Gruppe der Active Roles Administratoren werden Arbeitsabläufe unabhängig von der Option immer umgangen.

Informationen zu Active Roles Arbeitsabläufen entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.

Die nachfolgende Tabelle zeigt die Zusammenhänge.

Tabelle 5: Zusammenhänge zur Ansteuerung von Active Roles Arbeitsabläufen

Das Benutzerkonto ist Mitglied der Active Roles Administratoren?	Die Option "Active Roles Arbeitsabläufe ausführen" ist gesetzt?	Die Operation ist mit Active Roles Arbeitsabläufen verbunden?	Ergebnis
Ja	Ja	Nein	Die Operation wird sofort ausgeführt.
Ja	Nein	Nein	Die Operation wird sofort ausgeführt.
Ja	Ja	Ja	Die Operation wird sofort ohne Ansteuerung der Arbeitsabläufe ausgeführt.
Ja	Nein	Ja	Die Operation wird sofort ohne Ansteuerung der Arbeitsabläufe ausgeführt.
Nein	Ja	Nein	Die Operation wird sofort ausgeführt.
Nein	Nein	Nein	Die Operation wird sofort ausgeführt.
Nein	Ja	Ja	Die Operation löst die Arbeitsabläufe aus und wird abhängig vom finalen Status ausgeführt.
Nein	Nein	Ja	Die Operation wird abgebrochen und eine Fehlermeldung ausgegeben.

Verwandte Themen

- Erweiterungen für die Verwendung von Active Roles Arbeitsabläufen auf Seite 36
- ID und Status einer Operation auf Seite 37
- Zusätzliche virtuelle Eigenschaften im Schema auf Seite 37
- Benötigte Berechtigungen für die Synchronisation über One Identity Active Roles auf Seite 11

Erweiterungen für die Verwendung von Active Roles Arbeitsabläufen

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

Um die Stammdaten einer Active Directory Domäne zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Active Directory > Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Erfassen Sie auf dem Tabreiter **Active Roles** die folgenden Informationen für die Verwendung von Arbeitsabläufen.

   Tabelle 6: Erweiterte Eigenschaften für die Verwendung von Active Roles Arbeitsabläufen

Eigenschaft	Beschreibung
Active Roles Arbeitsabläufe ausführen	Gibt an, ob Active Roles Arbeitsabläufe ausgeführt werden sollen. Informationen zu Active Roles Arbeitsabläufen entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*. Ist diese Option gesetzt, erlaubt der integrierte Active Roles Konnektor die Ansteuerung von Active Roles Arbeitsabläufen. Gegebenenfalls müssen Sie die Prozesse im One Identity Manager benutzerdefiniert anpassen! Ist die Option nicht gesetzt, arbeitet der One Identity Manager ohne die Ansteuerung von Active Roles Arbeitsabläufen (Standardkonfiguration). Für das Standardverhalten wird ein administratives Benutzerkonto benötigt. HINWEIS: Ist das Benutzerkonto des One Identity Manager Service Mitglied in der Gruppe der Active Roles Administratoren werden Active Roles Arbeitsabläufe unabhängig von der Option immer umgangen.
Löschen von Benutzerkonten durch Active Roles Arbeitsabläufe	Gibt an, ob Benutzerkonten über Deprovisionierungsabläufe im Active Roles gelöscht werden.
Löschen von Gruppen durch Active Roles Arbeitsabläufe	Gibt an, ob Gruppen über Deprovisionierungsabläufe im Active Roles gelöscht werden.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Benötigte Berechtigungen für die Synchronisation über One Identity Active Roles auf Seite 11
- Interaktion mit Active Roles Arbeitsabläufen auf Seite 34
- Active Directory Benutzerkonten und Active Directory Gruppen deprovisionieren auf Seite 45

ID und Status einer Operation

Bei jeder Änderungsoperation im Active Directory wird die vom Active Roles Konnektor übermittelte ID an den Ausgabeparameter `LastOperationID` zurückgegeben. Der vom Active Roles übermittelte Status der Operation wird an den Ausgabeparameter `LastOperationStatus` zurückgegeben. Wird kein Arbeitsablauf ausgelöst, dann wird bei erfolgreicher Ausführung der Operation der Status **Completed** zurückgegeben. Wird ein Arbeitsablauf ausgelöst, dann wird der Status **Pending** zurückgeliefert. Diese Ausgabeparameter können Sie in den Folgeprozessen verwenden, um auf die Ausführung der Arbeitsabläufe zu warten.

Zusätzliche virtuelle Eigenschaften im Schema

Für die Abfrage der aktuellen Status von Arbeitsabläufen enthält das Schema des Active Roles Konnektors zusätzliche virtuelle Eigenschaften.

