One Identity Manager 8.1.4

Administrationshandbuch für die Anbindung einer Active Directory-Umgebung

Legende

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

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

One Identity Manager Administrationshandbuch für die Anbindung einer Active Directory-Umgebung
Aktualisiert - 19. Oktober 2020, 07:30 Uhr
Version - 8.1.4

Inhalt

1

Verwalten einer Active Directory-Umgebung

Komplexe Windows Umgebungen mit Active Directory lassen sich im One Identity Manager abbilden und synchronisieren. Im One Identity Manager ist die Verwaltung der Objekte des Active Directory wie beispielsweise Benutzerkonten, Kontakte, Gruppen, Computer und organisatorische Einheiten, in hierarchischen Domänenstrukturen möglich.

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

Um den Benutzerkonten die benötigten Berechtigungen zur Verfügung zu stellen, werden im One Identity Manager die Gruppen administriert. Im One Identity Manager können Sie organisatorische Einheiten in einer hierarchischen Containerstruktur einrichten. Organisatorische Einheiten (Geschäftsstellen oder Abteilungen) werden dazu genutzt, Objekte wie Benutzerkonten, Gruppen und Computer logisch zu organisieren und somit die Verwaltung der Objekte zu erleichtern.

Architekturüberblick

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

- Active Directory Domänen-Controller

  Domänen-Controller, gegen den die Synchronisation der Active Directory Objekte läuft. Der Synchronisationsserver verbindet sich gegen diesen Server, um auf die Active Directory Objekte zuzugreifen.

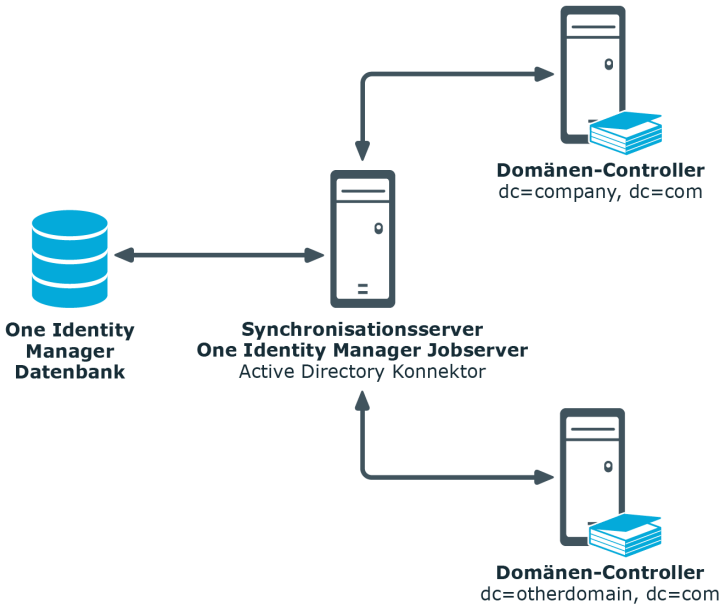
- Synchronisationsserver

  Synchronisationsserver für den Abgleich zwischen der One Identity Manager-Datenbank und der Active Directory-Umgebung. Auf diesem Server ist der One Identity Manager Service mit dem Active Directory Konnektor installiert. Der

Synchronisationsserver verbindet sich gegen den Active Directory Domänen-Controller.

Der Active Directory Konnektor des One Identity Manager verwendet das ADSI Interface für die Kommunikation mit einem Domänen-Controller. Der Active Directory Konnektor wird für die Synchronisation und Provisionierung der Active Directory-Umgebung eingesetzt. Der Active Directory Konnektor kommuniziert direkt mit einem Domänen-Controller.

Abbildung 1: Architektur für die Synchronisation



One Identity Manager Benutzer für die Verwaltung einer Active Directory-Umgebung

In die Verwaltung einer Active Directory-Umgebung sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

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

Benutzer	Aufgaben
	• Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen. • Legen die Zielsystemverantwortlichen fest. • Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein. • Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen. • Berechtigen weitere Personen als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Active Directory** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung

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

Einrichten der Synchronisation mit einer Active Directory-Umgebung

Der One Identity Manager unterstützt die Synchronisation mit einem Active Directory, welches mit Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 und Windows Server 2019 ausgeliefert wird.

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

1. Stellen Sie im Active Directory 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.
    - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.
    - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit dem Active Directory auf Seite 14
- Kommunikationsports und Firewall Konfiguration auf Seite 17
- Einrichten des Synchronisationsservers auf Seite 18
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Active Directory Domäne auf Seite 22
- Deaktivieren der Synchronisation auf Seite 41

- Anpassen einer Synchronisationskonfiguration auf Seite 30
- Konfigurationsparameter für die Verwaltung einer Active Directory-Umgebung auf Seite 206
- Standardprojektvorlage für Active Directory auf Seite 211

Benutzer und Berechtigungen für die Synchronisation mit dem Active Directory

Bei der Synchronisation des One Identity Manager mit einer Active Directory-Umgebung spielen folgende Benutzer eine Rolle.

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzer für den Zugriff auf das Active Directory	Für eine vollständige Synchronisation von Objekten einer Active Directory-Umgebung mit der ausgelieferten One Identity Manager Standardkonfiguration stellen Sie ein Benutzerkonto bereit, das die folgenden Berechtigungen besitzt. • Mitglied der Active Directory Gruppe **Domänen Administratoren** HINWEIS: In einer hierarchischen Domänenstruktur sollte das Benutzerkonto des One Identity Manager Service einer untergeordneten Domäne Mitglied in der Gruppe **Enterprise Admins** sein. Es kann keine sinnvolle Minimalkonfiguration empfohlen werden, die sich bezüglich der reinen Benutzerverwaltung effektiv in ihren Berechtigungen von einem Mitglied der Gruppe **Domänen Administratoren** unterscheidet.
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Rechte vergeben, Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Rechte für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Rechte für den internen Webservice über

Benutzer	Berechtigungen
	folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen) Das Setzen von Remote Access Service (RAS)-Eigenschaften erfordert Remote Procedure Calls (RPC), die im Kontext des Benutzerkontos des One Identity Manager Service ausgeführt werden. Um diese Eigenschaften zu lesen oder zu schreiben, muss das Benutzerkonto des One Identity Manager Service die entsprechenden Berechtigungen besitzen.
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer **Synchronization** bereitgestellt.

Erläuterungen zu den erforderlichen Rechten

In der Active Directory-Umgebung werden auf das Basisobjekt der Synchronisation folgende Rechte benötigt:

- Read
- Write

Ist das Basisobjekt das Domänenobjekt werden diese Rechte benötigt, um das Lesen und Setzen von Domäneneigenschaften wie beispielsweise Kennwortrichtlinien zu ermöglichen.

Um unterhalb des gewählten Basisobjektes uneingeschränkt arbeiten zu können, werden die folgenden Rechte benötigt:

- Create All Child Objects
- Delete All Child Objects

Um in einem Benutzerobjekt bestimmte Eigenschaften bearbeiten zu können, die eine Veränderung der Rechteliste eines Active Directory Objektes zur Folge haben (beispielsweise die Eigenschaft **Kennwort kann nicht geändert werden**), werden die folgenden Rechte benötigt:

- Read Permissions
- Modify Permissions

Als weiteres Privileg wird vorausgesetzt:

- Modify Owner

Das Privileg hat normalerweise nur die Gruppe der Administratoren. Wenn das Benutzerkonto des One Identity Manager Service nicht Mitglied dieser Gruppe oder einer äquivalenten Gruppe ist, muss es in die Lage versetzt werden, mit Konten umzugehen, auf die keine Berechtigungen mehr gesetzt sind.

Da über den One Identity Manager prinzipiell alle Werte eines Objektes änderbar sein sollen, sind die folgenden Rechte notwendig:

- Read All Properties
- Write All Properties
- All Extended Rights
- DeleteSubTree

Essentielle Funktionalitäten eines Benutzerkontos sind teilweise als Eintrag in der Berechtigungsliste (DACL) eines Active Directory Objektes hinterlegt. Es ist notwendig, das das Benutzerkonto des One Identity Manager Service diese DACL modifizieren kann. Beispiele für Eigenschaften, die über die DACL gepflegt werden, sind `UserCanNotChangePassword` am Benutzerkonto oder `AllowWriteMembers` an der Gruppe.

Die Modifikation einer DACL setzt sehr weitreichende Berechtigungen voraus. Wird zur Veränderung einer DACL ein Benutzerkonto verwendet, welches nicht die **Full Control**-Rechte auf das entsprechende Active Directory Objekt besitzt, wird die Änderung nur unter folgenden Bedingungen akzeptiert.

- Das Benutzerkonto ist Eigentümer des Objektes.

  – ODER –

- Das Benutzerkonto ist Mitglied in der selben primären Gruppe, wie der Eigentümer des Objektes. Das ist zumeist die Gruppe der **Domänen Administratoren**.

Andernfalls wird die Änderung abgelehnt. Wenn dem Benutzerkonto das **Take Ownership**-Recht zugewiesen ist, ist es möglich einen Eigentümerwechsel zu initiieren und die DACL daraufhin zu ändern. Das verfälscht jedoch die Berechtigungssituation des Active Directory Objektes und wird daher nicht empfohlen.

Des Weiteren sind für die Funktionen des Active Directory Papierkorbs zum Löschen und Wiederherstellen von Benutzerkonten sowie für den Umgang mit besonders geschützten Benutzerkonten und Gruppen die Berechtigungen eines Domänen Administrators erforderlich.

Hinweise für Read-Rechte

Grundsätzlich funktioniert der Teil der Synchronisation mit dem Active Directory, der die Active Directory Objekte in die One Identity Manager-Datenbank einliest, auch dann, wenn auf Strukturen nur **Read**-Rechte, jedoch keine **Write**-Rechte vergeben werden.

Folgende Probleme können jedoch auftreten:

- Um ein Benutzerkonto, auf welches nur **Read**-Rechte bestehen, in eine Gruppe aufzunehmen, welche nicht die primäre Gruppe des Benutzerkontos ist, muss der One Identity Manager Service mindestens **Write**-Rechte auf das Gruppenobjekt besitzen.
- Fehlerzustände zwischen One Identity Manager-Datenbank und Active Directory Daten treten auf, wenn durch die Administrationswerkzeuge des One Identity Manager oder durch Datenbankimporte Objekte im Active Directory angelegt oder verändert werden, auf welche nur **Read**-Rechte existieren. Diese Fälle sind durch geeignete Menüführung in den Administrationswerkzeugen, Objektrechte im One Identity Manager und entsprechende Vorsichtsmaßnahmen bei Importen auszuschließen.

Hinweise zur One Identity ManagerActive Directory Edition

Für die One Identity ManagerActive Directory Edition werden vollständige **Read**-Rechte und die Berechtigungen zum Erzeugen, Ändern und Löschen von Gruppen benötigt.

Kommunikationsports und Firewall Konfiguration

Der One Identity Manager besteht aus verschiedenen Komponenten die in verschiedenen Netzwerksegmenten laufen können. Zusätzlich benötigt der One Identity Manager Zugriff auf verschiedene Netzwerkdienste, welche ebenfalls in verschiedenen Netzwerksegmenten installiert sein können. Abhängig davon, welche Komponenten und Dienste Sie hinter ihrer Firewall installieren möchten, müssen Sie verschiedene Ports öffnen.

Die folgenden Basisports werden benötigt.

Tabelle 3: Kommunikationsports

Standardport	Beschreibung
1433	Port zur Kommunikation mit der One Identity Manager-Datenbank.
1880	Port für das HTTP-basierte Protokoll des One Identity Manager Service.
2880	Port für die Zugriffstests innerhalb des Synchronization Editor, beispielsweise im Zielsystembrowser oder zur Simulation der Synchronisation.
80	Port für den Zugriff auf die Webanwendungen.
88	Kerberos-Authentifizierungssystem. (Wenn Kerberos Authentifizierung eingesetzt wird). Benötigt für die Authentifizierung gegen Active Directory.
135	Microsoft End Point Mapper (EPMAP) (auch DCE/RPC Locator Service).

Standardport	Beschreibung
137	NetBIOS Name Service.
139	NetBIOS Session Service.
389	Lightweight Directory Access Protocol (LDAP Standard). Kommunikationsport auf dem Zielsystemserver.
445	Microsoft-DS Active Directory, Windows-Freigaben. Benötigt für Synchronisation (TCP/UDP).
53	Domain Name System (DNS), meist über UDP. Benötigt für den Zugriff auf die Active Directory-Gesamtstruktur.
636	Lightweight Directory Access Protocol über TLS/SSL (LDAP S). Benötigt für den Zugriff auf die Active Directory-Gesamtstruktur.
3268	Globaler Katalog. Benötigt für die Suche im Globalen Katalog. Je nach Verbindungseinstellung sollte entweder Port 3268 oder Port 3269 offen sein.
3269	Globaler Katalog über SSL. Benötigt für die Suche im Globalen Katalog. Je nach Verbindungseinstellung sollte entweder Port 3268 oder Port 3269 offen sein.

Einrichten des Synchronisationsservers

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 2008 R2 (nicht-Itanium 64-Bit) ab Service Pack 1
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 oder höher

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- One Identity Manager Service, Active Directory Konnektor
  - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.

1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen**.
2. Wählen Sie die Maschinenrolle **Server | Jobserver | 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. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein.

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

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

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

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

1. Starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation.
2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur

One Identity Manager-Datenbank ein.

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

      - ODER -

      Um einen neuen Jobserver 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 One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
      - **Vollständiger Servername**: Vollständiger Servername gemäß DNS Syntax.

        Syntax:

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

   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 Directory Konnektor**.
6. Auf der Seite **Dienstkonfiguration** erfassen Sie die Verbindungsinformationen und prüfen Sie die Konfiguration des One Identity Manager Service.

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

   - Für eine direkte Verbindung zu Datenbank:
     a. Wählen Sie **Prozessabholung | sqlprovider**
     b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
     c. Erfassen Sie die Verbindungsdaten zur One Identity Manager-Datenbank.
   - Für eine Verbindung zum Anwendungsserver:
     a. Wählen Sie **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen** und wählen Sie **AppServerJobProvider**.
     b. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die

Schaltfläche **Bearbeiten**.

c. Erfassen Sie die Verbindungsdaten zum Anwendungsserver.

d. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.

e. Wählen Sie das Authentifizierungsmodul. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

7. Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.
10. Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.

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

11. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Name oder IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
    - **Dienstkonto**: Angaben zum Benutzerkonto des One Identity Manager Service.
      - Um den Dienst unter dem Konto **NT AUTHORITY\SYSTEM** zu starten, aktivieren Sie die Option **Lokales Systemkonto**.
      - Um den Dienst unter einem anderen Konto zu starten, deaktivieren Sie die Option **Lokales Systemkonto** und erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung.
    - **Installationskonto**: Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.
      - Um das Benutzerkonto des angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Angemeldeter Benutzer**.
      - Um ein anderes Benutzerkonto zu verwenden, deaktivieren Sie die Option **Angemeldeter Benutzer** und geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.
    - Um das Installationsverzeichnis, den Namen, den Anzeigenamen oder die Beschreibung für den One Identity Manager Service zu ändern, nutzen Sie die weiteren Optionen.
12. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

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

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

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Active Directory Domäne

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.

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

WICHTIG: Für eine erfolgreiche Authentifizierung müssen der Domänen–Controller und die Domäne per DNS Anfrage aufgelöst werden können. Ist die DNS Auflösung nicht möglich, wird die Verbindung zum Zielsystem mit Fehlermeldung abgelehnt.

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Vollständiger Name der Domäne	Vollständiger Name der Domäne. Beispiel: `Doku.Testlab.dd`
Benutzerkonto und Kennwort zur Anmeldung an der Domäne	Benutzerkonto und Kennwort zur Anmeldung an der Domäne. Dieses Benutzerkonto wird für den Zugriff auf die Domäne verwendet. Stellen Sie ein Benutzerkonto mit ausreichenden Berechtigungen bereit. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit dem Active Directory auf Seite 14.
DNS Name des Domänen-Controllers	Vollständiger Name des Domänen-Controllers, gegen den sich der Synchronisationsserver verbindet, um auf die Active Directory Objekte zuzugreifen.

Angaben	Erläuterungen
	Beispiel: `Server.Doku.Testlab.dd`
Kommunikationsport auf dem Domänen-Controller	Kommunikationsport auf dem Domänen-Controller. LDAP Standard-Kommunikationsport ist Port 389.
Authentifizierungsart	Eine Verbindung zum Zielsystem kann nur hergestellt werden, wenn die richtige Authentifizierungsart gewählt wird. Als Standard wird die Authentifizierungsart **Secure** verwendet. Ausführliche Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library.
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 dem Active Directory Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. **Tabelle 5: Zusätzliche Eigenschaften für den Jobserver** **Eigenschaft** / **Wert** Serverfunktion / Active Directory Konnektor Maschinenrolle / Server/Jobserver/Active Directory Weitere Informationen finden Sie unter Einrichten des Synchronisationsservers auf Seite 18.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Datenbank • SQL Server Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung

Angaben	Erläuterungen
	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 Directory Konnektor ist installiert • Zielsystemspezifische Komponenten sind 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*.

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 einzurichten

1. Starten Sie das Launchpadund melden Sie sich an der One Identity Manager-Datenbank an.

   HINWEIS: Wenn die Synchronisation über einen Anwendungsserver ausgeführt werden soll, stellen Sie die Datenbankverbindung über den Anwendungsserver her.

2. Wählen Sie den Eintrag **Zielsystemtyp Active Directory** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors wird gestartet.

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

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

4. Auf der Seite **Domänenauswahl** legen Sie die zu synchronisierende Active Directory Domäne fest.
   - Wählen Sie in der Auswahlliste **Domäne** die Domäne oder tragen Sie den vollständigen Domänennamen ein.

5. Auf der Seite **Anmeldedaten** geben Sie das Benutzerkonto für den Zugriff auf die Domäne an. Dieses Benutzerkonto wird zur Synchronisation der Active Directory Objekte genutzt.
   a. Um ein definiertes Benutzerkonto zu verwenden, erfassen Sie das Benutzerkonto und das Kennwort zur Anmeldung am Zielsystem.

      Wenn das Benutzerkonto des aktuell angemeldeten Benutzers genutzt werden soll, lassen Sie die Angaben leer. Das Benutzerkonto, unter dem der One Identity Manager Service läuft, benötigt die unter Benutzer und Berechtigungen für die Synchronisation mit dem Active Directory auf Seite 14 beschriebenen Berechtigungen.

      HINWEIS: Wenn die Einstellung verwendet wird, dann wird während der Konfiguration im Synchronization Editor ebenfalls das Benutzerkonto des aktuell angemeldeten Benutzers verwendet. Dieses Benutzerkonto 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.

b. Klicken Sie im Bereich **Anmeldedaten verifizieren** auf **Test**, um die Verbindung zur Domäne zu testen.

6. Auf der Seite **Verbindungsoptionen konfigurieren** geben Sie den Domänen-Controller für die Synchronisation an und legen fest, mit welchen Optionen die Verbindung erfolgen soll.
   - Im Bereich **Binding Optionen** legen Sie die Authentifizierungsart für die Anmeldung am Zielsystem fest. Als Standard wird die Authentifizierungsart **Secure** verwendet.
   - Im Bereich **Domänen-Controller wählen oder eingeben** legen Sie den Domänen-Controller fest.
     a. Wählen Sie in der Auswahlliste **Domänen-Controller** einen vorhandenen Domänen-Controller aus oder tragen Sie den vollständiger Name des Domänen-Controllers direkt ein.
     b. Geben Sie im Eingabefeld **Port** den Kommunikationsport auf dem Domänen-Controller an. LDAP Standard-Kommunikationsport ist Port 389.
     c. Legen Sie über die Option **SSL verwenden** fest, ob eine sichere Verbindung verwendet werden soll.
     d. Klicken Sie **Test**, um die Verbindung zu testen. Es wird versucht eine Verbindung zum Domänen-Controller aufzubauen.
7. Auf der Seite **Konnektor Funktionen** legen Sie zusätzliche Einstellungen für die Synchronisation fest. Erfassen Sie folgende Einstellungen.

Tabelle 6: Zusätzliche Einstellungen

Eigenschaft	Beschreibung
Bei Anlage Objekte mit gleichem Distinguished Name oder GUID aus dem Papier-korb wieder-herstellen.	Angabe, ob gelöschte Active Directory Objekte beim Einfügen berücksichtigt werden sollen. Aktivieren Sie diese Option, wenn beim Einfügen eines Objektes zunächst geprüft werden soll, ob sich das Objekt im Active Directory Papierkorb befindet und von dort wiederhergestellt werden soll.
Erlaube das Lesen und Schreiben von Eigenschaften des Remote Access Service (RAS).	Angabe, ob Remote Access Service (RAS) Eigenschaften synchronisiert werden sollen. Wenn die Option nicht aktiviert ist, werden in der Synchronisation Standardwerte angenom-men. Es werden jedoch keine Eigenschaften gelesen oder geschrieben. Sie können diese Optionen zu einem späteren Zeitpunkt konfigurieren.
Erlaube das Lesen und Schreiben von Eigenschaften des Terminal-Dienstes.	Angabe, ob die Terminalserver-Eigenschaften synchronisiert werden sollen. Wenn die Option nicht aktiviert ist, werden in der Synchronisation Standardwerte angenommen. Es werden jedoch keine Eigenschaften gelesen oder geschrieben. Sie

Eigenschaft	Beschreibung
	können diese Optionen zu einem späteren Zeitpunkt konfigurieren.

HINWEIS: Das Einlesen der Terminalserver-Eigenschaften und RAS-Eigenschaften verlangsamt unter Umständen die Synchronisation.

8. 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.

9. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.

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

Tabelle 7: Zielsystemzugriff festlegen

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

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

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

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

    a. Klicken Sie , um einen neuen Jobserver anzulegen.

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

    c. Klicken Sie **OK**.

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

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

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

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

    Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

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

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

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

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

HINWEIS:

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

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

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

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Domäne die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **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.

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 18
- Benutzer und Berechtigungen für die Synchronisation mit dem Active Directory auf Seite 14
- Synchronisationsergebnisse anzeigen auf Seite 29
- Anpassen einer Synchronisationskonfiguration auf Seite 30
- Beschleunigung der Synchronisation durch Revisionsfilterung auf Seite 35
- Standardprojektvorlage für Active Directory auf Seite 211
- Kontendefinitionen für Active Directory Benutzerkonten auf Seite 45
- Automatische Zuordnung von Personen zu Active Directory Benutzerkonten auf Seite 137

Synchronisationsergebnisse anzeigen

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

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

Um das Protokoll einer Synchronisation anzuzeigen

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

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

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

Um das Protokoll einer Provisionierung anzuzeigen

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

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

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

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

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

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation einer 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 Mastersystem 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.

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

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

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

Detaillierte Informationen zum Thema

- Synchronisation in die Active Directory Domäne konfigurieren auf Seite 32
- Synchronisation verschiedener Active Directory Domänen konfigurieren auf Seite 33
- Schema aktualisieren auf Seite 33

Synchronisation in die Active Directory Domäne konfigurieren

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

Um eine Synchronisationskonfiguration für die Synchronisation in die Active Directory Domäne zu erstellen

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

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

Verwandte Themen

- Synchronisation verschiedener Active Directory Domänen konfigurieren auf Seite 33

Synchronisation verschiedener Active Directory Domänen konfigurieren

Voraussetzungen

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

Um ein Synchronisationsprojekt für die Synchronisation einer weiteren Domäne anzupassen

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

      Es wird eine Startkonfiguration erstellt, die das neu angelegte Variablenset verwendet.
4. Passen Sie bei Bedarf weitere Komponenten der Synchronisationskonfiguration an.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- Synchronisation in die Active Directory Domäne konfigurieren auf Seite 32

Schema aktualisieren

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

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

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

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

Um das Schema einer Systemverbindung zu aktualisieren

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

   - ODER -

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

   Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

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

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

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

Beschleunigung der Synchronisation durch Revisionsfilterung

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

Active Directory unterstützt die Revisionsfilterung. Als Revisionszähler wird die Update Sequence Number (USN) der Active Directory Objekte genutzt. Die Update Sequence Number (USN) ist eine fortlaufende Nummer, die bei Veränderungen an Active Directory Objekten inkrementiert wird. Auf jedem Domänen-Controller hat ein Active Directory Objekt eine eigene USN. Bei der Synchronisation wird die höchste USN der rootDSE, die am Domänen-Controller ermittelt werden kann, als Revision in der One Identity Manager-Datenbank gespeichert (Tabelle `DPRRevisionStore`, Spalte `Value`). Dieser Wert wird als Vergleichswert für die Revisionsfilterung bei der nächsten Synchronisation mit dem selben Workflow genutzt. Bei der Synchronisation mit diesem Workflow werden die USN der Active Directory Objekte mit der in der One Identity Manager-Datenbank gespeicherten Revision verglichen. Dabei werden die Objektpaare ermittelt, bei denen mindestens ein Objekt eine neuere USN besitzt als bei der letzten Synchronisation. Auf diese Weise werden nur die Objekte aktualisiert, die sich seit der letzten Synchronisation geändert haben.

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

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

Um die Revisionsfilterung an einem Workflow zuzulassen

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

Um die Revisionsfilterung an einer Startkonfiguration zuzulassen

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

HINWEIS: Beim Einrichten der initialen Synchronisation geben Sie bereits im Projektassistenten an, ob die Revisionsfilterung genutzt werden soll.

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

Nachbehandlung ausstehender Objekte

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

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

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

b. 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 8: Methoden zur Behandlung ausstehender Objekte

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

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 .

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.

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.

Provisionierung von Mitgliedschaften konfigurieren

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

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

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

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

Um die Einzelprovisionierung von Mitgliedschaften zu ermöglichen

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Active Directory**.
3. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
4. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
    - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` oder `CCC_XDateSubItem` hat.
    - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden (beispielsweise `ADSAccountInADSGroup`, `ADSGroupInADSGroup` und `ADSMachineInADSGroup`).
5. Klicken Sie **Merge-Modus**.
6. Speichern Sie die Änderungen.

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

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

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

Um die Standardbedingung wiederherzustellen

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

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

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

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

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

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

Um die Lastverteilung zu konfigurieren

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.
   - Weisen Sie diesen Jobservern die Serverfunktion **Active Directory 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*.

Detaillierte Informationen zum Thema

- Bearbeiten eines Servers auf Seite 81

Unterstützung bei der Analyse von Synchronisationsproblemen

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

- Ergebnisse der Konsistenzprüfung
- Einstellungen zur Revisionsfilterung
- Verwendeter Scope
- Analyse des Synchronisationspuffers
- Zugriffszeiten auf die Objekte in der One Identity Manager-Datenbank und im Zielsystem

Um den Synchronisationsanalysebericht zu erstellen

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

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

Deaktivieren der Synchronisation

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

Um regelmäßige Synchronisationen zu verhindern

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

   Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Verwandte Themen

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Active Directory Domäne auf Seite 22

3

Basisdaten für die Verwaltung einer Active Directory-Umgebung

Für die Verwaltung einer Active Directory-Umgebung im One Identity Manager sind folgende Basisdaten relevant.

- Konfigurationsparameter

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

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

  Weitere Informationen finden Sie unter Konfigurationsparameter für die Verwaltung einer Active Directory-Umgebung auf Seite 206.

- Kontendefinitionen

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

  Weitere Informationen finden Sie unter Kontendefinitionen für Active Directory Benutzerkonten auf Seite 45.

- Kennwortrichtlinien

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

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

Weitere Informationen finden Sie unter Kennwortrichtlinien für Active Directory Benutzerkonten auf Seite 65.

- Initiales Kennwort für neue Benutzerkonten

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

  Weitere Informationen finden Sie unter Initiales Kennwort für neue Active Directory Benutzerkonten auf Seite 76.

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

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

  Weitere Informationen finden Sie unter E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 77.

- Benutzerkontennamen

  Für die Rechtevergabe auf Verzeichnisse und Dateien ist es unter Umständen erforderlich die Benutzerkontennamen wie **Administrators**, **Everyone** oder **Domain Users** sprachabhängig zu hinterlegen.

  Weitere Informationen finden Sie unter Benutzerkontennamen auf Seite 78.

- Zielsystemtypen

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

  Weitere Informationen finden Sie unter Nachbehandlung ausstehender Objekte auf Seite 36.

- Zielsystemverantwortliche

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

  Wenn Sie die Bearbeitungsrechte der Zielsystemverantwortlichen auf einzelne Domänen einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

  Weitere Informationen finden Sie unter Zielsystemverantwortliche auf Seite 79.

- Server

  Für die Verarbeitung der Active Directory spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehören beispielsweise der Synchronisationsserver, Homeserver oder Profilserver.

  Weitere Informationen finden Sie unter Bearbeiten eines Servers auf Seite 81.

Kontendefinitionen für Active Directory Benutzerkonten

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

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

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

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

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

Erstellen einer Kontendefinition

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

2. Wählen Sie in der Ergebnisliste eine Kontendefinition. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

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

Detaillierte Informationen zum Thema

- Stammdaten einer Kontendefinition auf Seite 46

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 9: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Vorausgesetzte Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch mitbestellt oder zugeordnet. Für eine Active Directory Domäne lassen Sie die Angabe leer.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Personen. Erfassen Sie einen Wert zwischen 0 und 1. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.

Eigenschaft	Beschreibung
IT Shop	Angabe, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die Kontendefinition kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.
Automatische Zuweisung zu Personen	Angabe, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Kontendefinition an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition. WICHTIG: Aktivieren Sie diese Option nur, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen! Um die automatische Zuweisung der Kontendefinition an alle Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.
Kontendefinition bei dauerhafter Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei	Angabe zur Zuweisung der Kontendefinition bei verzögertem

Eigenschaft	Beschreibung
verzögertem Löschen beibehalten	Löschen von Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Kontendefinition bei Sicherheitsgefährdung beibehalten	Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen. Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten. Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.
Ressourcentyp	Ressourcentyp zur Gruppierung von Kontendefinitionen.
Freies Feld 01- Freies Feld 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Erstellen der Automatisierungsgrade

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

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

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

Personeneigenschaften zu einem späteren Zeitpunkt geändert, dann werden diese Änderungen an das Benutzerkonto weitergereicht.

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

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

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

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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

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

   - ODER -

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

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

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

Klicken Sie in der Ergebnisliste .

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

Verwandte Themen

- Stammdaten eines Automatisierungsgrades auf Seite 50

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 10: Stammdaten eines Automatisierungsgrades

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

Eigenschaft	Beschreibung
sperren	
Gruppen bei Sicherheitsgefährdung beibehalten	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Angabe, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

Eine Kontendefinition legt fest, nach welchen Regeln die IT Betriebsdaten für die Benutzerkonten gebildet werden, beispielsweise ob der Container für ein Benutzerkonto über die Abteilung, die Kostenstelle, den Standort oder die Geschäftsrolle einer Person gebildet wird, und welche Standardwerte genutzt werden, wenn keine IT Betriebsdaten über die primären Rollen einer Person ermittelt werden können.

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

- Active Directory Container
- Active Directory Homeserver
- Active Directory Profilserver
- Active Directory Terminal Homeserver
- Active Directory Terminal Profilserver
- Gruppen erbbar
- Identität
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **IT Betriebsdaten Abbildungsvorschrift bearbeiten** und

erfassen Sie folgende Informationen.

Tabelle 11: Abbildungsvorschrift für IT Betriebsdaten

Eigenschaft	Beschreibung
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
Quelle	Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen: • Primäre Abteilung • Primärer Standort • Primäre Kostenstelle • Primäre Geschäftsrolle HINWEIS: Verwenden Sie die primäre Geschäftsrolle nur, wenn das Geschäftsrollenmodul vorhanden ist. • keine Angabe Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen.
Standardwert	Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
Immer Standardwert verwenden	Angabe, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.
Benachrichtigung bei Verwendung des Standards	Angabe, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkontos mit Standardwerten** verwendet. Um die Mailvorlage zu ändern, passen Sie den Konfigurationsparameter **TargetSystem | ADS | Accounts | MailTemplateDefaultValues** an.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Erfassen der IT Betriebsdaten auf Seite 53

Erfassen der IT Betriebsdaten

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

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

Beispiel

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

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

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.

3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.

Tabelle 12: IT Betriebsdaten

Eigenschaft	Beschreibung
Wirksam für	Anwendungsbereich der IT Betriebsdaten. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden. Um den Anwendungsbereich festzulegen a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. b. Wählen Sie unter **Tabelle** die Tabelle, die das Zielsystem abbildet oder für eine Kontendefinition die Tabelle `TSBAccountDef`. c. Wählen Sie unter **Wirksam für** das konkrete Zielsystem oder die konkrete Kontendefinition. d. Klicken Sie **OK**.
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript `TSB_ITDataFromOrg` verwenden. Ausführliche Informationen dazu finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.
Wert	Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Erstellen einer Abbildungsvorschrift für IT Betriebsdaten auf Seite 51

IT Betriebsdaten ändern

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

Voraussetzungen

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

  - ODER -

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

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

Um die Bildungsregeln auszuführen

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

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

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

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinition an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

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

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

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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

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

Detaillierte Informationen zum Thema

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 57
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 57
- Kontendefinition an alle Personen zuweisen auf Seite 58
- Kontendefinition direkt an Personen zuweisen auf Seite 59
- Kontendefinition an Systemrollen zuweisen auf Seite 59
- Kontendefinition in den IT Shop aufnehmen auf Seite 60
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 62

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

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

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

Verwandte Themen

- Kontendefinition an Geschäftsrollen zuweisen auf Seite 57
- Kontendefinition an alle Personen zuweisen auf Seite 58
- Kontendefinition direkt an Personen zuweisen auf Seite 59
- Kontendefinition an Systemrollen zuweisen auf Seite 59
- Kontendefinition in den IT Shop aufnehmen auf Seite 60

Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Geschäftsrolle und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 57
- Kontendefinition an alle Personen zuweisen auf Seite 58
- Kontendefinition direkt an Personen zuweisen auf Seite 59
- Kontendefinition an Systemrollen zuweisen auf Seite 59
- Kontendefinition in den IT Shop aufnehmen auf Seite 60

Kontendefinition an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.

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

5. Speichern Sie die Änderungen.

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

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 57
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 57

- Kontendefinition direkt an Personen zuweisen auf Seite 59
- Kontendefinition an Systemrollen zuweisen auf Seite 59
- Kontendefinition in den IT Shop aufnehmen auf Seite 60

Kontendefinition direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 57
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 57
- Kontendefinition an alle Personen zuweisen auf Seite 58
- Kontendefinition an Systemrollen zuweisen auf Seite 59
- Kontendefinition in den IT Shop aufnehmen auf Seite 60

Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 57
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 57
- Kontendefinition an alle Personen zuweisen auf Seite 58
- Kontendefinition direkt an Personen zuweisen auf Seite 59
- Kontendefinition in den IT Shop aufnehmen auf Seite 60

Kontendefinition in den IT Shop aufnehmen

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

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

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

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

Um eine Kontendefinition in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

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

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

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

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

Verwandte Themen

- Stammdaten einer Kontendefinition auf Seite 46
- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 57
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 57
- Kontendefinition an alle Personen zuweisen auf Seite 58
- Kontendefinition direkt an Personen zuweisen auf Seite 59
- Kontendefinition an Systemrollen zuweisen auf Seite 59

Zuweisen der Kontendefinition an ein Zielsystem

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **Active Directory | Domänen** die Domäne.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Wählen Sie in der Auswahlliste **Kontaktdefinition (initial)** die Kontendefinition für die Kontakte.
5. Wählen Sie in der Auswahlliste **E-Mail Kontaktdefinition (initial)** die Kontendefinition für die E-Mail Kontakte.
6. Wählen Sie in der Auswahlliste **E-Mail Benutzerdefinition (initial)** die Kontendefinition für die E-Mail Benutzer.
7. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Automatische Zuordnung von Personen zu Active Directory Benutzerkonten auf Seite 137

Löschen einer Kontendefinition

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

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
    a. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.
    e. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
    a. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **An Personen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.
    e. Speichern Sie die Änderungen.
3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorten.
    a. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Organisationen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Abteilungen, Kostenstellen und Standorte.
    e. Speichern Sie die Änderungen.
4. Entfernen Sie die Zuordnung der Kontendefinition zu Geschäftsrollen.
    a. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
    Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
    d. Speichern Sie die Änderungen.

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

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

   Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

   a. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).

      - ODER -

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

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

   e. Klicken Sie **OK**.

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

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

   a. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

   b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

   e. Speichern Sie die Änderungen.

7. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.

   a. Wählen Sie im Manager in der Kategorie **Active Directory | Domänen** die Domäne.

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

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

   d. Speichern Sie die Änderungen.

8. Löschen Sie die Kontendefinition.

   a. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Klicken Sie , um die Kontendefinition zu löschen.

Kennwortrichtlinien für Active Directory Benutzerkonten

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

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

Detaillierte Informationen zum Thema

- Vordefinierte Kennwortrichtlinien auf Seite 65
- Anwenden einer Kennwortrichtlinie auf Seite 67
- Bearbeiten von Kennwortrichtlinien auf Seite 69
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 72
- Ausschlussliste für Kennwörter auf Seite 75
- Prüfen eines Kennwortes auf Seite 75
- Generieren eines Kennwortes testen auf Seite 76

Vordefinierte Kennwortrichtlinien

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

Kennwortrichtlinie für die Anmeldung am One Identity Manager

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

HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn

keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

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

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

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

Kennwortrichtlinien für Benutzerkonten

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

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

HINWEIS: Bei der Aktualisierung von One Identity Manager Version 7.x auf One Identity Manager Version 8.1.4 werden die Einstellung der Konfigurationsparameter zur Bildung von Kennwörtern auf die zielsystemspezifischen Kennwortrichtlinien umgesetzt.

Für Active Directory ist die Kennwortrichtlinie **Active Directory Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Active Directory Benutzerkonten (`ADSAccount.UserPassword`) einer Active Directory Domäne oder eines Active Directory Containers anwenden.

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

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

HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien, die Einstellungen der globalen Kontenrichtlinien für die Active Directory Domäne sowie die Active Directory Kontenrichtlinien beachtet.

Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die Anforderungen des Zielsystems verstößt.

Verwandte Themen

- Globale Kontenrichtlinien für eine Active Directory Domäne auf Seite 97
- Active Directory Kontenrichtlinien für Active Directory Domänen auf Seite 102

Anwenden einer Kennwortrichtlinie

Für Active Directory ist die Kennwortrichtlinie **Active Directory Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Active Directory Benutzerkonten (`ADSAccount.UserPassword`) einer Active Directory Domäne oder eines Active Directory Containers anwenden.

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

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

HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien, die Einstellungen der globalen Kontenrichtlinien für die Active Directory Domäne sowie die Active Directory Kontenrichtlinien beachtet.

Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die Anforderungen des Zielsystems verstößt.

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

1. Kennwortrichtlinie der Kontendefinition des Benutzerkontos
2. Kennwortrichtlinie des Automatisierungsgrades des Benutzerkontos
3. Kennwortrichtlinie des Active Directory Containers des Benutzerkontos
4. Kennwortrichtlinie der Active Directory Domäne des Benutzerkontos
5. Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** (Standardrichtlinie)

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

Um eine Kennwortrichtlinie neu zuzuweisen

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Klicken Sie im Bereich **Zuweisungen** die Schaltfläche **Hinzufügen** und erfassen Sie

folgende Daten.

Tabelle 13: Zuweisen einer Kennwortrichtlinie

Eigenschaft	Beschreibung
Anwenden auf	Anwendungsbereich der Kennwortrichtlinie. ***Um den Anwendungsbereich festzulegen*** a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. b. Wählen Sie unter **Tabelle** eine der folgenden Referenzen: • Die Tabelle, die die Basisobjekte der Synchronisation enthält. • Um die Kennwortrichtlinie abhängig von der Kontendefinition anzuwenden, wählen Sie die Tabelle `TSBAccountDef`. • Um die Kennwortrichtlinie abhängig vom Automatisierungsgrad anzuwenden, wählen Sie die Tabelle `TSBBehavoir`. c. Wählen Sie unter **Anwenden auf** die Tabelle, die die Basisobjekte enthält. • Wenn Sie die Tabelle mit den Basisobjekten der Synchronisation gewählt haben, dann wählen Sie das konkrete Zielsystem. • Wenn Sie die Tabelle `TSBAccountDef` gewählt haben, dann wählen Sie die konkrete Kontendefinition. • Wenn Sie die Tabelle `TSBBehavior` gewählt haben, dann wählen Sie den konkreten Automatisierungsgrad. d. Klicken Sie **OK**.
Kennwortspalte	Bezeichnung der Kennwortspalte.
Kennwortrichtlinie	Bezeichnung der Kennwortrichtlinie, die angewendet werden soll.

5. Speichern Sie die Änderungen.

Um die Zuweisung einer Kennwortrichtlinie zu ändern

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.

4. Wählen Sie im Bereich **Zuweisungen** die Zuweisung, die Sie ändern möchten.
5. Wählen Sie in der Auswahlliste **Kennwortrichtlinie** die neu anzuwendende Kennwortrichtlinie.
6. Speichern Sie die Änderungen.