HINWEIS: Die virtuellen Eigenschaften erfordern keine Erweiterung des Active Directory Schemas. Active Roles verhält sich so, als ob diese Eigenschaften wirklich existieren würden.

Diese virtuellen Eigenschaften sind nur lesend definiert und an jedem Objekt vorhanden, werden jedoch in der Standardprojektvorlage nicht gemappt. Um diese Funktionalität zu nutzen, müssen Sie das Mapping kundenspezifisch anpassen.

Beim Lesen der Eigenschaften führt der Active Roles Konnektor einen `OperationSearchRequest`-Aufruf zum Active Roles aus. Um die Performance so wenig wie möglich zu beeinträchtigen, wird das Ergebnis gleicher Anfragen für 30 Sekunden im Cache gehalten.

Tabelle 7: Virtuelle Eigenschaften des Active Roles Konnektors

Eigenschaft	Beschreibung
vrtLastOperationID	ID der letzten Operation im Active Roles.

Eigenschaft	Beschreibung
vrtLastOperationStatus	Status der letzten Operation im Active Roles. Mögliche Status sind **Unknown**, **Pending**, **Completed**, **Rejected**, **Failed** und **Canceled**.

Weitere Informationen entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.

4

Interaktion mit Active Roles Richtlinien

Bei der Definition von Bildungsregeln im One Identity Manager sollten Sie die im Active Roles definierte Richtlinien beachten. Werte, die der One Identity Manager generiert, werden ohne Prüfung auf Einhaltung der Active Roles Richtlinien an den Active Roles Konnektor übergeben. Verstoßen die übergebenen Werte gegen die Active Roles Richtlinien, wird der gesamte Prozess fehlschlagen. Um dies zu vermeiden, sollten Sie die One Identity Manager Bildungsregeln an die Active Roles anpassen.

Informationen zu Active Roles Richtlinien entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.

5

Verwalten der Active Directory Objekte

Im One Identity Manager können Sie organisatorische Einheiten in einer hierarchischen Containerstruktur einrichten. Organisatorische Einheiten (Geschäftsstellen oder Abteilungen) werden dazu genutzt, Objekte des Active Directory wie Benutzerkonten und Gruppen logisch zu organisieren und somit die Verwaltung der Objekte zu erleichtern.

HINWEIS: Nachfolgend wird auf Besonderheiten bei der Verwaltung von Active Directory Objekten über Active Roles eingegangen. Ausführliche Informationen zur Verwaltung einer Active Directory-Umgebung mit dem One Identity Manager finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung*.

Detaillierte Informationen zum Thema

Active Directory Gruppen automatisch in den IT Shop aufnehmen

Mit der **One Identity Manager Active Directory Edition** wird die Überführung der Funktionalität von Active Roles Self-Service Manager in den IT Shop des One Identity Manager direkt unterstützt.

Wenn Sie die **One Identity Manager Edition** einsetzen, führen Sie vor der initialen Synchronisation zusätzlich folgende Schritte aus.

Um Gruppen automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | ADSGroup**.
2. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | ADSGroup | ExcludeList** und legen Sie die Active Directory Gruppen fest, die nicht automatisch in den IT Shop übernommen werden sollen.

   Beispiel:

   ```
   .*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS
   ```
3. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | ARS_SSM**.
4. (Optional) Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | AutoPublish | ADSGroup | AutoFillDisplayName**.

   Ist der Konfigurationsparameter aktiviert, wird für Active Directory Gruppen ein Anzeigename gebildet, sofern noch kein Anzeigename vorhanden ist. Der Anzeigename wird beispielsweise für die Anzeige der Gruppe im Web Portal benötigt. Für eine über Active Roles verwaltete Active Directory Domäne wird der Anzeigename nur für Gruppen gebildet, die im Active Roles Self-Service Manager veröffentlicht ist.
5. Kompilieren Sie die Datenbank.

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

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

1. Es wird eine Leistungsposition für die Systemberechtigung ermittelt.

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

   - Für Systemberechtigungen mit Leistungsposition wird die Leistungsposition angepasst.
   - Systemberechtigungen ohne Leitungsposition erhalten eine neue Leistungsposition.
   - Die Leistungsposition wird abhängig davon, ob die Systemberechtigung im Active Roles Self-Service Manager veröffentlicht ist, aktiviert oder deaktiviert.
2. Die Leistungsposition wird einer der Standard-Servicekategorien zugeordnet.
3. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet.

   Die Produkteigner können Bestellungen von Mitgliedschaften in diesen Systemberechtigungen genehmigen. Standardmäßig wird der Kontomanager einer Systemberechtigung als Produkteigner ermittelt.