Bearbeiten von Kennwortrichtlinien

Um eine Kennwortrichtlinie zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie und wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   -ODER-

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Kennwortrichtlinie auf Seite 69
- Richtlinieneinstellungen auf Seite 70
- Zeichenklassen für Kennwörter auf Seite 71
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 72

Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 14: Stammdaten einer Kennwortrichtlinie

Eigenschaft	Bedeutung
Anzeigename	Bezeichnung der Kennwortrichtlinie. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.Übersetzen Sie den eingegebenen Text über die Schaltfläche .
Fehlermeldung	Kundenspezifische Fehlermeldung, die ausgegeben wird, wenn die Richtlinie nicht erfüllt wird. Übersetzen Sie den eingegebenen Text über die Schaltfläche .

Eigenschaft	Bedeutung
Eigentümer (Anwendungsrolle)	Anwendungsrolle, deren Mitglieder die Kennwortrichtlinie konfigurieren können.
Standardrichtlinie	Kennzeichnung als Standardrichtlinie für Kennwörter. HINWEIS: Die Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** ist als Standardrichtlinie gekennzeichnet. Diese Kennwortrichtlinie wird angewendet, wenn keine andere Kennwortrichtlinie für Personen, Benutzerkonten oder Systembenutzer ermittelt werden kann.

Richtlinieneinstellungen

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

Tabelle 15: Richtlinieneinstellungen

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

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

Zeichenklassen für Kennwörter

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

Tabelle 16: Zeichenklassen für Kennwörter

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

Eigenschaft	Bedeutung
Zulässige Sonderzeichen	Liste zulässiger Sonderzeichen.
Max. identische Zeichen insgesamt	Maximale Anzahl identischer Zeichen, die insgesamt im Kennwort vorkommen dürfen.
Max. identische Zeichen aufeinanderfolgend	Maximale Anzahl identischer Zeichen, die nacheinander wiederholt werden können.
Unzulässige Sonderzeichen	Liste unzulässiger Sonderzeichen.
Keine Kleinbuchstaben erzeugen	Angabe, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keinen Großbuchstaben erzeugen	Angabe, ob ein generiertes Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Ziffern erzeugen	Angabe, ob ein generiertes Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Sonderzeichen erzeugen	Angabe, ob ein generiertes Kennwort Sonderzeichen enthalten darf. Ist die Option aktiviert, sind nur Buchstaben, Zahlen und Leerzeichen in Kennwörtern erlaubt. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.

Kundenspezifische Skripte für Kennwortanforderungen

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

Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 73
- Skript zum Generieren eines Kennwortes auf Seite 74

Skript zum Prüfen eines Kennwortes

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

Syntax für Prüfskripte

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

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Kennwort, das zu prüfen ist

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

Beispiel für ein Skript zum Prüfen eines Kennwortes

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

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

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Kennwortrichtlinien.**

b. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.

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

d. Tragen Sie auf dem Tabreiter **Skripte** im Eingabefeld **Prüfskript** den Namen des Skriptes ein, das zum Prüfen eines Kennwortes verwendet wird.

e. Speichern Sie die Änderungen.

Verwandte Themen

- Skript zum Generieren eines Kennwortes auf Seite 74

Skript zum Generieren eines Kennwortes

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

Syntax für Generierungsskripte

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

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Generiertes Kennwort

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

Beispiel für ein Skript zum Generieren eines Kennwortes

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

```
Public Sub CCC_PwdGenerate( policy As VI.DB.Passwords.PasswordPolicy, spwd As
System.Security.SecureString)
    Dim pwd = spwd.ToInsecureArray()
    ' replace invalid characters at first position
    If pwd.Length>0
        If pwd(0)="?" Or pwd(0)="!"
            spwd.SetAt(0, CChar("_"))
        End If
    End If
End Sub
```

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

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

Verwandte Themen

- Skript zum Prüfen eines Kennwortes auf Seite 73

Ausschlussliste für Kennwörter

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

HINWEIS: Die Ausschlussliste ist global für alle Kennwortrichtlinien gültig.

Um einen Begriff in die Ausschlussliste aufzunehmen

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

Prüfen eines Kennwortes

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

Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht

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

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

Generieren eines Kennwortes testen

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

Um ein Kennwort zu generieren, das der Kennwortrichtlinie entspricht

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

   Das generierte Kennwort wird angezeigt.

Initiales Kennwort für neue Active Directory Benutzerkonten

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

- Erstellen Sie Benutzerkonten manuell und tragen Sie in den Stammdaten der Benutzerkonten ein Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | Accounts | InitialRandomPassword**.
- Verwenden Sie zielsystemspezifische Kennwortrichtlinien und definieren Sie in den Kennwortrichtlinien die Zeichenklassen, die das Kennwort enthalten muss.
- Legen Sie fest, an welche Person das initiale Kennwort per E-Mail versendet wird.

- Verwenden Sie das zentrale Kennwort der Person. Das zentrale Kennwort der zugeordneten Person wird auf das Kennwort des Benutzerkontos abgebildet. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Kennwortrichtlinien für Active Directory Benutzerkonten auf Seite 65
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 77

E-Mail-Benachrichtigungen über Anmeldeinformationen

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

Um Benachrichtigungen zu nutzen, sind folgende Voraussetzungen zu erfüllen:

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

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

Um die initialen Anmeldeinformationen per E-Mail zu versenden

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

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

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

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

Benutzerkontennamen

Für die Rechtevergabe auf Verzeichnisse und Dateien ist es unter Umständen erforderlich die Benutzerkontennamen wie **Administrators**, **Everyone** oder **Domain Users** sprachabhängig zu hinterlegen.

HINWEIS: Die Standardsprache für die Benutzerkontennamen ist Englisch.

Um Benutzerkontennamen zu bearbeiten

1. Wählen Sie die Kategorie **Active Directory | Basisdaten zur Konfiguration | Benutzerkontennamen**.
2. Wählen Sie einen Eintrag in der Ergebnisliste aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.

   - ODER-

   Klicken Sie in der Ergebnisliste .
3. Erfassen Sie die englische Bezeichnung des Benutzerkontennamens. Übersetzen Sie den eingegebenen Text über die Schaltfläche .
4. Speichern Sie die Änderungen.

Zielsystemverantwortliche

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

Wenn Sie die Bearbeitungsrechte der Zielsystemverantwortlichen auf einzelne Domänen einschränken wollen, definieren Sie weitere Anwendungsrollen. Die Anwendungsrollen müssen der Standardanwendungsrolle untergeordnet sein.

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

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

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

Tabelle 17: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | Active Directory** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.

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

Um initial Personen als Zielsystemadministrator festzulegen

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

Um initial Personen in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

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

Um als Zielsystemverantwortlicher weitere Personen als Zielsystemverantwortliche zu berechtigen

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

Um Zielsystemverantwortliche für einzelne Domänen festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **Active Directory | Domänen**.
3. Wählen Sie in der Ergebnisliste die Domäne.
4. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
5. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste

Zielsystemverantwortliche die Anwendungsrolle.

- ODER -

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

a. Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | Active Directory** zu.

b. Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.

6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, die Domäne im One Identity Manager zu bearbeiten.

HINWEIS: Sie können Zielsystemverantwortliche auch für einzelne Container festlegen. Die Zielsystemverantwortlichen eines Container sind berechtigt, die Objekte dieses Containers zu bearbeiten.

Verwandte Themen

- One Identity Manager Benutzer für die Verwaltung einer Active Directory-Umgebung auf Seite 10
- Allgemeine Stammdaten einer Active Directory Domäne auf Seite 94
- Stammdaten eines Active Directory Containers auf Seite 192

Bearbeiten eines Servers

Für die Verarbeitung der Active Directory spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehören beispielsweise der Synchronisationsserver, Homeserver oder Profilserver.

Um die Funktion eines Servers zu definieren, haben Sie mehrere Möglichkeiten:

- Erstellen Sie im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** einen Eintrag für den Jobserver. Ausführliche Informationen dazu finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Wählen Sie im Manager in der Kategorie **Active Directory | Basisdaten zur Konfiguration | Server** einen Eintrag für den Jobserver und bearbeiten Sie die Stammdaten des Jobservers.

  Nutzen Sie dieses Verfahren, wenn der Jobserver bereits im One Identity Manager bekannt ist und Sie für den Jobserver spezielle Funktionen wie beispielsweise Homeserver oder Profilserver konfigurieren möchten.

HINWEIS: Damit ein Server seine Funktion im One Identity Manager Netzwerk ausführen kann, muss ein One Identity Manager Service installiert, konfiguriert und gestartet sein. Gehen Sie dazu wie im *One Identity Manager Installationshandbuch* beschrieben vor.

Um einen Jobserver und seine Funktionen zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Active Directory | Basisdaten zur Konfiguration | Server**.
2. Wählen Sie in der Ergebnisliste den Jobserver-Eintrag.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für den Jobserver.
5. Wählen Sie die Aufgabe **Serverfunktionen zuweisen** und legen Sie die Serverfunktionen fest.
6. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Stammdaten eines Jobservers auf Seite 82
- Festlegen der Serverfunktionen auf Seite 85
- Vorbereiten eines Home- und Profilservers für die Anlage von Benutzerverzeichnissen auf Seite 87

Stammdaten eines Jobservers

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

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

Tabelle 18: Eigenschaften eines Jobservers

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

Eigenschaft	Bedeutung
Lokaler Active Directory DC	Für Homeserver oder Profilserver auf einem Memberserver, können Sie hier einen räumlich näher stehenden Domänen-Controller eintragen. Über diesen wird bei der Verarbeitung der Prozesse auf das Active Directory zugegriffen. Wird kein Server eingetragen, dann wird der zentrale Domänen-Controller der Domäne verwendet.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Max. Anzahl Homes	Maximale Anzahl der zu verwaltenden Homeverzeichnisse, wenn es sich um einen Homeserver handelt. Diese Anzahl wird bei Neuvergabe eines Homeverzeichnisses für einen Benutzer mit der Anzahl der (laut Datenbank) auf dem Server existierenden Homeverzeichnisse (Angelegte Homes) verglichen. Ist diese Anzahl kleiner als die angegebene maximale Anzahl der Homeverzeichnisse, wird die Anlage eines neuen Homeverzeichnisses zugelassen. Ansonsten wird die Anlage eines neuen Homeverzeichnisses verwehrt.
Angelegte Homes	Anzahl der bereits auf dem Homeserver vorhandenen Homeverzeichnisse.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme Robocopy und rsync unterstützt. Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm Robocopy und zwischen Servern mit einem Linux Betriebssystem mit dem Programm rsync. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt, das beide Server unterstützen.
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Max. Homespeicherplatz [MB]	Maximal zulässiger Speicherplatz für Homeverzeichnisse in MB auf dem Homeserver. Diese Angabe wird bei der Vergabe der Homeverzeichnisse berücksichtigt.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.

Eigenschaft	Bedeutung
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	Angabe, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur `QBM_PJobQueueLoad` aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Angabe, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen

Eigenschaft	Bedeutung
	Rechten im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Kein automatisches Softwareupdate	Angabe, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Angabe, ob gerade eine Softwareaktualisierung ausgeführt wird.
Letzter Abrufzeitpunkt	Zeitpunkt der letzten Prozessabholung.
Letzte Timeout Prüfung	Zeitpunkt der letzten Prüfung für geladene Prozessschritte, deren Auslieferung den Wert im Konfigurationsparameter **Common | Jobservice | LoadedJobsTimeOut** überschreitet.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 85

Festlegen der Serverfunktionen

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

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

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

Tabelle 19: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
Active Directory Konnektor	Server, auf dem der Active Directory Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem Active Directory aus.
CSV Konnektor	Server, auf dem der CSV Konnektor für die Synchronisation installiert ist.

Serverfunktion	Anmerkungen
Domänen-Controller	Active Directory Domänen-Controller. Server, die nicht als Domänen-Controller gekennzeichnet sind, werden als Memberserver betrachtet.
Druckserver	Server, der als Druckserver arbeitet.
Generischer Server	Server für die generische Synchronisation mit einem kundendefinierten Zielsystem.
Homeserver	Server zur Anlage von Homeverzeichnissen für Benutzerkonten.
Aktualisierungsserver	Der Server führt die automatische Softwareaktualisierung aller anderen Server aus. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Der Server kann SQL Aufträge ausführen. Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten.
Nativer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.
One Identity Manager-Datenbankkonnektor	Server, auf dem der One Identity Manager Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Manager aus.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
Primärer Domänen-Controller	Primärer Domänen-Controller.
Profilserver	Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten.
SAM Synchronisationsserver	Server für die Synchronisation mit einem SMB-basierten Zielsystem aus.

Serverfunktion	Anmerkungen
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell Konnektor	Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen.

Verwandte Themen

- Stammdaten eines Jobservers auf Seite 82

Vorbereiten eines Home- und Profilservers für die Anlage von Benutzerverzeichnissen

Bei der Anlage der Homeverzeichnisse und der Profilverzeichnissse der Benutzerkonten werden ein Homeserver und ein Profilserver erwartet.

Um Homeserver und Profilserver bekanntzugeben

- Aktivieren Sie im Designer die Konfigurationsparameter **TargetSystem | ADS | AutoCreateServers** und **TargetSystem | ADS | AutoCreateServers | PreferredLanguage**.

  Sind die Konfigurationsparameter aktiviert, werden bei der Synchronisation von Benutzerkonten automatisch Einträge für fehlende Homeserver und Profilserver erstellt.

- ODER -

1. Wählen Sie die Kategorie **Active Directory | Basisdaten zur Konfiguration | Server**.
2. Wählen Sie in der Ergebnisliste den Jobserver-Eintrag.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für den Jobserver.
5. Wählen Sie die Aufgabe **Serverfunktionen zuweisen** und legen Sie die Serverfunktionen **Homeserver** und **Profilserver** fest.
6. Speichern Sie die Änderungen.

Für die Erzeugung der Homeverzeichnisse und Profilverzeichnisse können Sie weitere Konfigurationseinstellungen nutzen.

- Wenn das Homeverzeichnis eines Benutzers beim Anmelden verbunden werden soll, aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | User | ConnectHomeDir**.
- Um das Benutzerprofil im Homeverzeichnis des Benutzers anzulegen, aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | User | PropertyMapping | ProfileFromHome**.
- Für die Erzeugung der Homeverzeichnisse können Sie eine Batchdatei einsetzen, von deren Ausführungsergebnis letztendlich die Aktivierung des Homeverzeichnisses abhängig ist.
- Für die Erzeugung der Profilverzeichnisse können Sie auf dem Profilserver eine Vorlagenstruktur erstellen, die bei der Erzeugung der Profilverzeichnisse genutzt wird.
- Die Vergabe von Berechtigungen auf die Homeverzeichnisse und Profilverzeichnisse kann durch den One Identity Manager Service erfolgen.

Verwandte Themen

- Erzeugen von Homeverzeichnissen über Batchdateien auf Seite 88
- Unterstützung von mehreren Profilverzeichnissen auf Seite 89
- Zugriffsberechtigungen auf Homeverzeichnisse und Profilverzeichnisse auf Seite 91
- Stammdaten eines Jobservers auf Seite 82
- Festlegen der Serverfunktionen auf Seite 85

Erzeugen von Homeverzeichnissen über Batchdateien

Um speziellen Anforderungen einzelner Netzwerkumgebungen gerecht zu werden, können Sie bei der Erstellung eines Homeverzeichnisses durch den One Identity Manager Service eine Batchdatei einsetzen, deren Ausführung beim Erstellen des Verzeichnisses erfolgt und von deren Ausführungsergebnis die letztendliche Aktivierung des Homeverzeichnisses abhängig ist.

Um diese Funktion zu nutzen, muss auf allen Homeservern eine Netlogonfreigabe vorhanden sein. In der Netlogonfreigabe werden Unterverzeichnisse angelegt, welche dem NetBIOS Namen der Domäne entsprechen. Ist in diesen Verzeichnissen eine Batchdatei mit dem Namen `HomePre.CMD` vorhanden, wird diese vor dem Anlegen des Homeverzeichnisses ausgeführt. Endet die Ausführung dieser Batchdatei mit einem Fehler (das heißt, mit einem Errorlevel <> 0), wird das Anlegen des Homeverzeichnisses abgebrochen.

Der Batchdatei `HomePre.CMD` übergeben Sie die folgenden Kommandozeilenparameter, die innerhalb der Ausführung weiter verwendet werden können (in der Reihenfolge der Aufzählung, es werden die Spaltennamen der Datenbank verwendet):

```
SAMAccountName (aus Tabelle ADSAccount)
```

```
Ident_Domain (aus Tabelle ADSAccount)
```

Ident_Server (aus Tabelle QBMServer)

SharedAs (aus Tabelle ADSAccount)

HomeDirPath (aus Tabelle ADSAccount)

HomeShare (aus Tabelle ADSAccount)

Nach dem Anlegen eines Homeverzeichnisses können Sie nochmals eine Batchdatei ausführen. Diese muss sich an derselben Stelle, wie oben erwähnt, befinden und den Namen HomePost.CMD tragen. Die Stellung der Parameter geschieht identisch zur HomePre.CMD. Es erfolgt lediglich keine Verarbeitung des Exitcodes (Errorlevels).

Beispiel

Es wird ein Benutzerkonto **Test1** in der Domäne **Dom2** angelegt. Sein Homeverzeichnis soll auf den Server **Serv3** in der Freigabe **Share7** mit dem Namen **TestHome6** angelegt und als **TestShare5** freigegeben werden. Auf dem ausführenden Homeserver **ServHome** befinden sich die Dateien HomePre.CMD und HomePost.CMD im Verzeichnis \\ServHome\Netlogon\Dom2.

Batchaufruf vor dem Erzeugen des Homes:

```
\\ServHome\Netlogon\Dom2\HomePre.CMD Test1 Dom2 Serv3 TestShare5 TestHome6 Share7
```

Gibt die Batchausführung einen Exitcode 0 zurück, wird das Homeverzeichnis erzeugt. Sonst wird die Verarbeitung mit einem Protokolleintrag abgebrochen.

Batchaufruf nach dem Erzeugen des Homes:

```
\\ServHome\Netlogon\Dom2\HomePost.CMD Test1 Dom2 Serv3 TestShare5 TestHome6 Share7
```

Unterstützung von mehreren Profilverzeichnissen

Die unterschiedlichen Windows Betriebssystemversionen verwenden unterschiedliche Speicherorte für Roamingbenutzerprofile. Genaue Informationen zur Ablage der Roamingbenutzerprofile finden Sie in der MicrosoftTechNet Library.

Um die Abbildung der Roamingbenutzerprofile im One Identity Manager zu erreichen.

- Stellen Sie auf dem Profilserver eine Vorlagenstruktur für die Benutzerprofile zur Verfügung.

  Beispiel für eine Vorlagenstruktur für Benutzerprofile auf dem Profilserver

  ```
  PROFILE
      UserProfile
          All required folders/files
  ```

```
UserProfile.V2
     All required folders/files
UserProfile.V3
     All required folders/files
UserProfile.V4
     All required folders/files
```

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | Accounts | ProfileFixedString** und legen Sie den Teil des Benutzerprofilverzeichnispfades fest, der an den Standardprofilpfad angehängt werden soll. Der Standardwert ist `UserProfile`.

Als Ergebnis werden die Verzeichnispfade für die Benutzerprofile in der Standardinstallation folgendermaßen gebildet.

- Wenn das Profilverzeichnis im Homeverzeichnis erzeugt wird:

  `\\Servername\HOMES\Username$\PROFILES\UserProfile`

- Wenn das Profilverzeichnis nicht im Homeverzeichnis erzeugt wird:

  `\\Servername\PROFILES\Username\UserProfile`

Nach Verarbeitung der Prozesse sind die folgenden Verzeichnisse vorhanden.

- Wenn das Profilverzeichnis im Homeverzeichnis erzeugt wird:

  `\\Servername\HOMES\Username$\PROFILES\UserProfile`

  `\\Servername\HOMES\Username$\PROFILES\UserProfile.v2`

  `\\Servername\HOMES\Username$\PROFILES\UserProfile.v3`

  `\\Servername\HOMES\Username$\PROFILES\UserProfile.v4`

- Wenn das Profilverzeichnis nicht im Homeverzeichnis erzeugt wird:

  `\\Servername\PROFILES\Username\UserProfile`

  `\\Servername\PROFILES\Username\UserProfile.v2`

  `\\Servername\PROFILES\Username\UserProfile.v3`

  `\\Servername\PROFILES\Username\UserProfile.v4`

Die Verzeichnispfade für die Ablage auf einem Terminalserver werden analog gebildet. Passen Sie für diesen Fall im Designer den Konfigurationsparameter **TargetSystem | ADS | Accounts | TProfileFixedString** an. Legen Sie im Konfigurationsparameter den Teil des Benutzerprofilverzeichnispfades fest, der an den Standardprofilpfad auf einem Terminalserver angehängt werden soll. Der Standardwert ist `UserProfile`.

Zugriffsberechtigungen auf Homeverzeichnisse und Profilverzeichnisse

Tabelle 20: Konfigurationsparameter für die Einrichtung von Benutzerverzeichnissen

Konfigurationsparameter	Bedeutung
QER | Person | User | AccessRights	Der Konfigurationsparameter erlaubt die Konfiguration der Zugriffsrechte auf Benutzerverzeichnisse.

HINWEIS: Für die Rechtevergabe auf Verzeichnisse und Dateien ist es unter Umständen erforderlich die Benutzerkontennamen wie **Administrators**, **Everyone** oder **Domain Users** sprachabhängig zu hinterlegen. Die Standardsprache für die Benutzerkontennamen ist Englisch.

Um Zugriffsrechte auf das Homeverzeichnis zu vergeben

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | User | AccessRights | HomeDir** und seine untergeordneten Konfigurationsparameter und tragen Sie die Zugriffsrechte in den Konfigurationsparametern ein.

  Die Vergabe der Zugriffsrechte auf das Homeverzeichnis erfolgt durch den One Identity Manager Service.

Tabelle 21: Konfigurationsparameter für Zugriffrsechte auf das Homeverzeichnis

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Person | User | AccessRights | HomeDir	Konfiguration der Zugriffsrechte auf das Homeverzeichnis eines Benutzers. Die Berechtigungen werden über die untergeordneten Parameter festgelegt.
QER | Person | User | AccessRights | HomeDir | EveryOne	Berechtigung von **Everyone** auf das Homeverzeichnis eines Benutzers. Standardmäßig: `-r-w-x`
QER | Person | User | AccessRights | HomeDir | User	Berechtigung des Benutzers auf sein Homeverzeichnis. Standardmäßig: `+r+w-x`

Um Zugriffsrechte auf das Profilverzeichnis zu vergeben

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | User | AccessRights | ProfileDir** und sein untergeordneten Konfigurationsparameter und tragen Sie die Zugriffsrechte in den Konfigurationsparametern ein.

  Die Vergabe der Zugriffsrechte auf das Profilverzeichnis erfolgt durch den One Identity Manager Service.

Tabelle 22: Konfigurationsparameter für Zugriffsrechte auf das Profilverzeichnis

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Person | User | AccessRights | ProfileDir	Konfiguration der Zugriffsrechte auf das Profilverzeichnis eines Benutzers. Die Berechtigungen werden über die untergeordneten Parameter festgelegt.
QER | Person | User | AccessRights | ProfileDir | EveryOne	Berechtigung von **Everyone** auf das Profilverzeichnis eines Benutzers. Standardmäßig: `-r-w-x`
QER | Person | User | AccessRights | ProfileDir | User	Berechtigung des Benutzers auf sein Profilverzeichnis. Standardmäßig: `+r+w-x`

Um Zugriffsrechte auf das Homeverzeichnis auf einem Terminalserver zu vergeben

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | User | AccessRights | TerminalHomeDir** und seine untergeordneten Konfigurationsparameter und tragen Sie die Zugriffsrechte in den Konfigurationsparametern ein.

  Die Vergabe der Zugriffsrechte auf das Homeverzeichnis erfolgt durch den One Identity Manager Service.

Tabelle 23: Konfigurationsparameter für Zugriffsrechte auf das Homeverzeichnis auf einem Terminalserver

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Person | User | AccessRights | TerminalHomeDir	Konfiguration der Zugriffsrechte auf das Terminalserver-Homeverzeichnis eines Active Directory Benutzerkontos. Die Berechtigungen werden über die untergeordneten Parameter festgelegt.
QER | Person | User | AccessRights | TerminalHomeDir | EveryOne	Berechtigung von **Everyone** auf das Terminalserver-Homeverzeichnis eines Benutzers. Standardmäßig: `-r-w-x`
QER | Person | User | AccessRights | TerminalHomeDir | User	Berechtigung des Benutzers auf sein Terminalserver-Homeverzeichnis. Standardmäßig: `+r+w-x`

Um Zugriffsrechte auf das Profilverzeichnis auf einem Terminalserver zu vergeben

- Aktivieren Sie im Designer den Konfigurationsparameter **QER | Person | User | AccessRights | TerminalProfileDir** und seine untergeordneten Konfigurationsparameter und tragen Sie die Zugriffsrechte in den

Konfigurationsparametern ein.

Die Vergabe der Zugriffsrechte auf das Profilverzeichnis erfolgt durch den One Identity Manager Service.

Tabelle 24: Konfigurationsparameter für Zugriffsrechte auf das Profilverzeichnis auf einem Terminalserver

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Person | User | AccessRights | TerminalProfileDir	Konfiguration der Zugriffsrechte auf das TerminalServer-Profilverzeichnis eines Active Directory Benutzerkontos. Die Berechtigungen werden über die untergeordneten Parameter festgelegt.
QER | Person | User | AccessRights | TerminalProfileDir | EveryOne	Berechtigung von **Everyone** auf das Terminalserver-Profilverzeichnis eines Benutzers. Standardmäßig: `-r-w-x`
QER | Person | User | AccessRights | TerminalProfileDir | User	Berechtigung des Benutzers auf sein Terminalserver-Profilverzeichnis. Standardmäßig: `+r+w-x`

Verwandte Themen

- Benutzerkontennamen auf Seite 78

Active Directory Domänen

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 die Kategorie **Active Directory | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für eine Domäne.
5. Speichern Sie die Änderungen.

Allgemeine Stammdaten einer Active Directory Domäne

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

Tabelle 25: Stammdaten einer Domäne

Eigenschaft	Beschreibung
Domäne	NetBIOS Name der Domäne. Dieser entspricht dem Prä-Windows 2000 Domänennamen. Eine nachträgliche Änderung des Domänennamens ist nicht möglich.
Übergeordnete Domäne	Übergeordnete Domäne zur Abbildung einer hierarchischen Domänenstruktur. Der vollständige Domänenname und der definierte Name werden dann automatisch durch Bildungsregeln aktualisiert.
Domänensubtyp	Funktionsebene des Active Directory. Auf den Funktionsebenen sind verschiedene Features im Active Directory verfügbar. Welche Funktionsebene das eingesetzte

Eigenschaft	Beschreibung
	Windows Betriebssystem des Domänen-Controllers unterstützt entnehmen Sie der Dokumentation zum eingesetzten Windows Server. Im One Identity Manager werden die Funktionsebenen unterstützt: • Windows Server 2000 (Win2000) • Windows Server 2003 einheitlich (Win2003 native) • Windows Server 2003 gemischt (Win2003 mixed) • Windows Server 2008 (Win2008) • Windows Server 2008 R2 (Win2008 R2) • Windows Server 2012 (Win2012) • Windows Server 2012 R2 (Win2012 R2) • Windows Server 2016 (Win2016)
Anzeigename	Anzeigename zur Anzeige der Domäne in der Benutzeroberfläche. Initial wird der NetBIOS Name der Domäne übernommen; den Anzeigenamen können Sie jedoch ändern.
Kontendefinition (initial)	Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diese Domäne die automatische Zuordnung von Personen zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet. Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.
Kontaktdefinition (initial)	Initiale Kontendefinition zur Erzeugung von Kontakten. Diese Kontendefinition wird verwendet, wenn für diese Domäne die automatische Zuordnung von Personen zu Kontakten genutzt wird und dabei bereits verwaltete Kontaken (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet. Ist keine Kontendefinition angegeben, werden die Kontakten nur mit der Person verbunden (Zustand **Linked**). Dies ist beispielsweise bei der initialen Synchronisation der Fall.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen der Domäne festgelegt sind. Die Zielsystemverantwortlichen

Eigenschaft	Beschreibung
	bearbeiten nur die Objekte der Domäne, der sie zugeordnet sind. Jeder Domäne können somit andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle, deren Mitglieder verantwortlich für die Administration dieser Domäne sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Synchronisiert durch	Art der Synchronisation, über welche die Daten zwischen der Domäne und dem One Identity Manager synchronisiert werden. Sobald Objekte für diese Domäne im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden. Beim Erstellen einer Domäne mit dem Synchronization Editor wird **One Identity Manager** verwendet. **Tabelle 26: Zulässige Werte** **Wert** / **Synchronisation durch** / **Provisionierung durch** One Identity Manager / Active Directory Konnektor / Active Directory Konnektor Keine Synchronisation / keine / keine HINWEIS: Wenn Sie **Keine Synchronisation** festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- Automatische Zuordnung von Personen zu Active Directory Benutzerkonten auf Seite 137
- Zielsystemverantwortliche auf Seite 79
- Informationen zur Active Directory Gesamtstruktur auf Seite 100

Globale Kontenrichtlinien für eine Active Directory Domäne

Beim Einrichten eines Benutzerkontos werden die global festgelegten Kontenrichtlinien und Angaben für die Kennwortvergabe gültig. Diese Einstellungen nehmen Sie an der Domäne vor. Die Kontenrichtlinien gelten bei der Neuanlage von Benutzerkonten.

Auf dem Tabreiter **Kontenrichtlinien** erfassen Sie die folgenden Stammdaten.

Tabelle 27: Kontenrichtlinien einer Domäne

Eigenschaft	Beschreibung
Min. Kennwortlänge	Minimale Länge des Kennwortes. Geben Sie die minimale Anzahl von Zeichen an, die ein Kennwort haben muss.
Min. Kennwortalter	Minimales Alter des Kennwortes. Tragen Sie die Zeitspanne ein, in der ein Kennwort benutzt werden muss, bevor der Benutzer das Kennwort ändern darf.
Max. Kennwortalter	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Hat ein Benutzer diese Anzahl erreicht, wird das Benutzerkonto gesperrt.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten 5 Kennwörter des Benutzers gespeichert.
Dauer der Sperrung [min]	Dauer der Sperrung in Minuten. Geben Sie an, für welchen Zeitraum die Benutzerkonten gesperrt werden, bevor sie automatisch zurückgesetzt werden.
Konto zurücksetzen [min]	Dauer bis zum Zurücksetzen des Benutzerkontos in Minuten. Geben Sie an, für welchen Zeitraum zwischen zwei ungültigen Kennworteingaben ein Benutzerkonto gesperrt werden soll.

Für Domänen ab der Funktionsebene **Windows Server 2008 R2** können Sie weitere Richtlinien definieren. Zusätzlich können Sie im One Identity Manager eigene Kennwortrichtlinien definieren, die auf die Kennwörter der Benutzerkonten angewendet werden.

HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien, die Einstellungen der globalen Kontenrichtlinien für die Active Directory Domäne sowie die Active Directory Kontenrichtlinien beachtet.

Verwandte Themen

- Kennwortrichtlinien für Active Directory Benutzerkonten auf Seite 65
- Active Directory Kontenrichtlinien für Active Directory Domänen auf Seite 102
- Kennwortdaten eines Active Directory Benutzerkontos auf Seite 122

Active Directory spezifische Stammdaten einer Active Directory Domäne

Auf dem Tabreiter **Active Directory** erfassen Sie die folgenden Stammdaten.

Tabelle 28: Angaben zum Active Directory

Eigenschaft	Beschreibung
Domänenname (pre Win2000)	Prä-Windows 2000 Domänenname.

Vollständiger Domänennamen	Domänennamen der Domäne gemäß DNS Syntax.
	`Name dieser Domäne.Name der übergeordneten Domäne.Name der Stammdomäne`
	Beispiel
	`Doku.Testlab.dd`

Kontomanager	Verantwortlicher für die Domäne. ***Um einen Kontomanager festzulegen*** 1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, welche die Konto-manager abbildet. 3. Wählen Sie unter **Kontomanager** den Verantwortlichen. 4. Klicken Sie **OK**.
Definierter Name	Definierter Name der Domäne. Der definierte Name wird per Bildungsregel aus dem vollständigen Domänennamen ermittelt und sollte nicht bearbeitet werden.
Gesamtstruktur	Name der Gesamtstruktur, zu der die Domäne gehört. Der Name ist anzugeben, wenn Gruppenmitgliedschaften über Domänengrenzen hinweg abgebildet werden.
Papierkorb aktiviert	Angabe, ob der Papierkorb aktiviert ist (ab Funktionsebene

Eigenschaft	Beschreibung
	Windows Server 2008 R2). Die Eigenschaft wird durch die Synchronisation eingelesen und sollte im One Identity Manager nicht bearbeitet werden.
Aufbewahrungsdauer	Aufbewahrungsdauer von Objekten im Papierkorb (ab Funktionsebene **Windows Server 2008 R2**). Die Eigenschaft wird durch die Synchronisation eingelesen und sollte im One Identity Manager nicht bearbeitet werden.
Komplexe Kennwörter	Angabe, ob in der Domäne komplexe Kennwörter eingesetzt werden. Komplexe Kennwörter müssen bestimmte Mindestanforderungen erfüllen. Für weitere Informationen lesen Sie die Dokumentation zum eingesetzten Windows Server. Für Domänen ab der Funktionsebenen **Windows Server 2008 R2** ist es möglich diese Einstellung über Kontenrichtlinien zu definieren.
Standard-Homelaufwerk	Standard-Homelaufwerk, welches bei der Anmeldung eines Benutzers verbunden werden soll.
Strukturelle Objektklasse	Strukturelle Objektklasse, die den Typ des Objektes repräsentiert. Standardmäßig werden die Domänen im One Identity Manager mit der Objektklasse `DOMAINDNS` angelegt.
Objektklasse	Liste von Klassen, die die Attribute dieses Objektes definieren. Als Objektklassen werden die Klassen angeboten, die durch die Synchronisation aus der Active Directory-Umgebung in die Datenbank eingelesen wurden. Sie können jedoch zusätzliche Objektklassen in das Eingabefeld eintragen.

Verwandte Themen

- Zulässigkeit von Gruppenmitgliedschaften auf Seite 163
- Löschen und Wiederherstellen von Active Directory Benutzerkonten auf Seite 146
- Active Directory Kontenrichtlinien für Active Directory Domänen auf Seite 102
- Vorbereiten eines Home- und Profilservers für die Anlage von Benutzerverzeichnissen auf Seite 87

Festlegen der Kategorien für die Vererbung von Active Directory Gruppen

Im One Identity Manager können Gruppen selektiv an die Benutzerkonten und Kontakte vererbt werden. Dazu werden die Gruppen und die Benutzerkonten (Kontakte) in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält die Tabellen, in denen die Benutzerkonten (Kontakte) und die Gruppen abgebildet werden. In der Tabelle für Benutzerkonten (Kontakte) legen Sie Ihre Kategorien für die Benutzerkonten (Kontakte) fest. In Gruppentabelle geben Sie Ihre Kategorien für die Gruppen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

Um Kategorien zu definieren

1. Wählen Sie die Kategorie **Active Directory | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wechseln Sie auf den Tabreiter **Kategorien**.
5. Öffnen Sie den jeweiligen Basisknoten einer Tabelle.
6. Aktivieren Sie die Kategorie per Maus-Doppelklick auf das Symbol .
7. Tragen Sie eine beliebige Benennung der Kategorie für Benutzerkonten, Kontakte und Gruppen in der verwendeten Anmeldesprache ein.
8. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbung von Active Directory Gruppen anhand von Kategorien auf Seite 181

Informationen zur Active Directory Gesamtstruktur

Die Informationen zur Gesamtstruktur werden im One Identity Manager benötigt, um Vertrauensstellungen zwischen Domänen zu definieren und Gruppenmitgliedschaften über Domänengrenzen hinweg abzubilden.

Die Informationen zur Active Directory Gesamtstruktur werden durch die Synchronisation in den One Identity Manager eingelesen.

Um Informationen zu einer Gesamtstruktur anzuzeigen

1. Wählen Sie die Kategorie **Active Directory | Gesamtstruktur**.
2. Wählen Sie in der Ergebnisliste eine Gesamtstruktur.
3. Um die Domänen einer Gesamtstruktur anzuzeigen, wählen Sie die Aufgabe **Überblick über die Gesamtstruktur**.
4. Um die Stammdaten einer Gesamtstruktur anzuzeigen, wählen Sie die Aufgabe **Stammdaten bearbeiten.**

Verwandte Themen

- Vertrauensstellungen zwischen Active Directory Domänen auf Seite 101
- Zulässigkeit von Gruppenmitgliedschaften auf Seite 163

Vertrauensstellungen zwischen Active Directory Domänen

Zur Erläuterung des Konzeptes der Vertrauensstellungen unter Active Directory lesen Sie die Dokumentation zum eingesetzten Windows Server. Abhängig von der Vertrauensstellung der Domänen können Benutzer auf Ressourcen anderer Domänen zugreifen.

- Die expliziten Vertrauensstellungen werden durch die Synchronisation mit der Active Directory Umgebung in den One Identity Manager eingelesen. Es werden die Domänen ermittelt, die der aktuell synchronisierten Domäne vertrauen.
- Um die impliziten Zwei-Wege-Vertrauensstellungen zwischen Domänen innerhalb einer Active Directory Gesamtstruktur im One Identity Manager bekanntzugeben, stellen Sie sicher, dass an allen untergeordneten Domänen die übergeordnete Domäne eingetragen ist.

Um die übergeordnete Domäne einzutragen

1. Wählen Sie im Manager die Kategorie **Active Directory | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Erfassen Sie die übergeordnete Domäne.
5. Speichern Sie die Änderungen.

   Die impliziten Vertrauensstellungen werden automatisch erzeugt.

Um die Vertrauensstellungen der Domänen zu prüfen

1. Wählen Sie im Manager die Kategorie **Active Directory | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.

3. Wählen Sie die Aufgabe **Vertrauensstellungen festlegen**.

   Angezeigt werden die Domänen, die der gewählten Domäne vertrauen.

Active Directory Kontenrichtlinien für Active Directory Domänen

Die globalen Kontenrichtlinien richten Sie an einer Domäne ein. Diese Informationen werden als Standardeinstellungen in der Domäne bekannt gegeben. Für Domänen ab der Funktionsebene **Windows Server 2008 R2** ist es möglich mehrere Kontenrichtlinien zu definieren. Somit können einzelne Benutzerkonten mit strengeren Kontenrichtlinien versehen werden, als es die globalen Einstellungen der Domäne vorsehen. Zum Konzept der fein abgestimmten Kennwortrichtlinien unter Active Directory lesen Sie die Dokumentation zum eingesetzten Windows Server.

Zusätzlich können Sie im One Identity Manager eigene Kennwortrichtlinien definieren, die auf die Kennwörter der Benutzerkonten angewendet werden.

HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien, die Einstellungen der globalen Kontenrichtlinien für die Active Directory Domäne sowie die Active Directory Kontenrichtlinien beachtet.

Detaillierte Informationen zum Thema

- Erfassen von Active Directory Kontenrichtlinien auf Seite 102
- Zuweisen von Active Directory Kontenrichtlinien an Active Directory Benutzerkonten und Active Directory Gruppen auf Seite 105

Verwandte Themen

- Kennwortrichtlinien für Active Directory Benutzerkonten auf Seite 65
- Globale Kontenrichtlinien für eine Active Directory Domäne auf Seite 97

Erfassen von Active Directory Kontenrichtlinien

Kontenrichtlinien werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen. Sie können bereits vorhandene Kontenrichtlinien bearbeiten und neue Kontenrichtlinien einfügen.

Um die Stammdaten einer Kontenrichtlinie zu bearbeiten

1. Wählen Sie die Kategorie **Active Directory | Kontenrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Kontenrichtlinie und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste **Neu**.
3. Bearbeiten Sie die Stammdaten für eine Kontenrichtlinie.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Active Directory Kontenrichtlinie auf Seite 103
- Richtlinien definieren auf Seite 104

Allgemeine Stammdaten einer Active Directory Kontenrichtlinie

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

Tabelle 29: Allgemeine Stammdaten einer Kontenrichtlinie

Eigenschaft	Beschreibung
Bezeichnung	Bezeichnung der Kontenrichtlinie.
Domäne	Active Directory Domäne, für welche die Kontenrichtlinie verfügbar ist.
Definierter Name	Definierter Name der Kontenrichtlinie. Der definierte Name wird per Bildungsregel aus dem Namen der Kontenrichtlinie, dem Systemcontainer für Kennwortrichtlinien **Password Settings Container** und der Domäne ermittelt.
Anzeigename	Anzeigename zur Darstellung in den One Identity Manager- Werkzeugen.
Einfache Anzeige	Anzeigename für Systeme, die nicht alle Zeichen des normalen Anzeigenamens interpretieren können.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Verwandte Themen

- Richtlinien definieren auf Seite 104

Richtlinien definieren

Auf dem Tabreiter **Richtlinie** erfassen Sie die folgenden Stammdaten.