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

- Ist der Kontomanager der Systemberechtigung bereits Mitglied einer Anwendungsrolle für Produkteigner, dann wird diese Anwendungsrolle der Leistungsposition zugewiesen. Alle Mitglieder dieser Anwendungsrolle werden dadurch Produkteigner der Systemberechtigung.
- Ist der Kontomanager der Systemberechtigung noch kein Mitglied einer Anwendungsrolle für Produkteigner, dann wird eine neue Anwendungsrolle erzeugt. Die Bezeichnung der Anwendungsrolle entspricht der Bezeichnung des Kontomanagers.
    - Handelt es sich beim Kontomanager um ein Benutzerkonto oder einen Kontakt, wird die Person des Benutzerkontos oder des Kontaktes in die Anwendungsrolle aufgenommen.
    - Handelt es sich um eine Gruppe von Kontomanagern, werden die Personen aller Benutzerkonten dieser Gruppe in die Anwendungsrolle aufgenommen.
- Besitzt die Systemberechtigung keine Kontomanager wird die Standard-Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner | Ohne Eigentümer im AD** verwendet.

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

Anschließend können die Kunden des Shops Mitgliedschaften in Systemberechtigungen über das Web Portal bestellen.

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

Verwandte Themen

- Active Directory Gruppen über das Web Portal bestellen auf Seite 42
- Active Roles spezifische Erweiterungen für Active Directory Gruppen auf Seite 43

Active Directory Gruppen über das Web Portal bestellen

HINWEIS: Bei der Bestellung der Gruppenmitgliedschaft wird in der Standardinstallation der Entscheidungsworkflow **Entscheidung der Bestellungen von Mitgliedschaften in Active Directory Gruppen** wirksam.

Um eine neue Active Directory Gruppe zu bestellen

- Wählen Sie im Web Portal im Menü **Servicekatalog > Bestellung** die Servicekategorie **Active Directory Gruppen**.

- Bestellen Sie die Active Directory Gruppe über die Produkte **Anlegen einer Active Directory Verteilerliste** oder **Anlegen einer Active Directory Sicherheitsgruppe**.

Bei der Bestellung einer neuen Active Directory Gruppe werden automatisch die folgenden Schritte ausgeführt:

- Es wird ein Eintrag für die Active Directory Gruppe im One Identity Manager erzeugt.
- Die Active Directory Gruppe wird mit der Option **Gruppe ist im Self-Service Manager veröffentlicht** gekennzeichnet.
- Die Active Directory Gruppe wird mit der Option **IT Shop** gekennzeichnet.
- Es wird eine zugehörige Leistungsposition erzeugt. Es wird eine neue Anwendungsrolle erstellt, in welcher der Besteller Mitglied wird. Die Anwendungsrolle wird als Produkteigner der Leistungsposition eingetragen.

  Durch dieses Vorgehen ist der Besteller einer Active Directory Gruppe entscheidungsberechtigt bei der Bestellung von Mitgliedschaften in dieser Active Directory Gruppe.
- Die Active Directory Gruppe wird im Standardshop **Identity & Access Lifecycle** dem Regal **Active Directory Gruppen** zugewiesen.

Anschließend ist Mitgliedschaft in der Active Directory Gruppe für die Kunden des Shops über das Web Portal bestellbar.

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

Verwandte Themen

- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 40
- Active Roles spezifische Erweiterungen für Active Directory Gruppen auf Seite 43

Active Roles spezifische Erweiterungen für Active Directory Gruppen

Für Active Roles werden für eine Active Directory Gruppe zusätzliche Stammdaten abgebildet. Ausführliche Informationen zur Verwaltung von Active Directory Gruppen im One Identity Manager finden Sie im *One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung*.

Um die aus dem Active Roles ermittelten Stammdaten einer Active Directory Gruppe anzuzeigen

1. Wählen Sie im Manager die Kategorie **Active Directory > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Active Roles**.

Die folgenden Eigenschaften werden abgebildet.