Tabelle 30: Stammdaten einer Richtliniendefinition

Eigenschaft	Beschreibung
Dauer der Sperrung [min	Dauer der Sperrung in Minuten. Geben Sie an, für welchen Zeitraum die Benutzerkonten gesperrt werden, bevor sie automatisch zurückgesetzt werden.
Konto zurücksetzen [min]	Dauer bis zum Zurücksetzen des Benutzerkontos in Minuten. Geben Sie an, für welchen Zeitraum zwischen zwei ungültigen Kennworteingaben ein Benutzerkonto gesperrt werden soll.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Hat ein Benutzer diese Anzahl erreicht, wird das Benutzerkonto gesperrt.
Max. Kennwortalter	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird.
Min. Kennwortalter	Minimales Alter des Kennwortes. Tragen Sie die Zeitspanne ein, in der ein Kennwort benutzt werden muss, bevor der Benutzer das Kennwort ändern darf.
Min. Kennwortlänge	Minimale Länge des Kennwortes. Geben Sie die minimale Anzahl von Zeichen an, die ein Kennwort haben muss.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten 5 Kennwörter des Benutzers gespeichert.
Rangfolge	Rangfolge für Kennworteinstellungen. Falls mehrere Kontenrichtlinien einem Benutzerkonto oder einer Gruppe zugewiesen sind, wird die Kontenrichtlinie mit dem niedrigsten Wert angewendet.
Komplexe Kennwörter	Angabe, ob das Kennwort komplex sein muss. Komplexe Kennwörter müssen bestimmte Mindestanforderungen erfüllen. Für weitere Informationen lesen Sie die Dokumentation zum eingesetzten Windows Server.
Kennwort mit reversibler Verschlüsselung speichern	Angabe zur Verschlüsselung von Kennwörtern. Standardmäßig werden Kennwörter im Active Directory verschlüsselt gespeichert. Bei Verwendung dieser Option werden Kennwörter in Klartext gespeichert und können so wieder hergestellt werden.

Verwandte Themen

- Allgemeine Stammdaten einer Active Directory Kontenrichtlinie auf Seite 103

Zuweisen von Active Directory Kontenrichtlinien an Active Directory Benutzerkonten und Active Directory Gruppen

Falls mehrere Kontenrichtlinien an ein Benutzerkonto zugewiesen sind, wird nach bestimmten Regeln die wirksame Kontenrichtlinie ermittelt. Gibt es keine spezielle Kontenrichtlinie wirken die Einstellungen der Domäne. Die Berechnungsregeln entnehmen Sie dem Konzept der fein abgestimmten Kennwortrichtlinien unter Active Directory in der Dokumentation zum eingesetzten Windows Server.

Um Kontenrichtlinien für ein Benutzerkonto festzulegen

1. Wählen Sie die Kategorie **Active Directory | Kontenrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Kontenrichtlinie.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

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

   Um eine Zuweisung zu entfernen

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

Um Kontenrichtlinien für ein Gruppen festzulegen

1. Wählen Sie die Kategorie **Active Directory | Kontenrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Kontenrichtlinie.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

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

Synchronisationsprojekt bearbeiten

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

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

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

1. Wählen Sie die Kategorie **Active Directory | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten**.

Verwandte Themen

- Anpassen einer Synchronisationskonfiguration auf Seite 30

Überwachen der Anzahl von Mitgliedschaften in Active Directory Gruppen und Active Directory Containern

Tabelle 31: Wirksame Konfigurationsparameter

Konfigurationsparameter	Bedeutung
TargetSystem | ADS | MemberShipRestriction | Container	Der Konfigurationsparameter enthält die Anzahl von Active Directory Objekten pro Container, bei deren Überschreitung eine Warnmail gesendet werden soll.
TargetSystem | ADS | MemberShipRestriction | Group	Der Konfigurationsparameter enthält die Anzahl von Active Directory Objekten pro Gruppe, bei deren Überschreitung eine Warnmail gesendet werden soll.
TargetSystem | ADS | MemberShipRestriction | MailNotification	Der Konfigurationsparameter enthält die Standard-Mailadresse zum Versenden von Warnmails.

Um die Anzahl von Mitgliedern in Gruppen und Containern zu limitieren, wurde ein Mechanismus zur Überwachung der Mitgliedschaften implementiert.

- Die Tabellen `ADSAccountInADSGroup` und `ADSAccount` werden hinsichtlich der Anzahl der Mitgliedschaften von Benutzerkonten in einer Gruppe und der Anzahl von Benutzerkonten in einem Container überwacht.
- Die Tabellen `ADSContactInADSGroup` und `ADSContact` werden hinsichtlich der Anzahl der Mitgliedschaften von Kontakten in einer Gruppe und der Anzahl von Kontakten in einem Container überwacht.
- Die Tabellen `ADSGroupInADSGroup` und `ADSGroup` werden hinsichtlich der Anzahl der Mitgliedschaften von Gruppen in einer Gruppe und der Anzahl von Gruppen in einem Container überwacht.
- Die Tabellen `ADSMachineInADSGroup` und `ADSMachine` werden hinsichtlich der Anzahl der Mitgliedschaften von Computern in einer Gruppe und der Anzahl von Computern in einem Container überwacht.

HINWEIS: Die primären Gruppen von Active Directory Objekten werden bei der Berechnung der Mitglieder pro Gruppe nicht berücksichtigt.

Über Konfigurationsparameter werden Schwellwerte festgelegt, bei deren Überschreitung eine Warnmail an eine definierte Mailadresse gesendet wird. Die Warnmail wird nur bei erstmaligem Überschreiten des festgelegten Schwellwertes generiert. Somit wird verhindert, dass bei mehrmaligem Überschreiten eines Schwellwertes beispielsweise innerhalb einer Synchronisation eine große Anzahl von Warnmails an die angegebene Adresse geschickt wird.

Beispiel für die Überwachung

Der Schwellwert für die Anzahl der Objekte in einer Gruppe **Members** wurde auf zehn Mitglieder begrenzt (**TargetSystem | ADS | MemberShipRestriction | Group=10**). In der Gruppe **Member** befinden sich derzeit zehn Benutzerkonten. Beim Hinzufügen des elften Benutzerkontos wird die Warnmail an die angegebene Mailadresse versendet. Beim Hinzufügen weiterer Benutzerkonten wird jedoch keine weitere Warnmail generiert und versendet.

Active Directory Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Benutzerkonten einer Active Directory-Umgebung. Im Active Directory ist ein Benutzerkonto ein Sicherheitsprinzipal. Das bedeutet ein Benutzerkonto kann sich an der Domäne anmelden. Ein Benutzerkonto erhält über seine Gruppenmitgliedschaften und Rechte Zugriff auf die Netzwerkressourcen.

Die in Windows Server 2008 R2 eingeführten verwalteten Dienstkonten und die mit Windows Server 2012 eingeführten gruppenverwalteten Dienstkonten werden im One Identity Manager nicht unterstützt.

Verwandte Themen

- Benutzerkonten mit Personen verbinden auf Seite 108
- Unterstützte Typen von Benutzerkonten auf Seite 109
- Erfassen der Stammdaten für Active Directory Benutzerkonten auf Seite 116

Benutzerkonten mit Personen verbinden

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

Da die Anforderungen von Unternehmen zu Unternehmen unterschiedlich sind, bietet der One Identity Manager verschiedene Verfahren zur Versorgung einer Person mit den

benötigten Benutzerkonten an. Der One Identity Manager unterstützt die folgenden Vorgehensweisen, um Personen und ihre Benutzerkonten zu verknüpfen:

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

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

Verwandte Themen

- Erfassen der Stammdaten für Active Directory Benutzerkonten auf Seite 116
- Kontendefinitionen für Active Directory Benutzerkonten auf Seite 45
- Automatische Zuordnung von Personen zu Active Directory Benutzerkonten auf Seite 137
- Ausführliche Informationen zu den Grundlagen zur Behandlung und Administration von Personen und Benutzerkonten finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Unterstützte Typen von Benutzerkonten

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

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität

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

Tabelle 32: Identitäten von Benutzerkonten

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

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

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

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

Benutzerkonten mit einer Zusatzidentität, einer Gruppenidentität oder einer Dienstidentität verbinden Sie mit Dummy-Personen, die keinen Bezug zu einer realen Person haben. Diese Dummy-Personen werden benötigt, um Berechtigungen an die Benutzerkonten vererben zu können. Bei der Auswertung von Berichten, Attestierungen oder Complianceprüfungen prüfen Sie, ob die Dummy-Personen gesondert betrachtet werden müssen.

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

- Privilegiertes Benutzerkonto

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

Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 111
- Administrative Benutzerkonten auf Seite 112
- Administratives Benutzerkonto für eine Person bereitstellen auf Seite 112
- Administratives Benutzerkonto für mehrere Personen bereitstellen auf Seite 113
- Privilegierte Benutzerkonten auf Seite 114

Standardbenutzerkonten

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

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

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

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

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

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

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

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

5. Weisen Sie die Kontendefinition an die Personen zu.

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

Verwandte Themen

- Kontendefinitionen für Active Directory Benutzerkonten auf Seite 45

Administrative Benutzerkonten

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

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

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

Verwandte Themen

- Administratives Benutzerkonto für eine Person bereitstellen auf Seite 112
- Administratives Benutzerkonto für mehrere Personen bereitstellen auf Seite 113

Administratives Benutzerkonto für eine Person bereitstellen

Voraussetzungen

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

Um ein administratives Benutzerkonto für eine Person bereitzustellen

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

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

Verwandte Themen

- Administratives Benutzerkonto für mehrere Personen bereitstellen auf Seite 113
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administratives Benutzerkonto für mehrere Personen bereitstellen

Voraussetzung

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

Um ein administratives Benutzerkonto für mehrere Personen bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als Gruppenidentität.
    a. Wählen Sie im Manager die Kategorie **Active Directory | Benutzerkonten**.
    b. Wählen Sie in der Ergebnisliste das Benutzerkonto.

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

d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Gruppenidentität**.

2. Verbinden Sie das Benutzerkonto mit einer Dummy-Person.

   a. Wählen Sie im Manager die Kategorie **Active Directory | Benutzerkonten**.

   b. Wählen Sie in der Ergebnisliste das Benutzerkonto.

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

   d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Dummy-Person.

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

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

   a. Wählen Sie im Manager die Kategorie **Active Directory | Benutzerkonten**.

   b. Wählen Sie in der Ergebnisliste das Benutzerkonto.

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

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

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

      Um eine Zuweisung zu entfernen

      - Wählen Sie die Person und doppelklicken Sie .

Verwandte Themen

- Administratives Benutzerkonto für eine Person bereitstellen auf Seite 112
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Privilegierte Benutzerkonten

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

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

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

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

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

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

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

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

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

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

- Um ein Präfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_Prefix**.
- Um ein Postfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_Postfix**.

Diese Konfigurationsparameter werden in der Standardinstallation ausgewertet, wenn Sie ein Benutzerkonto, mit der Eigenschaft **Privilegiertes Benutzerkonto** (Spalte `IsPrivilegedAccount`) kennzeichnen. Die Anmeldenamen der Benutzerkonten werden entsprechend der Bildungsregeln umbenannt. Dies erfolgt auch, wenn die Benutzerkonten über den Zeitplan **Ausgewählte Benutzerkonten als privilegiert kennzeichnen** als privilegiert gekennzeichnet werden.

Verwandte Themen

- Kontendefinitionen für Active Directory Benutzerkonten auf Seite 45

Erfassen der Stammdaten für Active Directory Benutzerkonten

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

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

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

Um ein Benutzerkonto zu erstellen

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

Um die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

3. Bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

Um ein Benutzerkonto für eine Person manuell zuzuweisen oder zu erstellen

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Active Directory Benutzerkontos auf Seite 117
- Kennwortdaten eines Active Directory Benutzerkontos auf Seite 122
- Homeverzeichnis und Profilverzeichnis auf Seite 124
- Anmeldeinformationen eines Active Directory Benutzerkontos
- Einwahlrechte über Remote Access Service auf Seite 126
- Verbindungsdaten für Terminalserver auf Seite 128
- Erweiterungsdaten eines Active Directory Benutzerkontos auf Seite 130
- Erweiterte Angaben zur Identifikation auf Seite 130
- Kontaktinformationen eines Active Directory Benutzerkontos auf Seite 132

Verwandte Themen

- Kontendefinitionen für Active Directory Benutzerkonten auf Seite 45
- Benutzerkonten mit Personen verbinden auf Seite 108
- Unterstützte Typen von Benutzerkonten auf Seite 109

Allgemeine Stammdaten eines Active Directory Benutzerkontos

Tabelle 33: Konfigurationsparameter für die Einrichtung von Benutzerkonten

Konfigurationsparameter	Bedeutung
TargetSystem | ADS | Accounts | TransferJPegPhoto	Der Konfigurationsparameter legt fest, 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.

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

Tabelle 34: Allgemeine Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Person	Person, die das Benutzerkonto verwendet. Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Person bereits eingetragen. Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Person aus der Auswahlliste wählen. Wenn Sie die automatische Personenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Person gesucht und in das Benutzerkonto übernommen. Für ein Benutzerkonto mit einer Identität vom Typ **Organisatorische Identität**, **Persönliche Administratoridentität**, **Zusatzidentität**, **Gruppenidentität** oder **Dienstidentität** können Sie eine neue Person erstellen. Klicken Sie dafür neben dem Eingabefeld und erfassen Sie die erforderlichen Personenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp.
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden.
Automatisierungsgrad	Automatisierungsgrad des Benutzerkontos. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
Vorname	Vorname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Nachname	Nachname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Initialen	Initialen des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Titel	Akademischer Titel des Benutzers. Haben Sie eine Konten-

Eigenschaft	Beschreibung
	definition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Bezeichnung	Bezeichnung des Benutzerkontos. Die Bezeichnung wird aus dem Vornamen und dem Nachnamen des Benutzers gebildet.
Definierter Name	Definierter Name des Benutzerkontos. Der definierte Name wird aus der Bezeichnung des Benutzerkontos und dem Container gebildet und kann nicht bearbeitet werden.
Domäne	Domäne, in der das Benutzerkonto erzeugt werden soll.
Container	Container in dem das Benutzerkonto erzeugt werden soll. Haben Sie eine Kontendefinition zugeordnet, wird der Container, abhängig vom Automatisierungsgrad, aus den gültigen IT Betriebsdaten der zugeordneten Person ermittelt. Bei der Auswahl des Containers wird per Bildungsregel der definierte Name für das Benutzerkonto ermittelt.
Primäre Gruppe	Primäre Gruppe des Benutzerkontos. Die Synchronisation mit der Active Directory-Umgebung weist das Benutzerkonto standardmäßig der Gruppe **Domain Users** zu. Als primäre Gruppen stehen dabei nur die Gruppen zur Auswahl, die dem Benutzerkonto bereits zugewiesen wurden.
Anmeldename (pre Win2000)	Anmeldename für die Vorgängerversion von Active Directory. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, der Anmeldename (pre Win2000) aus dem zentralen Benutzerkonto der Person gebildet.
Benutzeranmeldename	Anmeldename des Benutzerkontos. Der Benutzeranmeldename entspricht dem Benutzerprinzipalnamen (User Principal Name) des Benutzers im Active Directory. Haben Sie bereits den Container festgelegt und den Anmeldenamen (pre Win2000) eingegeben, wird der Benutzeranmeldename durch eine Bildungsregel nach folgendem Schema gebildet: `Anmeldename (pre Win2000)@AD Domänenname`
E-Mail-Adresse	E-Mail-Adresse des Benutzerkontos. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, die E-Mail-Adresse aus der Standard-E-Mail-Adresse der Person gebildet.
Weitere E-Mail-Adressen	Weitere E-Mail-Adressen des Benutzerkontos.
Kontoverfallsdatum	Kontoverfallsdatum. Die Festlegung eines Kontoverfallsdatums bewirkt, dass die Anmeldung für dieses Benutzerkonto

Eigenschaft	Beschreibung
	verweigert wird, sobald das eingegebene Datum überschritten ist. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, das Austrittsdatum der Person als Kontoverfallsdatum übernommen. Ein bereits eingetragenes Kontoverfallsdatum des Benutzerkontos wird dabei überschrieben.
Strukturelle Objektklasse	Strukturelle Objektklasse, die den Typ des Objektes repräsentiert. Standardmäßig richten Sie Benutzerkonten im One Identity Manager mit der Objektklasse `USER` ein. Es wird jedoch auch die Objektklasse `INETORGPERSON` unterstützt, welche von anderen LDAP- und X.500-Verzeichnisdiensten zur Abbildung von Benutzerkonten genutzt wird.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Identität	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Person. • **Organisatorische Identität**: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. • **Zusatzidentität**: Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.

Eigenschaft	Beschreibung
Privilegiertes Benutzerkonto	Angabe, ob es sich um ein privilegiertes Benutzerkonto handelt.
Gruppen erbbar	Angabe, ob das Benutzerkonto Gruppen über die Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.
Bevorzugtes Benutzerkonto	Bevorzugtes Benutzerkonto, wenn eine Person mehrere Benutzerkonten im Active Directory besitzt.
Benutzerkonto ist deaktiviert	Angabe, ob das Benutzerkonto deaktiviert ist. Wird ein Benutzerkonto vorübergehend nicht benötigt, können Sie das Benutzerkonto über die Option zeitweilig deaktivieren.
Konto gesperrt	Angabe, ob das Benutzerkonto gesperrt ist. Abhängig von der Konfiguration wird nach mehrmaliger falscher Kennworteingabe das Benutzerkonto in der Active Directory-Umgebung gesperrt. Im Manager können Sie das Benutzerkonto über die Aufgabe **Benutzerkonto entsperren** wieder entsperren. Ist das Benutzerkonto mit einer Person verbunden, wird das Benutzerkonto entsperrt, wenn ein neues zentrales Kennwort für die Person gesetzt wird. Das Verhalten wird über den Konfigurationsparameter **TargetSystem | ADS | Accounts | UnlockByCentralPassword** gesteuert. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- Kontendefinitionen für Active Directory Benutzerkonten auf Seite 45
- Vererbung von Active Directory Gruppen anhand von Kategorien auf Seite 181
- Benutzerkonten mit Personen verbinden auf Seite 108
- Unterstützte Typen von Benutzerkonten auf Seite 109
- Deaktivieren von Active Directory Benutzerkonten auf Seite 144
- Active Directory Benutzerkonto entsperren auf Seite 134

- Automatische Zuordnung von Personen zu Active Directory Benutzerkonten auf Seite 137

Kennwortdaten eines Active Directory Benutzerkontos

Tabelle 35: Konfigurationsparameter für die Einrichtung der Kennwortdaten

Konfigurationsparameter	Bedeutung
TargetSystem | ADS | Accounts | NotRequirePassword	Der Konfigurationsparameter legt fest, ob beim Anlegen eines neuen Benutzerkontos die Option **Kein Kennwort erforderlich** in der Active Directory-Umgebung aktiviert wird.
TargetSystem | ADS | Accounts | UserMustChangePassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten die Option **Kennwort bei der nächsten Anmeldung ändern** gesetzt wird.

HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien, die Einstellungen der globalen Kontenrichtlinien für die Active Directory Domäne sowie die Active Directory Kontenrichtlinien beachtet.