Tabelle 8: Active Roles-spezifische Eigenschaften einer Active Directory Gruppe

Eigenschaft	Beschreibung
Gruppe ist im Self-Service Manager veröffentlicht	Wenn eine Active Directory Gruppe veröffentlicht ist, kann diese Active Directory Gruppe nach der Synchronisation sofort das Web Portal bestellt werden. Die Angabe wird bei der Synchronisation aus dem Active Roles gelesen. Bei Anlage einer Active Directory Gruppe über das Web Portal wird diese Angabe publiziert, um bei Bedarf weitere Arbeitsabläufe in Active Roles zu starten.
Entscheidung durch die Besitzer der Gruppe	Gibt an, ob die Entscheidung über die Gruppenmitgliedschaft durch den Besitzer (Kontomanager) der Active Directory Gruppe erfolgen muss. Die Angabe hat Auswirkung auf den Ablauf des Genehmigungsverfahrens im IT Shop.
Entscheidung durch einen zusätzlichen Besitzer der Gruppe	Gibt an, ob die Entscheidung über die Gruppenmitgliedschaft durch die zusätzlichen Besitzer der Active Directory Gruppe erfolgen muss. Die Angabe hat Auswirkung auf den Ablauf des Genehmigungsverfahrens im IT Shop.
Dynamische Gruppe	Gibt an, ob die Mitglieder dieser Gruppe in Active Roles dynamisch ermittelt werden. Manuelle Änderungen der Mitgliedschaften sind nicht zulässig.
Kontrollierte Gruppe	Gibt an, ob die Gruppe ist unter Kontrolle von Active Roles ist. Die Gruppe gehört zu einer Group Family in Active Roles. Die Mitgliedschaften werden über die Group Family geregelt. Manuelle Änderungen der Mitgliedschaften sind nicht zulässig.
Group Family	Gibt an, ob diese Gruppe eine Group Family in Active Roles repräsentiert. Group Family erstellt automatisch Gruppen und verwaltet die Mitgliedschaften in Übereinstimmung mit konfigurierbaren Regeln in Active Roles. Manuelle Änderungen der Mitgliedschaften sind nicht zulässig.
Zusätzliche Besitzer	Liste zusätzlicher Besitzer. Zulässig sind Active Directory Gruppen oder Active Directory Benutzerkonten.
Deprovisionierungsstatus	Status der Deprovisionierungsabläufe durch Active Roles beim Löschen des Objektes. Die Angabe wird bei der Synchronisation aus dem Active Roles gelesen. • **Keine Deprovisionierung**: Das Active Directory Objekt ist aktiv. • **Deprovisionierung erfolgreich**: Das Active

Eigenschaft	Beschreibung
	Directory Objekt wurde erfolgreich deprovisioniert. • **Deprovisionierung fehlerhaft**: Bei der Deprovisionierung des Active Directory Objektes ist ein Fehler aufgetreten.
Deprovisionierungsdatum	Datum der Deprovisionierungsabläufe durch Active Roles beim Löschen des Objektes. Die Angabe wird bei der Synchronisation aus Active Roles gelesen.

Verwandte Themen

- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 40
- Active Directory Gruppen über das Web Portal bestellen auf Seite 42
- Abbildung der Informationen zur Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 48

Active Directory Benutzerkonten und Active Directory Gruppen deprovisionieren

Der One Identity Manager unterstützt die Deprovisionierung über Active Roles. Anhand konfigurierter Deprovisionierungsrichtlinien im Active Roles wird ein Active Directory Objekt dabei so modifiziert, dass es temporär oder dauerhaft deaktiviert ist und gegebenenfalls erst nach dem Ablauf eines bestimmten Zeitraumes endgültig gelöscht wird. Detaillierte Informationen zur Active Roles Deprovisionierung entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.

HINWEIS: Die Konfiguration der Deprovisionierungsrichtlinien im Active Roles kann im Widerspruch zur Standardkonfiguration One Identity Manager stehen. Nehmen Sie in diesem Fall entsprechende kundenspezifische Anpassungen, beispielsweise an Bildungsregeln oder Prozessen, vor.

Zur Deprovisionierung der Active Directory Benutzerkonten und Active Directory Gruppen über den One Identity Manager werden folgenden Verfahren eingesetzt:

- Deprovisionieren statt Löschen
- Direktes Deprovisionieren

Detaillierte Informationen zum Thema

- Deprovisionieren statt Löschen auf Seite 46
- Direkte Deprovisionierung auf Seite 47

- Abbildung der Informationen zur Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 48
- Wiederherstellen deprovisionierter Active Directory Benutzerkonten und Active Directory Gruppen im One Identity Manager auf Seite 49
- Interaktion mit Active Roles Richtlinien auf Seite 39

Deprovisionieren statt Löschen

Um dieses Verfahren einzusetzen

- Aktivieren Sie im Manager für die Active Directory Domäne die Optionen **Löschen von Benutzerkonten durch Active Roles Arbeitsabläufe** und **Löschen von Gruppen durch Active Roles Arbeitsabläufe**.

Beim Löschen eines Active Directory Benutzerkontos oder einer Active Directory Gruppe im One Identity Manager wird anstelle der Standardprozesse zum Löschen ein Prozess zur Deprovisionierung im Active Roles erzeugt. Der Prozess stellt das Active Directory Objekt zur Deprovisionierung im Active Roles ein, setzt den Deprovisionierungsstatus und prüft den Deprovisionierungsverlauf. Abhängig davon erfolgt die Weiterbehandlung der Active Directory Objekte im One Identity Manager.