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

Tabelle 36: Kennwortdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Kennwort	Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Person kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*. Wenn Sie ein initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen.
Kennwortbestätigung	Kennwortwiederholung.
Letzte Kennwortänderung	Datum der letzten Kennwortänderung. Das Datum wird aus der Active Directory-Umgebung ausgelesen und kann nicht bearbeitet werden.
Kennwort läuft nie ab	Angabe, ob ein Kennwort abläuft. Diese Option wird in der Regel für Dienstkonten verwendet. Die Option überschreibt das maximale Kennwortalter und die Option **Kennwort bei der**

Eigenschaft	Beschreibung
	nächsten Anmeldung ändern.
Kennwort nicht änderbar	Angabe, ob das Kennwort änderbar ist. Diese Option wird in der Regel für Benutzerkonten gesetzt, die von mehreren Benutzern verwendet werden.
Kennwort bei der nächsten Anmeldung ändern	Angabe, ob der Benutzer bei der nächsten Anmeldung das Kennwort anpassen muss. TIPP: Um die Option bei Neuanlage von Benutzerkonten immer zu setzen, können Sie den Konfigurationsparameter **TargetSystem | ADS | Accounts | UserMustChangePassword** aktivieren.
Kennwort mit reversibler Verschlüsselung speichern	Angabe zur Verschlüsselung des Kennwortes. Standardmäßig werden Kennwörter im Active Directory verschlüsselt gespeichert. Bei Verwendung dieser Option werden Kennwörter in Klartext gespeichert und können so wieder hergestellt werden.
SmartCard zur Anmeldung erforderlich	Angabe zur Anmeldung mittels SmartCard. Aktivieren Sie die Option, um öffentliche und private Schlüssel, Kennwörter und andere persönliche Informationen für dieses Active Directory Benutzerkonto sicher zu speichern. Um sich am Netzwerk anmelden zu können, muss der Computer des Benutzers mit einem Smartcard-Leser ausgestattet sein und der Benutzer muss über eine persönliche Identifikationsnummer (PIN) verfügen.
Konto wird für Delegierungszwecke vertraut	Angabe zur Delegierung. Aktivieren Sie die Option, damit ein Benutzer die Verantwortung für die Verwaltung und Administration eines Teilbereichs der Domäne an ein anderes Active Directory Benutzerkonto oder eine andere Gruppe delegieren kann.
Konto kann nicht delegiert werden	Angabe zur Delegierung. Aktivieren Sie die Option, falls dieses Benutzerkonto nicht zu Delegierungszwecken von einem anderen Benutzerkonto zugewiesen werden kann.
Konto verwendet DES Verschlüsselung	Angabe zur Verschlüsselung. Aktivieren Sie die Option, falls Sie die Data Encryption Standard (DES)-Unterstützung aktivieren möchten.
Keine Kerberos-Präauthentifizierung nötig	Angabe, ob eine Kerberos-Präauthentifizierung notwendig ist. Aktivieren Sie die Option, wenn das Benutzerkonto eine andere Implementierung des Kerberos-Protokolls verwendet.

Verwandte Themen

- Kennwortrichtlinien für Active Directory Benutzerkonten auf Seite 65
- Initiales Kennwort für neue Active Directory Benutzerkonten auf Seite 76
- Globale Kontenrichtlinien für eine Active Directory Domäne auf Seite 97
- Active Directory Kontenrichtlinien für Active Directory Domänen auf Seite 102

- Active Directory Kontenrichtlinien an ein Active Directory Benutzerkonto zuweisen auf Seite 134

Homeverzeichnis und Profilverzeichnis

Tabelle 37: Konfigurationsparameter für die Einrichtung von Benutzerverzeichnissen

Konfigurationsparameter	Bedeutung
QER | Person | User | ConnectHomeDir	Der Konfigurationsparameter legt fest, ob das Homeverzeichnis beim Anmelden des Benutzers verbunden werden soll.

Erfassen Sie die Daten für das Homeverzeichnis und das Profilverzeichnis des Benutzers.

HINWEIS: Ist der Konfigurationsparameter **QER | Person | User | ConnectHomeDir** aktiviert, werden einige der nachfolgenden Daten für das Homeverzeichnis automatisch gebildet. Aktivieren Sie den Konfigurationsparameter bei Bedarf im Designer.

Wenn Sie ein Profilverzeichnis angeben, so wird durch den One Identity Manager Service ein neues Benutzerprofil erzeugt, das bei einer Anmeldung des Benutzers vom Netzwerk geladen wird.

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

Tabelle 38: Stammdaten für Benutzerverzeichnisse

Eigenschaft	Beschreibung
Homeserver	Homeserver. Den Homeserver können Sie, in Abhängigkeit von der Anzahl der bereits (laut Datenbank) vorhandenen Homeverzeichnisse pro Homeserver, auswählen. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, der Homeserver aus den gültigen IT Betriebsdaten der zugeordneten Person ermittelt.
Homefreigabe	Freigabe, unter der das Homeverzeichnis des Benutzers auf dem Homeserver angelegt wird. Standard ist HOMES.
Homeverzeichnispfad	Name des Homeverzeichnisses für den Benutzer, unterhalb der Homefreigabe. Im Standard wird der Anmeldename (pre Windows 2000) zur Bildung des Homeverzeichnispfades verwendet.
Home freigegeben als	Freigabe des Homeverzeichnisses. Die Freigabe wird im Standard aus dem Homeverzeichnispfad gebildet.
Homelaufwerk	Laufwerk, welches bei der Anmeldung eines Benutzers verbunden werden soll. Es wird das Standard-Homelaufwerk der Domäne übernommen.

Eigenschaft	Beschreibung
Homeverzeichnis	Homeverzeichnis des Benutzers. Das angegebene Homeverzeichnis wird vom One Identity Manager Service automatisch angelegt und freigegeben.
Größe Homeverzeichnis [MB]	Größe des Homeverzeichnisses in MB. Die Größe des Homeverzeichnisses ermitteln Sie über einen standardmäßig mitgelieferten Zeitplan. Konfigurieren und aktivieren Sie im Designer den Zeitplan **Homegrößen für Benutzerkonten auslesen**.
Maximaler Homespeicherplatz [MB]	Maximal zulässige Größe des Homeverzeichnisses in MB auf dem Homeserver.
Profilserver	Profilserver. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, der Profilserver aus den gültigen IT Betriebsdaten der zugeordneten Person ermittelt.
Profilfreigabe	Freigabe, unter der das Profilverzeichnis des Benutzers auf dem Profilserver angelegt wird. Standard ist `PROFILES`.
Profil freigegeben als	Freigabe des Profilverzeichnisses.
Profilverzeichnispfad	Name des Profilverzeichnisses für den Benutzer, unterhalb der Profilfreigabe. Im Standard wird der Anmeldename (pre Windows 2000) zur Bildung des Profilverzeichnispfades verwendet.
Anmeldeskript	Name des Anmeldeskriptes. Befindet sich das Anmeldeskript in einem Unterverzeichnis des Anmeldeskriptpfades (in der Regel `Winnt\Sysvol\domain\scripts`), dann müssen Sie dieses Unterverzeichnis mit angeben. Das angegebene Anmeldeskript wird bei Anmeldung des Benutzers ausgeführt.

Verwandte Themen

- Vorbereiten eines Home- und Profilservers für die Anlage von Benutzerverzeichnissen auf Seite 87

Anmeldeinformationen eines Active Directory Benutzerkontos

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

Tabelle 39: Anmeldeinformationen

Eigenschaft	Beschreibung
Letzte Anmeldung	Datum der letzten Anmeldung. Das Datum wird aus der Active Directory-Umgebung ausgelesen und kann manuell nicht geändert werden.
Anmeldestationen	Arbeitsstationen, an welchen sich der Benutzer anmelden kann. Standardmäßig kann sich ein Benutzer an allen Arbeitsstationen anmelden. Über die Schaltfläche neben dem Eingabefeld schalten Sie die Eingabe frei und können Arbeitsstationen hinzufügen. Über die Schaltfläche können Sie Arbeitsstationen aus der Liste entfernen.
Anmeldezeiten	Tage und Stunden, an denen ein Benutzer angemeldet sein kann. Standardmäßig ist die Anmeldung während aller Stunden an jedem Tag der Woche erlaubt. Ist ein Benutzer angemeldet, wird die Anmeldung nach Ablauf der erlaubten Anmeldezeit getrennt. Der Kalender zeigt eine 7-Tage Woche, jede Box stellt eine Stunde dar. Die konfigurierten Anmeldezeiten werden entsprechend farbig dargestellt. Ist eine Box gefüllt, ist die Anmeldung erlaubt. Ist die Box leer, wird die Anmeldung verweigert. ***Um Anmeldezeiten festzulegen*** • Wählen Sie einen Zeitraum per Maus oder Tastatur aus. • Über **Zuweisen** erlauben Sie die Anmeldung im ausgewählten Zeitraum. • Über **Entfernen** verbieten Sie die Anmeldung im ausgewählten Zeitraum. • Über **Umkehren** markieren Sie die gewählten Zeiträume entgegengesetzt. • Über die Pfeiltasten können Sie eine Auswahl zurücksetzen oder wiederholen.

Einwahlrechte über Remote Access Service

HINWEIS: Remote Access Service (RAS) Eigenschaften werden nur synchronisiert und provisioniert, wenn im Synchronisationsprojekt die Option **RAS Eigenschaften aktivieren** aktiviert ist.

Erteilen Sie dem Benutzerkonto Remote-Einwahlrechte in das Netz und legen die Rückrufoptionen fest. Einige der Angaben sind abhängig vom gewählten Domänenmodus (einheitlich oder gemischt) bearbeitbar.

Auf dem Tabreiter **RAS** erfassen Sie die folgenden Stammdaten.

Tabelle 40: Remote Access Service

Eigenschaft	Beschreibung	
Einwahl erlaubt	Angabe, ob sich der Benutzer in das Netzwerk einwählen darf. Zulässige Werte sind:	
	Zugriff erlaubt	Mit dieser Angabe gestatten Sie dem Benutzer sich in das Netzwerk einzuwählen.
	Zugriff nicht erlaubt	Mit dieser Angabe verweigern Sie dem Benutzer die Einwahl in das Netzwerk.
	Zugriffssteuerung über Remote Access Policy	Mit dieser Angabe legen Sie fest, dass der Zugriff auf das Netzwerk per RAS-Richtlinien gesteuert wird. RAS-Richtlinien werden in der Regel genutzt, um die gleichen Zugriffsberechtigungen auf mehrere Active Directory Benutzerkonten anzuwenden.
Kein Rückruf	Die Rückruffunktion wird durch diese Option ausgeschaltet.	
Vom Anrufer festgelegt	Der Server erwartet vom Benutzer die Angabe einer Telefonnummer unter der er den Anrufer zurückruft.	
Immer Rückruf	Der Server versucht unter der angegebenen Rückrufnummer den Benutzer zurückzurufen.	
Verifizierende Anruferkennung	Definierte Nummer von der sich ein Benutzer in das Netzwerk einwählen soll.	
Statische IP Adresse	Feste IP-Adresse im Netzwerk, die dem Benutzer zugewiesen wird.	
Statische Routen mit IP Adresse, Netzwerkadresse und Metrik	IP-Adressen, Netzwerkadressen und Metriken zum Zielnetzwerk für die Einwahlverbindung über statische Routen.	

Verwandte Themen

- Einrichten der Synchronisation mit einer Active Directory-Umgebung auf Seite 13

Verbindungsdaten für Terminalserver

Tabelle 41: Konfigurationsparameter für Terminalserver-Eigenschaften

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Person | User | ConnectHomeDir	Der Konfigurationsparameter legt fest, ob das Homeverzeichnis beim Anmelden des Benutzers verbunden werden soll.

HINWEIS: Terminalserver Eigenschaften werden nur synchronisiert und provisioniert, wenn im Synchronisationsprojekt die Option **Terminalserver Eigenschaften aktivieren** aktiviert ist.

Erfassen Sie folgende Daten für die Anlage eines Benutzerprofils, welches für die Anmeldung des Active Directory Benutzerkontos an einem Terminalserver zur Verfügung stehen soll. Für die Terminalserver Sitzungen kann für den Benutzer ein Profilverzeichnis, welches für die Anmeldung des Benutzers an einem Terminalserver zur Verfügung stehen soll, angegeben werden. Ebenso ist die Anlage eines Homeverzeichnisses auf dem Terminalserver möglich.

HINWEIS: Ist der Konfigurationsparameter **QER | Person | User | ConnectHomeDir** aktiviert, werden einige der nachfolgenden Daten für das Homeverzeichnis automatisch gebildet. Aktivieren Sie den Konfigurationsparameter bei Bedarf im Designer.

Auf dem Tabreiter **Terminal Service** erfassen Sie die folgenden Stammdaten.

Tabelle 42: Stammdaten für Terminalserver

Eigenschaft	Beschreibung
Anmeldung am Terminalserver erlaubt	Angabe, ob die Anmeldung am Terminalserver erlaubt ist. Aktivieren Sie die Option, um einem Benutzer die Anmeldung am Terminalserver zu gestatten.
Eigene Konfiguration verwenden	Angabe, ob eine Startanwendung festgelegt werden kann. Aktivieren Sie die Option, um eine Anwendung festzulegen, welche bei Anmeldung am Terminalserver gestartet werden soll und geben Sie die Befehlszeile zum Start und das Arbeitsverzeichnis der Anwendung an. HINWEIS: Sollen diese Angaben vom Client geerbt werden, deaktivieren Sie die Option.
Befehlszeile	Befehlszeile zum Starten der Anwendung.
Arbeitsverzeichnis	Arbeitsverzeichnis der zu startenden Anwendung.
Client-Laufwerke beim Anmelden verbinden	Angabe, ob bei der Anmeldung an einen Terminalserver die Client-Laufwerke automatisch wiederhergestellt werden sollen.
Client-Drucker beim	Angabe, ob bei der Anmeldung an einen Terminalserver Client-

Eigenschaft	Beschreibung
Anmelden verbinden	Drucker automatisch wiederhergestellt werden sollen.
Standarddrucker des Clients	Angabe, ob bei der Anmeldung an einen Terminalserver der Standarddrucker automatisch wiederhergestellt werden sollen.
Aktives Sitzungslimit [min]	Maximale Verbindungszeit in Minuten. Nach Ablauf dieses Intervalls werden die Terminalserver-Verbindungen getrennt oder beendet.
Getrennte Sitzung beenden [min]	Zeitintervall in Minuten, über das eine getrennte Verbindung noch aufrecht erhalten wird.
Leerlaufsitzungslimit [min]	Maximale Zeit in Minuten ohne Clientaktivitäten vor dem Trennen und Beenden einer Verbindung.
Getrennte Sitzungen von vorherigem Client verbinden	Angabe, ob eine getrennte Sitzung von jedem beliebigen Clientcomputer wieder aufgenommen werden kann.
Bei abgebrochener Verbindung Sitzung beenden	Angabe, ob bei Abbruch einer Verbindung die Sitzung wieder in den getrennten Zustand zurückgesetzt werden soll.
Remoteüberwachung aktivieren	Angabe, ob für die Benutzersitzung eine Remoteüberwachung oder -steuerung aktiviert werden soll.
Erlaubnis des Benutzers einholen	Angabe, ob die Erlaubnis des Benutzers zur Überwachung der Sitzung einzuholen ist.
Benutzersitzung anzeigen	Angabe, ob die Benutzersitzung überwacht werden soll.
In Sitzung eingreifen	Angabe, ob dem überwachenden Benutzer Eingaben per Tastatur oder Maus in der überwachten Sitzung ermöglicht werden.
Profilserver	Profilserver. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, der Profilserver aus den gültigen IT Betriebsdaten der zugeordneten Person ermittelt.
Profilfreigabe	Freigabe, unter der das Profilverzeichnis des Benutzers auf dem Profilserver angelegt wird. Standard ist `TPROFILES`.
Profilverzeichnispfad	Name des Profilverzeichnisses für den Benutzer, unterhalb der Profilfreigabe. Im Standard wird der Anmeldename (pre Windows 2000) zur Bildung des Profilverzeichnispfades verwendet.
Profilpfad	Kompletter Pfad zum Profilverzeichnis des Benutzers.
Homeserver	Homeserver. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, der Profilserver aus den gültigen IT Betriebsdaten der zugeordneten Person ermittelt.

Eigenschaft	Beschreibung
Homefreigabe	Freigabe, unter der das Homeverzeichnis des Benutzers auf dem Homeserver angelegt wird. Standard ist `THOMES`.
Homeverzeichnispfad	Name des Homeverzeichnisses für den Benutzer, unterhalb der Homefreigabe. Im Standard wird der Anmeldename (pre Windows 2000) zur Bildung des Homeverzeichnispfades verwendet.
Freigegeben als	Freigabe des Homeverzeichnisses. Die Freigabe wird im Standard aus dem Homeverzeichnispfad gebildet.
Homelaufwerk	Laufwerk, welches bei der Anmeldung eines Benutzers verbunden werden soll. Es wird das Standard-Homelaufwerk der Domäne übernommen.
Homeverzeichnis	Homeverzeichnis. Das angegebene Homeverzeichnis wird vom One Identity Manager Service automatisch angelegt und freigegeben.

Verwandte Themen

- Vorbereiten eines Home- und Profilservers für die Anlage von Benutzerverzeichnissen auf Seite 87

Erweiterungsdaten eines Active Directory Benutzerkontos

Auf dem Tabreiter **Erweiterungen** erfassen Sie benutzerdefinierte Active Directory Schemaerweiterungen für das Benutzerkonto.

Tabelle 43: Erweiterungsdaten

Eigenschaft	Beschreibung
Erweiterungsdaten	Unternehmensspezifische Erweiterungsdaten im Binärformat.
Attributerweiterung 01 - Attributerweiterung 15	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Erweiterte Angaben zur Identifikation

Auf dem Tabreiter **Identifikation** erfassen Sie die folgenden Adressinformationen zur Erreichbarkeit der Person, die das Benutzerkonto verwendet.

Tabelle 44: Stammdaten zur Identifikation

Eigenschaft	Beschreibung
Büro	Büro. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Straße	Straße. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Postfach	Postfach. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Postleitzahl	Postleitzahl. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Ort	Ort. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. Anhand des Ortes können automatisch Standorte erzeugt und den Personen zugeordnet werden.
Bundesland	Bundesland. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Länderkennung	Länderkennung.
Firma	Firma der Person. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Abteilung	Abteilung der Person. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt. Anhand der Abteilungsinformation können automatisch Abteilungen erzeugt und den Personen zugeordnet werden.
Berufsbezeichnung	Berufsbezeichnung. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Personenkennung	Eindeutige Kennung der Person, zum Beispiel die ID.
Personennummer	Nummer zur Kennzeichnung der Person zusätzlich zur Personenkennung.
Kontomanager	Verantwortlicher für das Benutzerkonto. ***Um einen Kontomanager festzulegen***

Eigenschaft	Beschreibung
	1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, welche die Konto-manager abbildet. 3. Wählen Sie unter **Kontomanager** den Verantwortlichen. 4. Klicken Sie **OK**.

Verwandte Themen

- Automatisches Erzeugen von Abteilungen und Standorten anhand von Benutzerkonteninformationen auf Seite 143

Kontaktinformationen eines Active Directory Benutzerkontos

Auf dem Tabreiter **Kontakt** erfassen Sie die Daten zur telefonischen Erreichbarkeit der Person, die das Benutzerkonto verwendet.

Tabelle 45: Kontaktinformationen

Eigenschaft	Beschreibung
Telefon	Telefonnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Telefon privat	Private Telefonnummer.
Fax	Faxnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Mobiltelefon	Mobiltelefonnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Funkruf	Funkrufnummer.
Webseite	Webseite.
IP Telefonnummer	IP-Telefonnummer.
Anmerkung	Freitextfeld für zusätzliche Erläuterungen.

Zusätzliche Aufgaben für die Verwaltung von Active Directory Benutzerkonten

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Überblick über das Active Directory Benutzerkonto

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

Um einen Überblick über ein Benutzerkonto zu erhalten

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das Active Directory Benutzerkonto**.

Ändern des Automatisierungsgrades an einem Active Directory Benutzerkonto

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

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

1. Wählen Sie im Manager die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Erfassen der Stammdaten für Active Directory Benutzerkonten auf Seite 116

Active Directory Benutzerkonto entsperren

Nach mehrmaliger (abhängig von der Konfiguration) falscher Kennworteingabe wird das Benutzerkonto in der Active Directory-Umgebung gesperrt.

Ist das Benutzerkonto mit einer Person verbunden, wird das Benutzerkonto entsperrt, wenn ein neues zentrales Kennwort für die Person gesetzt wird. Das Verhalten wird über den Konfigurationsparameter **TargetSystem | ADS | Accounts | UnlockByCentralPassword** gesteuert. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Um ein Benutzerkonto manuell zu entsperren

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Benutzerkonto entsperren**.
5. Bestätigen Sie die Sicherheitsabfrage mit **OK**.

   Das Entsperren des Benutzerkontos erfolgt durch den One Identity Manager Service.

Verwandte Themen

- Erfassen der Stammdaten für Active Directory Benutzerkonten auf Seite 116

Active Directory Kontenrichtlinien an ein Active Directory Benutzerkonto zuweisen

Für Domänen ab der Funktionsebene **Windows Server 2008 R2** ist es möglich zu den Standardkennwortrichtlinien der Domäne weitere Kontenrichtlinien zu definieren. Somit können einzelne Benutzerkonten und Gruppen mit strengeren Kontenrichtlinien versehen werden, als es die globalen Einstellungen vorsehen.

Um Kontenrichtlinien für ein Benutzerkonto festzulegen

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Kontenrichtlinien zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontenrichtlinien zu.

   - ODER -

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

Verwandte Themen

- Active Directory Kontenrichtlinien für Active Directory Domänen auf Seite 102
- Globale Kontenrichtlinien für eine Active Directory Domäne auf Seite 97
- Active Directory Kontenrichtlinien an eine Active Directory Gruppe zuweisen auf Seite 184

Active Directory Gruppen direkt an ein Active Directory Benutzerkonto zuweisen

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

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Benutzerkonto die Gruppen direkt zuweisen.

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

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

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

Verwandte Themen

- Active Directory Gruppe an Active Directory Benutzerkonten, Active Directory Kontakte und Active Directory Computer zuweisen auf Seite 166
- Zulässigkeit von Gruppenmitgliedschaften auf Seite 163
- Allgemeine Stammdaten eines Active Directory Benutzerkontos auf Seite 117

Assistenten an ein Active Directory Benutzerkonto zuweisen

Weisen Sie dem Benutzerkonto einen Assistenten zu. Der Assistent wird im Microsoft Outlook in den Eigenschaften eines E-Mail-Empfängers abgebildet.

Um einen Assistenten an ein Benutzerkonto zuzuweisen

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Assistenten zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste **Tabelle** die Tabelle, welche die Assistenten enthält. Zur Auswahl stehen:
   - Active Directory Benutzerkonten
   - Active Directory Kontakte
   - Active Directory Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** den Assistenten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** den Assistenten.
6. Speichern Sie die Änderungen.

Active Directory Benutzerkonto verschieben

HINWEIS: Benutzerkonten können Sie nur innerhalb einer Domäne verschieben.

Um ein Benutzerkonto zu verschieben

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Active Directory Container ändern**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Container** den neuen Container.
7. Speichern Sie die Änderungen.

Zusatzeigenschaften an ein Active Directory Benutzerkonto zuweisen

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

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

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

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

   Um eine Zuweisung zu entfernen

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

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

Automatische Zuordnung von Personen zu Active Directory Benutzerkonten

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

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

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

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

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

  Beispiel:

  ```
  ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $
  ```
- Legen Sie über den Konfigurationsparameter **TargetSystem | ADS | PersonAutoDisabledAccounts** fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
- Weisen Sie der Domäne eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Personenzuordnung an der Domäne.

HINWEIS:

Für die Synchronisation gilt:

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

Außerhalb der Synchronisation gilt:

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

HINWEIS:

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

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

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Domäne die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **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 zur automatischen Personenzuordnung finden Sie im *One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul*.

Verwandte Themen

- Erstellen einer Kontendefinition auf Seite 45
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 62
- Bearbeiten der Suchkriterien für die automatische Personenzuordnung auf Seite 139

Bearbeiten der Suchkriterien für die automatische Personenzuordnung

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

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

HINWEIS: Bei der Zuordnung der Personen zu Benutzerkonten anhand der Suchkriterien

erhalten die Benutzerkonten den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

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

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

Um Kriterien für die Personenzuordnung festzulegen

1. Wählen Sie die Kategorie **Active Directory | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Suchkriterien für die Personenzuordnung definieren**.
4. Legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person übereinstimmen müssen, damit die Person mit dem Benutzerkonto verbunden wird.

Tabelle 46: Standardsuchkriterien für Benutzerkonten und Kontakte

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto /Kontakt
Active Directory Benutzerkonten	Zentrales Benutzerkonto (CentralAccount)	Anmeldename (pre Win2000) (SAMAccountName)
Active Directory Kontakte	Zentrales Benutzerkonto (CentralAccount)	Bezeichnung (Cn)

5. Speichern Sie die Änderungen.

Direkte Zuordnung von Personen an Benutzerkonten anhand einer Vorschlagsliste

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

Tabelle 47: Ansichten zur manuellen Zuordnung

Ansicht	Beschreibung
Vorgeschlagene Zuordnungen	Die Ansicht listet alle Benutzerkonten auf, denen der One Identity Manager eine Person zuordnen kann. Dazu werden die Personen angezeigt, die durch die Suchkriterien ermittelt und zugeordnet werden können.

Ansicht	Beschreibung
Zugeordnete Benutzerkonten	Die Ansicht listet alle Benutzerkonten auf, denen eine Person zugeordnet ist.
Ohne Personenzuordnung	Die Ansicht listet alle Benutzerkonten auf, denen keine Person zugeordnet ist und für die über die Suchkriterien keine passende Person ermittelt werden kann.

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

Um die Suchkriterien auf die Benutzerkonten anzuwenden

- Klicken Sie **Neu laden**.

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

Um Personen direkt über die Vorschlagsliste zuzuordnen

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

      Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet.

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

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

Um Zuordnungen zu entfernen

1. Klicken Sie **Zugeordnete Benutzerkonten**.
   a. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Personenzuordnung entfernt werden soll. Mehrfachauswahl ist möglich.
   b. Klicken Sie **Ausgewählte entfernen**.

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

   Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

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

Verwandte Themen

- Automatische Zuordnung von Personen zu Active Directory Benutzerkonten auf Seite 137

Aktualisieren von Personen bei Änderung von Active Directory Benutzerkonten

Im One Identity Manager werden Änderungen der Personeneigenschaften an die verbundenen Benutzerkonten weitergereicht und anschließend in das Active Directory provisioniert. Unter Umständen kann es notwendig sein, Änderungen von Benutzerkonten im Active Directory auf die Personeneigenschaften im One Identity Manager weiterzureichen.

Beispiel

Während des Testbetriebs werden die Benutzerkonten aus dem Active Directory in den One Identity Manager nur eingelesen und Personen erzeugt. Die Verwaltung der Benutzerkonten (Erstellen, Ändern und Löschen) über den One Identity Manager soll erst zu einem späteren Zeitpunkt in Betrieb genommen werden. Während des Testbetriebs werden die Benutzerkonten weiterhin im Active Directory geändert, was zu Abweichungen der Benutzerkonteneigenschaften und Personeneigenschaften führen kann. Aus diesem Grund sollen vorübergehend die durch eine erneute Synchronisation eingelesenen Änderungen von Benutzerkonten an die bereits erzeugten Personen publiziert werden. Damit führt die Inbetriebnahme der Benutzerkontenverwaltung über den One Identity Manager nicht zu Datenverlusten.

Um Personen bei Änderungen von Benutzerkonten zu aktualisieren

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | PersonUpdate**.

Während der Synchronisation werden die Änderungen der Benutzerkonten in den One Identity Manager eingelesen. Durch anschließende Skript- und Prozessverarbeitung werden diese Änderungen an die verbundenen Personen weitergereicht.

HINWEIS: Die Aktualisierung der Personen bei Änderungen von Benutzerkonten erfolgt nur für Benutzerkonten, die den Automatisierungsgrad **Unmanaged** besitzen und mit

einer Person verbunden sind.

HINWEIS: Es wird nur die Person aktualisiert, die aus dem geänderten Benutzerkonto erzeugt wurde. Die Datenquelle, aus der eine Person erzeugt wurde, wird über die Eigenschaft **Datenquelle Import** der Person angezeigt. Sind der Person weitere Benutzerkonten zugeordnet, dann führen Änderungen dieser Benutzerkonten nicht zur Aktualisierung der Person.

Das Mapping von Benutzerkontoeigenschaften auf Personeneigenschaften erfolgt über das Skript `ADS_PersonUpdate_ADSAccount`. Das Mapping von Kontakteigenschaften auf Personeneigenschaften erfolgt über das Skript `ADS_PersonUpdate_ADSContact` . Um das Mapping einfacher anzupassen, sind die Skripte als überschreibbar definiert.

Für unternehmensspezifische Anpassungen, erzeugen Sie eine Kopie des jeweiligen Skriptes und beginnen Sie den Skriptcode folgendermaßen:

```
Public Overrides Function ADS_PersonUpdate_ADSAccount(ByVal UID_Account As
String,OldAccountDN As String, ProcID As String)
```

Damit wird das Skript neu definiert und überschreibt das originale Skript. Eine Anpassung der Prozesse ist in diesem Fall nicht erforderlich.

Automatisches Erzeugen von Abteilungen und Standorten anhand von Benutzerkonteninformationen

Anhand der Abteilungsinformationen oder Ortsinformationen der Benutzerkonten können neue Abteilungen und Standorte im One Identity Manager erzeugt werden. Zusätzlich werden die Abteilungen und Standorte den Personen der Benutzerkonten als primäre Abteilung und primärer Standort zugeordnet. Bei entsprechender Konfiguration des One Identity Manager können die Personen über diese Zuordnungen ihre Unternehmensressourcen erhalten.

Voraussetzung für den Einsatz dieses Verfahrens

Personen müssen beim Anlegen und Ändern von Benutzerkonten automatisch erzeugt werden. Mindestens einer der folgenden Konfigurationsparameter muss aktiviert sein und das entsprechende Verfahren eingerichtet sein.

Tabelle 48: Konfigurationsparameter für automatische Personenzuordnung

Konfigurationsparameter	Wirkung bei Aktivierung
TargetSystem | ADS | PersonAutoDefault	Anhand des angegebenen Modus erfolgt die automatische Personenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.

Konfigurationsparameter	Wirkung bei Aktivierung
TargetSystem | ADS | PersonAutoFullsync	Anhand des angegebenen Modus erfolgt die automatische Personenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem | ADS | PersonUpdate	Es erfolgt eine fortlaufende Aktualisierung von Personenobjekten aus verbundenen Benutzerkonten.

Um dieses Verfahren zu nutzen

- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | AutoCreateDepartment**, um Abteilungen aus den Benutzerkonteninformationen zu erzeugen.
- Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | ADS | AutoCreateLocality**, um Standorte aus den Benutzerkonteninformationen zu erzeugen.

Verwandte Themen

- Erweiterte Angaben zur Identifikation auf Seite 130
- Automatische Zuordnung von Personen zu Active Directory Benutzerkonten auf Seite 137
- Aktualisieren von Personen bei Änderung von Active Directory Benutzerkonten auf Seite 142

Deaktivieren von Active Directory Benutzerkonten

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

Szenario:

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

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

Szenario:

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

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

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

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu deaktivieren

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

Szenario:

- Benutzerkonten sind nicht mit Personen verbunden.

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

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

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

Verwandte Themen

- Kontendefinitionen für Active Directory Benutzerkonten auf Seite 45
- Erstellen der Automatisierungsgrade auf Seite 48

- Löschen und Wiederherstellen von Active Directory Benutzerkonten auf Seite 146

Löschen und Wiederherstellen von Active Directory Benutzerkonten

Im Active Directory werden Objekte wie zum Beispiel Benutzerkonten mit einer eindeutigen Identifikationsnummer (ID) versehen, mit der auch die Berechtigungen verknüpft sind. Für Domänen mit den Funktionsebenen kleiner als **Windows Server 2008 R2** gehen beim Löschen der Benutzerkonten im Active Directory die ID und die damit verbundenen Berechtigungen irreversibel verloren. Somit sind Benutzerkonten nur schwer wiederherstellbar. Für Domänen ab der Funktionsebene **Windows Server 2008 R2** können Benutzerkonten über den Papierkorb gelöscht werden. Dabei werden die Benutzerkonten in den Papierkorb verschoben und können ohne Verlust der ID und der Berechtigungen innerhalb einer definierten Aufbewahrungszeit wiederhergestellt werden.

Ob beim Einfügen eines Active Directory Objektes zunächst geprüft werden soll, ob sich das Objekt im Active Directory Papierkorb befindet und von dort wiederhergestellt werden soll, legen Sie bei der Konfiguration des Synchronisationsprojektes fest.

Der One Identity Manager nutzt verschiedene Verfahren zum Löschen von Benutzerkonten.

Löschen ohne Active Directory Papierkorb

Dieses Verfahren wird für alle Domänen eingesetzt, in denen:

- aufgrund einer Funktionsebene kleiner als **Windows Server 2008 R2** kein Papierkorb vorhanden ist.

  - ODER-

- der Papierkorb ab der Funktionsebene **Windows Server 2008 R2** nicht aktiviert ist.

Nach Bestätigung der Sicherheitsabfrage wird das Benutzerkonto im One Identity Manager zunächst zum Löschen markiert. Das Benutzerkonto wird im One Identity Manager gesperrt und je nach Einstellung der Löschverzögerung endgültig aus der One Identity Manager-Datenbank und aus dem Active Directory gelöscht.

Löschen über den Active Directory Papierkorb

Dieses Verfahren wird für Domänen ab Funktionsebene **Windows Server 2008 R2** eingesetzt, bei denen der Papierkorb aktiviert ist.

Nach Bestätigung der Sicherheitsabfrage wird das Benutzerkonto im One Identity Manager zunächst zum Löschen markiert. Das Benutzerkonto wird im One Identity Manager gesperrt und nach Ablauf der Löschverzögerung endgültig aus der One Identity Manager-Datenbank gelöscht. Das Benutzerkonto wird im Active Directory in den Papierkorb verschoben und nach Ablauf der Aufbewahrungszeit endgültig aus dem Active Directory gelöscht. Die Aufbewahrungszeit für Objekte im Papierkorb ist an der Domäne in der Eigenschaft **Aufbewahrungsdauer** eingetragen.

HINWEIS: Beim Löschen eines Benutzerkontos wird im One Identity Manager ein Eintrag für die Active Directory SID erzeugt.

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

Um ein Benutzerkonto zu löschen

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Löschen Sie das Benutzerkonto.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um ein Benutzerkonto wiederherzustellen

1. Wählen Sie die Kategorie **Active Directory | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste die Schaltfläche **Löschen rückgängig machen**.

Beim Löschen eines Benutzerkontos werden die Konfigurationsparameter zur Behandlung der Benutzerverzeichnisse berücksichtigt.

- Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.

Tabelle 49: Konfigurationsparameter für das Löschen von Benutzerkonten

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Person | User | DeleteOptions	Der Konfigurationsparameter steuert das Verhaltens beim Löschen von Benutzerkonten.
QER | Person | User | DeleteOptions | FolderAnonymPre	Wenn in den Löschoptionen festgelegt ist, dass ein Verzeichnis oder eine Freigabe nicht gelöscht werden soll, so wird es umbenannt und erhält das angegebene Präfix.
QER | Person | User | DeleteOptions | HomeDir	Das Homeverzeichnis des Benutzers wird gelöscht.
QER | Person | User | DeleteOptions | HomeShare	Die Homefreigabe des Benutzers wird gelöscht.
QER | Person | User | DeleteOptions | ProfileDir	Das Profilverzeichnis des Benutzers wird gelöscht.
QER | Person | User | DeleteOptions | ProfileShare	Die Profilfreigabe des Benutzers wird gelöscht.

Konfigurationsparameter	Wirkung bei Aktivierung
QER | Person | User | DeleteOptions | TerminalHomeDir	Das Terminalhomeverzeichnis des Benutzers wird gelöscht.
QER | Person | User | DeleteOptions | TerminalHomeShare	Die Terminalhomefreigabe des Benutzers wird gelöscht.
QER | Person | User | DeleteOptions | TerminalProfileDir	Das Terminalprofilverzeichnis des Benutzers wird gelöscht.
QER | Person | User | DeleteOptions | TerminalProfileShare	Die Terminalprofilfreigabe des Benutzers wird gelöscht.

Konfigurieren der Löschverzögerung

Standardmäßig werden Benutzerkonten mit einer Löschverzögerung von 30 Tagen endgültig aus der Datenbank entfernt. Die Benutzerkonten werden zunächst deaktiviert. Bis zum Ablauf der Löschverzögerung besteht die Möglichkeit die Benutzerkonten wieder zu aktivieren. Nach Ablauf der Löschverzögerung werden die Benutzerkonten aus der Datenbank gelöscht und ein Wiederherstellen ist nicht mehr möglich. Eine abweichende Löschverzögerung konfigurieren Sie im Designer an der Tabelle ADSAccount.

Verwandte Themen

- Deaktivieren von Active Directory Benutzerkonten auf Seite 144
- Löschen und Wiederherstellen von Active Directory Kontakten auf Seite 158
- Active Directory Sicherheits-IDs auf Seite 190
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer Active Directory Domäne auf Seite 22
- Active Directory spezifische Stammdaten einer Active Directory Domäne auf Seite 98

6

Active Directory Kontakte

Ein Kontakt ist ein Nicht-Sicherheitsprinzipal, das bedeutet ein Kontakt kann sich nicht an der Domäne anmelden. Er stellt zum Beispiel einen Benutzer außerhalb der Organisation dar und wird hauptsächlich für Verteilergruppen oder zu E-Mail Zwecken benutzt.

Verwandte Themen

- Erfassen der Stammdaten für Active Directory Kontakte auf Seite 149
- Benutzerkonten mit Personen verbinden auf Seite 108
- Unterstützte Typen von Benutzerkonten auf Seite 109

Erfassen der Stammdaten für Active Directory Kontakte

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

HINWEIS:

- Um Kontakte für die Personen eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen. Wird für die Erstellung der Kontakte eine Kontendefinition eingesetzt, dann werden einige der nachfolgend beschriebenen Stammdaten über Bildungsregeln aus den Personenstammdaten gebildet. Der Umfang ist dabei abhängig vom Automatisierungsgrad der Kontendefinition. Die mitgelieferten Bildungsregeln können Sie kundenspezifisch anpassen.
- Sollen Personen ihre Kontakte über Kontendefinitionen erhalten, müssen die Personen ein zentrales Benutzerkonto besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.

Um die Stammdaten eines Kontaktes zu bearbeiten

1. Wählen Sie die Kategorie **Active Directory | Kontakte**.
2. Wählen Sie in der Ergebnisliste den Kontakt und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten für einen Kontakt.
4. Speichern Sie die Änderungen.

Um einen Kontakt für eine Person manuell zuzuweisen oder zu erstellen

1. Wählen Sie die Kategorie **Personen | Personen**.
2. Wählen Sie in der Ergebnisliste die Person aus und führen Sie die Aufgabe **Active Directory Kontakte zuweisen** aus.
3. Weisen Sie einen Kontakt zu.

   - ODER -

   Wählen Sie die Aufgabe **Neuer Kontakt** und bearbeiten Sie die Stammdaten.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines Active Directory Kontaktes auf Seite 150
- Kontaktinformationen eines Active Directory Kontaktes auf Seite 153
- Erweiterte Angaben zur Identifikation auf Seite 153
- Erweiterungsdaten eines Active Directory Kontaktes auf Seite 154

Allgemeine Stammdaten eines Active Directory Kontaktes

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

Tabelle 50: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Person	Person, die den Kontakt verwendet. Wurde der Kontakt über eine Kontendefinition erzeugt, ist die Person bereits eingetragen. Wenn Sie die automatische Personenzuordnung nutzen, wird beim Speichern des Kontaktes eine zugehörige Person erzeugt

Eigenschaft	Beschreibung
	und in den Kontakt übernommen. Wenn Sie den Kontakt manuell erstellen, können Sie die Person aus der Auswahlliste auswählen.
Kontendefinition	Kontendefinition, über die der Kontakt erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des Kontaktes automatisch zu befüllen und um einen Automatisierungsgrad für den Kontakt festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Kontaktes ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Kontaktes nicht geändert werden. Um den Kontakt manuell über eine Kontendefinition zu erstellen, tragen Sie im Eingabefeld **Person** eine Person ein. Es können alle Kontendefinitionen ausgewählt werden, die dieser Person zugewiesen sind und über die noch kein Kontakt für diese Person erstellt wurde.
Automatisierungsgrad	Automatisierungsgrad des Kontaktes. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
Vorname	Vorname des Kontaktes. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Nachname	Nachname des Kontaktes. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Initialen	Initialen des Kontaktes. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Titel	Akademischer Titel des Kontaktes. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Anzeigename	Anzeigename des Kontaktes. Der Anzeigename wird aus dem Vornamen und dem Nachnamen des Kontaktes gebildet.
Strukturelle Objektklasse	Strukturelle Objektklasse, die den Typ des Objektes repräsentiert. Standardmäßig richten Sie Kontakte im One Identity Manager mit der Objektklasse "CONTACT" ein.

Eigenschaft	Beschreibung
Bezeichnung	Bezeichnung des Kontaktes. Die Bezeichnung wird aus dem Vornamen und dem Nachnamen des Kontaktes gebildet.
Definierter Name	Definierter Name des Kontaktes. Der definierte Name wird aus der Bezeichnung des Kontaktes und dem Container gebildet und kann nicht bearbeitet werden.
Domäne	Domäne, in der der Kontakt erzeugt werden soll.
Container	Container, in dem der Kontakt erzeugt werden soll. Haben Sie eine Kontendefinition zugeordnet, wird der Container, abhängig vom Automatisierungsgrad, aus den gültigen IT Betriebsdaten der zugeordneten Person ermittelt. Bei der Auswahl des Containers wird per Bildungsregel der definierte Name für den Kontakt ermittelt.
E-Mail-Adresse	E-Mail-Adresse des Kontaktes. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, die E-Mail-Adresse aus der Standard-E-Mail-Adresse der Person gebildet.
Risikoindex (berechnet)	Maximalwert der Risikoindexwerte aller zugeordneten Gruppen. Die Eigenschaft ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen an den Kontakt. Gruppen können selektiv an die Kontakte vererbt werden. Dazu werden die Gruppen und die Kontakte in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Identität	Typ der Identität des Kontaktes.
Gruppen erbbar	Angabe, ob Gruppen der Person geerbt werden. Wenn die Option aktiviert ist, werden Gruppen über hierarchische Rollen an den Kontakt vererbt. Wenn Sie eine Person mit Kontakten beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt der Kontakt diese Gruppen.