- Wurde das Active Directory Objekt im Active Roles sofort gelöscht, wird das Active Directory Objekt auch im One Identity Manager gelöscht.
- Wurde das Active Directory Objekt im Active Roles umbenannt oder in einen anderen Active Directory Container verschoben, dann erfolgt dies auch im One Identity Manager.

  Das Active Directory Objekt verbleibt in der One Identity Manager-Datenbank zunächst im Status **gelöscht**.

HINWEIS: Active Directory Benutzerkonten und Active Directory Gruppen, bei denen die Option **Schutz von versehentlichem Löschen** aktiviert ist, können nicht verschoben oder gelöscht werden.

Um ein Benutzerkonto zu löschen

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

Um eine Active Directory Gruppe zu löschen

1. Wählen Sie im Manager die Kategorie **Active Directory > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Klicken Sie in der Ergebnisliste .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Verwandte Themen

- Erweiterungen für die Verwendung von Active Roles Arbeitsabläufen auf Seite 36
- Direkte Deprovisionierung auf Seite 47
- Abbildung der Informationen zur Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 48
- Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen aufheben auf Seite 50
- Wiederherstellen gelöschter Objekte auf Seite 51

Direkte Deprovisionierung

Dieses Verfahren können Sie einsetzen, wenn die Active Directory Domäne nicht für die Deprovisionierung gekennzeichnet ist. Um einzelne Active Directory Benutzerkonten oder Active Directory Gruppen zu deprovisionieren, wird an diesen Objekten die Aufgabe **Deprovisionieren** angeboten.

Es wird ein Prozess zur Deprovisionierung im Active Roles erzeugt. Der Prozess stellt das Active Directory Objekt zur Deprovisionierung im Active Roles ein, setzt den Deprovisionierungsstatus und prüft den Deprovisionierungsverlauf. Abhängig davon erfolgt die Weiterbehandlung der Active Directory Objekte im One Identity Manager.

- Wurde das Active Directory Objekt im Active Roles sofort gelöscht, wird das Active Directory Objekt auch im One Identity Manager gelöscht.
- Wurde das Active Directory Objekt im Active Roles umbenannt oder in einen anderen Active Directory Container verschoben, dann erfolgt dies auch im One Identity Manager.

  Das Active Directory Objekt verbleibt in der One Identity Manager-Datenbank zunächst im Status **geändert**. Durch die nächste Synchronisation werden alle Eigenschaften des Active Directory Objektes in die One Identity Manager-Datenbank eingelesen und der Status auf **publiziert** gesetzt.

HINWEIS: Active Directory Benutzerkonten und Active Directory Gruppen, bei denen die Option **Schutz von versehentlichem Löschen** aktiviert ist, können nicht verschoben oder gelöscht werden.

Um ein Active Directory Benutzerkonto zu deprovisionieren

1. Wählen Sie im Manager die Kategorie **Active Directory > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Deprovisionieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Bestätigen Sie mit **OK**.

Um eine Active Directory Gruppe zu deprovisionieren

1. Wählen Sie im Manager die Kategorie **Active Directory > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Deprovisionieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Bestätigen Sie mit **OK**.

Verwandte Themen

- Deprovisionieren statt Löschen auf Seite 46
- Abbildung der Informationen zur Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 48
- Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen aufheben auf Seite 50

Abbildung der Informationen zur Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen

Folgende Eigenschaften werden für die Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen abgebildet.

Tabelle 9: Informationen zur Deprovisionierung

Eigenschaft	Beschreibung
Deprovisionierungsstatus	Status der Deprovisionierungsabläufe durch Active Roles beim Löschen des Objektes. Die Angabe wird bei der Synchronisation aus dem Active Roles gelesen. • **Keine Deprovisionierung**: Das Active Directory Objekt ist aktiv. • **Deprovisionierung erfolgreich**: Das Active Directory Objekt wurde erfolgreich deprovisioniert. • **Deprovisionierung fehlerhaft**: Bei der Deprovisionierung des Active Directory Objektes ist ein Fehler aufgetreten.
Deprovisionierungsdatum	Datum der Deprovisionierungsabläufe durch Active Roles beim Löschen des Objektes. Die Angabe wird bei der Synchronisation aus Active Roles gelesen.

Um die Stammdaten für die Deprovisionierung eines Active Directory Benutzerkontos anzuzeigen

1. Wählen Sie im Manager die Kategorie **Active Directory > Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Active Roles**.

Um die Stammdaten für die Deprovisionierung einer Active Directory Gruppe anzuzeigen

1. Wählen Sie im Manager die Kategorie **Active Directory > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Active Roles**.

Verwandte Themen

- Active Roles spezifische Erweiterungen für Active Directory Gruppen auf Seite 43

Wiederherstellen deprovisionierter Active Directory Benutzerkonten und Active Directory Gruppen im One Identity Manager

Deprovisionierte Active Directory Benutzerkonten und Active Directory Gruppen können Sie über den One Identity Manager bei Bedarf wiederherstellen. Dabei werden die folgenden Verfahren eingesetzt:

- Deprovisionierung aufheben
- Wiederherstellen gelöschter Objekte

Mit beiden Verfahren wird ein Prozess zur Deprovisionierung des Active Directory Objektes im Active Roles initiiert. Der Prozess ermittelt den Deprovisionierungsstatus, aktualisiert einige der Eigenschaften des Active Directory Objektes in der One Identity Manager-Datenbank, wie beispielsweise den Namen und den Active Directory Container, und setzt den Status des Active Directory Objektes auf **geändert**. Durch die nächste Synchronisation werden alle Eigenschaften des Active Directory Objektes in die One Identity Manager-Datenbank eingelesen und der Status auf **publiziert** geändert.

Detaillierte Informationen zum Thema

- Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen aufheben auf Seite 50
- Wiederherstellen gelöschter Objekte
- Active Directory Benutzerkonten und Active Directory Gruppen deprovisionieren auf Seite 45

Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen aufheben

Mit diesem Verfahren heben Sie die Deprovisionierung der Active Directory Benutzerkonten und Active Directory Gruppen wieder auf. Das Verfahren können Sie unabhängig vom eingesetzten Deprovisionierungsverfahren nutzen.

Um die Deprovisionierung eines Active Directory Benutzerkonto aufzuheben

1. Wählen Sie im Manager die Kategorie **Active Directory > Benutzerkonten > Deprovisionierte Konten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Deprovisionierung aufheben**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Bestätigen Sie mit **OK**.

Um die Deprovisionierung einer Active Directory Gruppe aufzuheben

1. Wählen Sie im Manager die Kategorie **Active Directory > Gruppen > Deprovisionierte Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Deprovisionierung aufheben**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
5. Bestätigen Sie mit **OK**.

Verwandte Themen

- Wiederherstellen gelöschter Objekte auf Seite 51
- Active Directory Benutzerkonten und Active Directory Gruppen deprovisionieren auf Seite 45

Wiederherstellen gelöschter Objekte

Dieses Verfahren können Sie alternativ auf die Active Directory Benutzerkonten und Active Directory Gruppen anwenden, die Sie über das Verfahren **Deprovisionieren statt Löschen** deprovisioniert haben. Das deprovisionierte Active Directory Objekt befindet sich in diesem Fall in der One Identity Manager-Datenbank im Status **gelöscht**.

Um ein Benutzerkonto wiederherzustellen

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

Um eine Gruppe wiederherzustellen

1. Wählen Sie im Manager die Kategorie **Active Directory > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Klicken Sie in der Ergebnisliste die Schaltfläche **Löschen rückgängig machen**.

Verwandte Themen

- Deprovisionieren statt Löschen auf Seite 46
- Active Directory Benutzerkonten und Active Directory Gruppen deprovisionieren auf Seite 45
- Deprovisionierung von Active Directory Benutzerkonten und Active Directory Gruppen aufheben auf Seite 50

Anhang A

Konfigurationsparameter für die Verwaltung einer Active Directory-Umgebung

Mit der Installation des Active Directory Moduls und des Active Roles Moduls sind zusätzlich folgende Konfigurationsparameter im One Identity Manager verfügbar.

Tabelle 10: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
QER | ITShop | AutoPublish | ADSGroup	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der automatischen Übernahme von Active Directory Gruppen in den IT Shop. Ist der Parameter aktiviert, werden alle Gruppen automatisch als Produkte dem IT Shop zugewiesen. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
QER | ITShop | AutoPublish | ADSGroup | AutoFillDisplayName	Der Konfigurationsparameter legt fest, ob die Bildungsregel für die Spalte `ADSGroup.DisplayName` angewendet werden soll.
QER | ITShop | AutoPublish | ADSGroup | ExcludeList	Auflistung aller Active Directory Gruppen, 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`

Konfi-gurationsparameter	Beschreibung
TargetSystem | ADS	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems Active Directory. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
TargetSystem | ADS | Accounts	Erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem | ADS | 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 | ADS | Accounts | InitialRandomPassword | SendTo	Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter **TargetSystem | ADS | DefaultAddress** hinterlegte Adresse versandt.
TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto** verwendet.
TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Person - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem | ADS | 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 **Person - Erstellung neues Benutzerkonto mit Standardwerten**

Konfi-gurationsparameter	Beschreibung
	verwendet.
TargetSystem | ADS | Accounts | NotRequirePassword	Gibt an, ob bei der Neuanlage von Active Directory Benutzerkonten im One Identity Manager die Angabe eines Kennwortes erforderlich ist. Ist der Konfigurationsparameter deaktiviert, wird bei der Neuanlage eines Active Directory Benutzerkontos die Eingabe eines Kennworts entsprechend der definierten Kennwortrichtlinien gefordert. Ist der Konfigurationsparameter aktiviert, ist bei der Neuanlage von Active Directory Benutzerkonten die Angabe eines Kennwortes nicht erforderlich.
TargetSystem | ADS | Accounts | PrivilegedAccount	Erlaubt die Konfiguration der Einstellungen für privilegierte Active Directory Benutzerkonten.
TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_ Postfix	Postfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | ADS | Accounts | Privi-legedAccount | SAMAccountName_ Prefix	Präfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | ADS | Accounts | ProfileFixedString	Feste Zeichenkette, die an den Standardprofilpfad eines Benutzerprofils angehängt wird.
TargetSystem | ADS | Accounts | TransferJPegPhoto	Gibt an, ob bei Änderung des Bildes in den Stammdaten der Person dieses an bestehende Benutzerkonten publiziert wird. Das Bild ist nicht Bestandteil der normalen Synchronisation, es wird nur bei Änderung der Personenstammdaten publiziert.
TargetSystem | ADS | Accounts | TransferSIDHistory	Gibt an, ob die Historie einer SID aus dem Zielsystem gelesen werden soll.
TargetSystem | ADS | Accounts | TSProfileFixedString	Feste Zeichenkette, die an den Standardprofilpfad eines Benutzerprofils auf einem Terminalserver angehängt wird.
TargetSystem | ADS | Accounts | UnlockByCentralPasswo	Gibt an, ob das Active Directory Benutzerkonto der Person bei der Synchronisation des zentralen Kennworts ebenfalls entsperrt wird.

Konfi-gurationsparameter	Beschreibung
rd	
TargetSystem | ADS | Accounts | UserMustChangePassword	Gibt an, ob bei Neuanlage von Benutzerkonten die Option **Kennwort bei der nächsten Anmeldung ändern** gesetzt wird.
TargetSystem | ADS | ARS	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Unterstützung von Active Roles. Ist der Parameter aktiviert, sind die Bestandteile 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 | ADS | ARS_SSM	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Überführung der Funktionalität von One Identity Active Roles Self-Service Manager in den One Identity ManagerIT Shop. Ist der Parameter aktiviert, sind die Bestandteile 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 | ADS | AuthenticationDomains	Pipe (|) getrennte Liste von Domänen, gegen die manuelle Active Directory Authentifizierungsmodule die Benutzer authentifizieren sollen. Die Liste wird in der Reihenfolge abgearbeitet, in der sie hier angegeben ist. Die Liste sollte nur Domänen enthalten, die synchronisiert werden. Beispiel: `MyDomain|MyOtherDomain` Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager*

Konfi-gurationsparameter	Beschreibung
	Handbuch zur Autorisierung und Authentifizierung.
TargetSystem | ADS | AutoCreateDepartment	Gibt an, ob beim Synchronisieren oder Ändern von Benutzerkonten automatisch Abteilungen erzeugt werden.
TargetSystem | ADS | AutoCreateLocality	Gibt an, ob beim Synchronisieren oder Ändern von Benutzerkonten automatisch Standorte erzeugt werden.
TargetSystem | ADS | AutoCreateHardwaretype	Gibt an, ob für importierte Druckerobjekte automatisch entsprechende Gerätetypen in der Datenbank erzeugt werden.
TargetSystem | ADS | AutoCreateServers	Gibt an, ob bei der Synchronisation der Benutzerkonten automatisch Einträge für fehlende Homeserver und Profileserver erstellt werden.
TargetSystem | ADS | AutoCreateServers | PreferredLanguage	Sprache der automatisch angelegten Server.
TargetSystem | ADS | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | ADS | HardwareInGroupFromOrg	Gibt an , ob Computer aufgrund von Gruppenzuordnung zu Rollen in Gruppen aufgenommen werden.
TargetSystem | ADS | 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 | ADS | MembershipAssignCheck	Gibt an, ob bei Zuweisungen von Gruppenmitgliedschaften in der One Identity Manager-Datenbank bereits beim Speichern die Zulässigkeit dieser Mitgliedschaft geprüft wird. Sollen in der Datenbank mehrere getrustete Domänen mit übergreifenden Mitgliedschaften verwaltet werden, so ist dieser Konfigurationsparameter zu deaktivieren.
TargetSystem | ADS | MemberShipRestriction	Allgemeiner Konfigurationsparameter zur Einschränkung der Mitgliedschaften für Active Directory.
TargetSystem | ADS | MemberShipRestriction | Container	Anzahl von Active Directory Objekten pro Container, bei deren Überschreitung eine Warnmail gesendet werden soll.
TargetSystem | ADS |	Anzahl von Active Directory Objekten pro Gruppe, bei deren

Konfi-gurationsparameter	Beschreibung
MemberShipRestriction | Group	Überschreitung eine Warnmail gesendet werden soll.
TargetSystem | ADS | MemberShipRestriction | MailNotification	Standard-Mailadresse zum Versenden von Warnmails.
TargetSystem | ADS | PersonAutoDefault	Modus für die automatische Personenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | ADS | PersonAutoDisabledAccounts	Gibt an, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | ADS | PersonAutoFullSync	Modus für die automatische Personenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem | ADS | PersonExcludeList	Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $`
TargetSystem | ADS | PersonUpdate	Gibt an, ob Personen bei Änderung ihrer Benutzerkonten aktualisiert werden. Aktivieren Sie diesen Konfigurationsparameter, um eine fortlaufende Aktualisierung von Personenobjekten aus verbundenen Benutzerkonten zu erreichen.
TargetSystem | ADS | ReplicateImmediately	Beschleunigung der Synchronisation von Änderungen zwischen den Domänen-Controllern. Bei Aktivierung werden die aufgelaufenen Änderungen im Active Directory sofort zwischen den Domänen-Controllern repliziert.
TargetSystem | ADS | VerifyUpdates	Gibt an, ob bei einem Update geänderte Eigenschaften im Zielsystem überprüft werden. Ist der Parameter aktiviert, werden nach jedem Update die Eigenschaften des Objektes im Zielsystem verifiziert.

Anhang B

Standardprojektvorlage für One Identity Active Roles

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 11: Abbildung der Schematypen

Schematyp im Active Roles	Tabelle im One Identity Manager Schema
builtInDomain	ADSContainer
computer	ADSMachine
contact	ADSContact
container	ADSContainer
domainDNS	ADSDomain
group	ADSGroup
inetOrgPerson	ADSAccount
msDS-PasswordSettings	ADSPolicy
msExchSystemObjectsContainer	ADSContainer
oganization	ADSContainer
organizationalUnit	ADSContainer
printQueue	ADSPrinter

Schematyp im Active Roles	Tabelle im One Identity Manager Schema
rpcContainer	ADSContainer
user	ADSAccount

Anhang C

Einstellungen des Active Roles Konnektors

Für die Systemverbindung mit dem Active Roles Konnektor werden die folgenden Einstellungen konfiguriert.

Tabelle 12: Einstellungen des Active Roles Konnektors

Einstellung	Bedeutung
Domäne	Vollständiger Name der Domäne. Variable: `CP_Rootdn`
Benutzerkonto	Benutzerkonto zur Anmeldung am Active Roles. Variable: `CP_User`
Kennwort	Kennwort zum Benutzerkonto. Variable: `CP_Password`
DNS Name oder IP Adresse des Active Roles Servers	Vollständiger Name oder IP Adresse des Active Roles Servers, gegen den sich der Synchronisationsserver verbindet. Beispiel: `<Name des Servers>.<Vollqualifizierter Domänenname>` Variable: `CP_Server`
Begründung für Arbeits-abläufe	Begründung, welche bei der Ausführung von Arbeitsabläufen eingetragen wird. Variable: `DefaultWorkflowReason`
Active Roles Arbeitsabläufe ausführen	Gibt an, ob Active Roles Arbeitsabläufe ausgeführt werden sollen. Wenn der Wert **False** ist, werden keine Active Roles Arbeitsabläufe ausgeführt. Das Benutzerkonto benötigt die Berechtigungen unter Benötigte Berechtigungen für die Synchronisation über One Identity Active Roles auf Seite 11. Wenn der Wert **True** ist, versucht der Konnektor die Active Roles

Einstellung	Bedeutung
	Arbeitsabläufe auszuführen, die mit der Operation verknüpft sind. Dies funktioniert nur, wenn das Verbindungskonto nicht Mitglied der Active Roles Administratorengruppe ist. Standard: **False** Variable: `RunArsWorkflowsByDefault`
ForestName	Bezeichnung der Domänengesamtstruktur. Variable: `ForestName`

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

P

S

Z