Verwandte Themen

- Kontendefinitionen für Active Directory Benutzerkonten auf Seite 45
- Unterstützte Typen von Benutzerkonten auf Seite 109
- Benutzerkonten mit Personen verbinden auf Seite 108
- Vererbung von Active Directory Gruppen anhand von Kategorien auf Seite 181

Kontaktinformationen eines Active Directory Kontaktes

Auf dem Tabreiter **Kontakt** erfassen Sie folgende Daten zur telefonischen Erreichbarkeit der Person, die den Kontakt verwendet.

Tabelle 51: Kontaktinformationen

Eigenschaft	Beschreibung
Telefon	Telefonnummer.
Telefon privat	Private Telefonnummer.
Fax	Faxnummer.
Mobiltelefon	Mobiltelefonnummer.
Funkruf	Funkrufnummer.
Webseite	Webseite.
IP Telefonnummer	IP-Telefonnummer.
Anmerkung	Freitextfeld für zusätzliche Erläuterungen.

Erweiterte Angaben zur Identifikation

Auf dem Tabreiter **Identifikation** erfassen Sie folgende Adressinformationen zur Erreichbarkeit der Person, die den Kontakt verwendet.

Tabelle 52: Stammdaten zur Identifikation

Eigenschaft	Beschreibung
Büro	Büro.
Straße	Straße.
Postfach	Postfach.
Postleitzahl	Postleitzahl.
Ort	Ort.
Bundesland	Bundesland.
Länderkennung	Länderkennung.
Firma	Firma der Person.
Abteilung	Abteilung der Person.

Eigenschaft	Beschreibung
Berufsbezeichnung	Berufsbezeichnung.
Personenkennung	Eindeutige Kennung der Person, zum Beispiel die ID.
Kontomanager	Verantwortlicher für den Kontakt. ***Um einen Kontomanager festzulegen*** 1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, welche die Kontomanager abbildet. 3. Wählen Sie unter **Kontomanager** den Verantwortlichen. 4. Klicken Sie **OK**.

Erweiterungsdaten eines Active Directory Kontaktes

Auf dem Tabreiter **Erweiterungen** erfassen Sie benutzerdefinierte Active Directory Schemaerweiterungen für den Kontakt.

Tabelle 53: Erweiterungsdaten

Eigenschaft	Beschreibung
Erweiterungsdaten	Unternehmensspezifische Erweiterungsdaten im Binärformat.
Attributerweiterung 01 - Attributerweiterung 15	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Zusätzliche Aufgaben für die Verwaltung von Active Directory Kontakten

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Überblick über den Active Directory Kontakt

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

Um einen Überblick über einen Kontakt zu erhalten

1. Wählen Sie die Kategorie **Active Directory | Kontakte**.
2. Wählen Sie in der Ergebnisliste den Kontakt.
3. Wählen Sie die Aufgabe **Überblick über den Active Directory Kontakt**.

Ändern des Automatisierungsgrades an einem Active Directory Kontakt

Wenn Sie Kontakte über die automatische Personenzuordnung erstellen, wird der Automatisierungsgrad **Unmanaged** genutzt. Sie können den Automatisierungsgrad eines Kontaktes nachträglich ändern.

Um den Automatisierungsgrad für einen Kontakt zu ändern

1. Wählen Sie die Kategorie **Active Directory | Kontakte**.
2. Wählen Sie in der Ergebnisliste den Kontakt.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Automatisierungsgrad** den Automatisierungsgrad.
5. Speichern Sie die Änderungen.

Active Directory Gruppen direkt an einen Active Directory Kontakt zuweisen

Gruppen können einem Kontakt direkt oder indirekt zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Gruppen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person einen Kontakt im Active Directory, werden die Gruppen der Rollen an diesen Kontakt vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Kontakt die Gruppen auch direkt zuweisen.

Um Gruppen direkt an einen Kontakt zuzuweisen

1. Wählen Sie die Kategorie **Active Directory | Kontakte**.
2. Wählen Sie in der Ergebnisliste den Kontakt.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Active Directory Gruppe an Active Directory Benutzerkonten, Active Directory Kontakte und Active Directory Computer zuweisen auf Seite 166
- Zulässigkeit von Gruppenmitgliedschaften auf Seite 163

Assistenten an einen Active Directory Kontakt zuweisen

Weisen Sie dem Kontakt einen Assistenten zu. Der Assistent wird im Microsoft Outlook in den Eigenschaften eines E-Mail-Empfängers abgebildet.

Um einen Assistenten an einen Kontakt zuzuweisen

1. Wählen Sie die Kategorie **Active Directory | Kontakte**.
2. Wählen Sie in der Ergebnisliste den Kontakt.
3. Wählen Sie die Aufgabe **Assistenten zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste **Tabelle** die Tabelle, welche die Assistenten enthält. Zur Auswahl stehen:
   - Active Directory Benutzerkonten
   - Active Directory Kontakte
   - Active Directory Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** den Assistenten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** den Assistenten.
6. Speichern Sie die Änderungen.

Active Directory Kontakt verschieben

Table Cell Outside Table:
HINWEIS: Kontakte können Sie nur innerhalb einer Domäne verschieben.

Um einen Kontakt zu verschieben

1. Wählen Sie die Kategorie **Active Directory | Kontakte**.
2. Wählen Sie in der Ergebnisliste den Kontakt.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Active Directory Container ändern**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Container** den neuen Container.
7. Speichern Sie die Änderungen.

Zusatzeigenschaften an einen Active Directory Kontakt zuweisen

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

Um Zusatzeigenschaften für einen Kontakt festzulegen

1. Wählen Sie die Kategorie **Active Directory | Kontakte**.
2. Wählen Sie in der Ergebnisliste den Kontakt.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

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

Löschen und Wiederherstellen von Active Directory Kontakten

Zum Löschen von Kontakten nutzt der One Identity Manager verschiedene Verfahren. Weitere Informationen finden Sie unter Löschen und Wiederherstellen von Active Directory Benutzerkonten auf Seite 146.

HINWEIS: Solange eine Kontendefinition für eine Person wirksam ist, behält die Person ihren daraus entstandenen Kontakt. Wird die Zuweisung einer Kontendefinition entfernt, dann wird der Kontakt, der aus dieser Kontendefinition entstanden ist, gelöscht.

Um einen Kontakt zu löschen

1. Wählen Sie die Kategorie **Active Directory | Kontakte**.
2. Wählen Sie in der Ergebnisliste den Kontakt.
3. Löschen Sie den Kontakt.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um einen Kontakt wiederherzustellen

1. Wählen Sie die Kategorie **Active Directory | Kontakte**.
2. Wählen Sie in der Ergebnisliste den Kontakt.
3. Klicken Sie in der Ergebnisliste die Schaltfläche **Löschen rückgängig machen**.

Konfigurieren der Löschverzögerung

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

7

Active Directory Gruppen

Zur Erläuterung des Gruppenkonzeptes unter Active Directory lesen Sie die Dokumentation zum eingesetzten Windows Server.

In Active Directory können Benutzerkonten, Kontakte, Computer und Gruppen in Gruppen zusammengefasst werden, mit denen sowohl innerhalb einer Domäne als auch domänenübergreifend der Zugriff auf Ressourcen geregelt werden kann.

Es wird unterschieden zwischen zwei Gruppentypen:

- Sicherheitsgruppen

  Über Sicherheitsgruppen werden Berechtigungen erteilt. In Sicherheitsgruppen werden Benutzerkonten, Computer und andere Gruppen aufgenommen und somit die Administration erleichtert. Sicherheitsgruppen werden außerdem als E-Mail Verteilergruppen eingesetzt.

- Verteilergruppen

  Verteilergruppen können als E-Mail aktivierte Verteilergruppen eingesetzt werden. Verteilergruppen haben keine Sicherheitsfunktion.

Weiterhin wird für jeden Gruppentyp ein Gruppenbereich definiert. Als Gruppenbereiche sind zulässig:

- Universal

  Gruppen mit diesem Bereich werden als universale Gruppen bezeichnet. Universale Gruppen können eingesetzt werden, um domänenübergreifend Berechtigungen zur Verfügung zu stellen. Mitglieder einer universalen Gruppe können Benutzerkonten und Gruppen aller Domänen einer Domänenstruktur sein.

- Lokale Domäne

  Gruppen mit diesem Bereich werden als Gruppen der lokalen Domäne bezeichnet. Lokale Gruppen werden eingesetzt, um Berechtigungen innerhalb einer Domäne zu erteilen. Mitglieder in einer Gruppe der lokalen Domäne können Benutzerkonten, Computer und Gruppen beliebiger Domänen sein.

- Global

  Gruppen mit diesem Bereich werden als globale Gruppen bezeichnet. Globale Gruppen können eingesetzt werden, um domänenübergreifend Berechtigungen zur Verfügung zu stellen. Mitglieder in einer globalen Gruppe sind nur Benutzerkonten, Computer und Gruppen der Domäne der globalen Gruppe.

Verwandte Themen

- Erfassen der Stammdaten für Active Directory Gruppen auf Seite 160
- Zulässigkeit von Gruppenmitgliedschaften auf Seite 163

Erfassen der Stammdaten für Active Directory Gruppen

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer Active Directory Gruppe auf Seite 160
- Erweiterungsdaten einer Active Directory Gruppe auf Seite 163

Allgemeine Stammdaten einer Active Directory Gruppe

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

Tabelle 54: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Bezeichnung	Bezeichnung der Gruppe. Aus der Bezeichnung der Gruppe wird der Gruppenname für die Vorgängerversionen **Gruppenname (pre Win2000)** gebildet.
Domäne	Domäne, in der die Gruppe angelegt werden soll.
Container	Container, in dem die Gruppe angelegt werden soll.
Definierter Name	Definierter Name der Gruppe. Der definierte Name wird per Bildungsregel aus dem Namen der Gruppe und dem Container ermittelt und kann nicht bearbeitet werden.

Eigenschaft	Beschreibung
Anzeigename	Anzeigename zur Anzeige der Gruppe in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Gruppenname (pre Win2000)	Gruppenname für die Vorgängerversionen. Der Gruppenname wird aus der Bezeichnung der Gruppe gebildet.
Strukturelle Objektklasse	Strukturelle Objektklasse, die den Typ des Objektes repräsentiert. Standardmäßig richten Sie Gruppen im One Identity Manager mit der Objektklasse GROUP ein.
Objektklasse	Liste von Klassen, die die Attribute dieses Objektes definieren. Als Objektklassen werden die Klassen angeboten, die durch die Synchronisation aus der Active Directory-Umgebung in die Datenbank eingelesen wurden. Sie können weitere Objektklassen und Hilfsklassen, die von anderen LDAP- und X.500 Verzeichnisdiensten genutzt werden, über das Eingabefeld hinzufügen.
Kontomanager	Verantwortlicher für die Gruppe. ***Um einen Kontomanager festzulegen*** 1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, welche die Konto-manager abbildet. 3. Wählen Sie unter **Kontomanager** den Verantwortlichen. 4. Klicken Sie **OK**.
Gruppenmanager darf die Mitgliederliste aktualisieren	Angabe, ob der Kontomanager die Mitgliedschaften für diese Gruppe ändern darf.
E-Mail-Adresse	E-Mail-Adresse der Gruppe.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten und Kontakte vererbt werden. Dazu werden die Gruppen und die Benutzerkonten oder die Kontakte in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

Eigenschaft	Beschreibung
Anmerkungen	Freitextfeld für zusätzliche Erläuterungen. Die Abkürzungen für die Kombinationen von Gruppentyp und Gruppenbereich werden in die Anmerkungen übernommen und sollten nicht geändert werden.
Sicherheitsgruppe	Gruppentyp. Über Sicherheitsgruppen werden Berechtigungen erteilt. In Sicherheitsgruppen werden Benutzerkonten, Computer und andere Gruppen aufgenommen und somit die Administration erleichtert. Sicherheitsgruppen werden außerdem als E-Mail Verteilergruppen eingesetzt.
Verteilergruppe	Gruppentyp. Verteilergruppen können als E-Mail Verteilergruppen eingesetzt werden. Verteilergruppen haben keine Sicherheitsfunktion.
Universale Gruppe	Gruppenbereich. Universale Gruppen können eingesetzt werden, um domänenübergreifend Berechtigungen zur Verfügung zu stellen. Mitglieder einer universalen Gruppe können Benutzerkonten und Gruppen aller Domänen einer Domänenstruktur sein.
Lokale Gruppe	Gruppenbereich. Lokale Gruppen werden eingesetzt, um Berechtigungen innerhalb einer Domäne zu erteilen. Mitglieder in einer Gruppe der lokalen Domäne können Benutzerkonten, Computer und Gruppen beliebiger Domänen sein.
Globale Gruppe	Gruppenbereich. Globale Gruppen können eingesetzt werden, um domänenübergreifend Berechtigungen zur Verfügung zu stellen. Mitglieder in einer globalen Gruppe sind nur Benutzerkonten, Computer und Gruppen der Domäne der globalen Gruppe.
IT Shop	Angabe, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Leistungsposition	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.

Verwandte Themen

- Vererbung von Active Directory Gruppen anhand von Kategorien auf Seite 181
- Ausführliche Informationen zur Vorbereitung der Gruppen für die Bestellung über den IT Shop finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Erweiterungsdaten einer Active Directory Gruppe

Auf dem Tabreiter **Erweiterungen** erfassen Sie benutzerdefinierte Active Directory Schemaerweiterungen für die Gruppe.

Tabelle 55: Erweiterungsdaten

Eigenschaft	Beschreibung
Attributerweiterung 01 - Attributerweiterung 15	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Zulässigkeit von Gruppenmitgliedschaften

Abhängig vom Aufbau der Domänenstruktur und den Vertrauensstellungen der Domänen sind unterschiedliche Zuweisungen zu Gruppen möglich. Genaue Informationen über zulässige Gruppenmitgliedschaften entnehmen Sie der Dokumentation zum eingesetzten Windows Server.

Um Gruppenmitgliedschaften über Forests abzubilden, stellen Sie Folgendes sicher:

- Die Vertrauensstellungen der Domänen sind bekannt.
- Der Name des Forests ist an der Domäne eingetragen.

In den nachfolgenden Tabellen sind die im One Identity Manager zulässigen Mitgliedschaften von Gruppen, Benutzerkonten, Kontakten und Computern in Gruppen aufgeführt.

Legende für die Tabellen:

- G = Global
- U = Universal
- L = Lokal

Tabelle 56: Zulässige Gruppenmitgliedschaften innerhalb einer Domäne

Zielgruppe		Mitglieder in der Zielgruppe								
		Gruppe						Benutzerkonto	Kontakt	Computer
		Verteiler			Sicherheit					
		G	U	L	G	U	L			
Verteiler	Global	x			x			x	x	x
	Universal	x	x		x	x		x	x	x
	Lokal	x	x	x	x	x	x	x	x	x
Sicherheit	Global	x			x			x	x	x
	Universal	x	x		x	x		x	x	x
	Lokal	x	x	x	x	x	x	x	x	x

Tabelle 57: Zulässige Gruppenmitgliedschaften in einer hierarchischen Domänenstruktur

Zielgruppe		Mitglieder in der Zielgruppe								
		Gruppe						Benutzerkonto	Kontakt	Computer
		Verteiler			Sicherheit					
		G	U	L	G	U	L			
Verteiler	Global								x	
	Universal	x	x		x	x		x	x	x
	Lokal	x	x		x	x		x	x	x
Sicherheit	Global									
	Universal	x	x		x	x		x	x	x
	Lokal	x	x		x	x		x	x	x

Tabelle 58: Zulässige Gruppenmitgliedschaften innerhalb einer Gesamtstruktur

Zielgruppe		Mitglieder in der Zielgruppe								
		Gruppe						Benut-zerkonto	Kontak-t	Compu-ter
		Verteiler			Sicherheit					
		G	U	L	G	U	L			
Verteiler	Global									
	Univer-sal									
	Lokal	x	x		x	x		x		x
Sicher-heit	Global									
	Univer-sal									
	Lokal	x	x		x	x		x		x

Tabelle 59: Zulässige Gruppenmitgliedschaften zwischen Gesamtstrukturen

Zielgruppe		Mitglieder in der Zielgruppe								
		Gruppe						Benut-zerkonto	Kontak-t	Compu-ter
		Verteiler			Sicherheit					
		G	U	L	G	U	L			
Verteiler	Global									
	Univer-sal									
	Lokal	x	x		x	x		x		x
Sicher-heit	Global									
	Univer-sal									
	Lokal	x	x		x	x		x		x

Verwandte Themen

- Vertrauensstellungen zwischen Active Directory Domänen auf Seite 101
- Active Directory spezifische Stammdaten einer Active Directory Domäne auf Seite 98

Active Directory Gruppe an Active Directory Benutzerkonten, Active Directory Kontakte und Active Directory Computer zuweisen

Gruppen können direkt oder indirekt an Benutzerkonten, Arbeitsplätze und Geräte zugewiesen werden. Bei der indirekten Zuweisung werden Personen (Arbeitsplätze, Geräte) und Gruppen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der Gruppen, die einer Person (einem Arbeitsplatz oder einem Gerät) zugewiesen ist.

Wenn Sie eine Person in Rollen aufnehmen und die Person ein Benutzerkonto oder einen Kontakt besitzt, dann wird dieses Benutzerkonto oder dieser Kontakt in die Gruppe aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind

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

Wenn Sie ein Gerät in die Rollen aufnehmen, dann wird der Computer, der dieses Gerät referenziert, in die Gruppe aufgenommen. Voraussetzungen für die indirekte Zuweisung an Computer sind

- Für die Rollenklasse (Abteilung, Kostenstelle, Standort oder Geschäftsrolle) ist die Zuweisung von Geräten und Gruppen erlaubt.
- Der Computer ist mit einem Gerät verbunden, das als PC oder als Server gekennzeichnet ist.
- Der Konfigurationsparameter **TargetSystem | ADS | HardwareInGroupFromOrg** ist aktiviert.

Wenn ein Gerät einen Arbeitsplatz besitzt und Sie den Arbeitsplatz in die Rollen aufnehmen, dann wird der Computer, der dieses Gerät referenziert, zusätzlich in alle Gruppen der Rollen des Arbeitsplatzes aufgenommen. Voraussetzungen für die indirekte Zuweisung an Computer über Arbeitsplätze sind

- Für die Rollenklasse (Abteilung, Kostenstelle, Standort oder Geschäftsrolle) ist die Zuweisung von Arbeitsplätzen und Gruppen erlaubt.
- Der Computer ist mit einem Gerät verbunden, das als PC oder als Server gekennzeichnet ist. Dieses Gerät besitzt einen Arbeitsplatz.

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

Detaillierte Informationen zum Thema

- Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 167
- Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 168
- Active Directory Benutzerkonten direkt an eine Active Directory Gruppe zuweisen auf Seite 170
- Active Directory Kontakte direkt an eine Active Directory Gruppe zuweisen auf Seite 171
- Active Directory Computer direkt an eine Active Directory Gruppe zuweisen auf Seite 172
- Active Directory Gruppe in Systemrollen aufnehmen auf Seite 173
- Active Directory Gruppe in den IT Shop aufnehmen auf Seite 174
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 176
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen

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

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

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
   - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
   - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
   - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

   Um eine Zuweisung zu entfernen

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

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

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

   - ODER -

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

   - ODER -

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 168
- Active Directory Benutzerkonten direkt an eine Active Directory Gruppe zuweisen auf Seite 170
- Active Directory Kontakte direkt an eine Active Directory Gruppe zuweisen auf Seite 171
- Active Directory Computer direkt an eine Active Directory Gruppe zuweisen auf Seite 172
- Active Directory Gruppe in Systemrollen aufnehmen auf Seite 173
- Active Directory Gruppe in den IT Shop aufnehmen auf Seite 174
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 176
- One Identity Manager Benutzer für die Verwaltung einer Active Directory-Umgebung auf Seite 10

Active Directory Gruppe an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Weisen Sie die Gruppe an Geschäftsrollen zu, damit die Gruppe über diese Geschäftsrollen an Benutzerkonten, Kontakte und Computer zugewiesen wird.

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

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Um Gruppen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 167
- Active Directory Benutzerkonten direkt an eine Active Directory Gruppe zuweisen auf Seite 170
- Active Directory Kontakte direkt an eine Active Directory Gruppe zuweisen auf Seite 171
- Active Directory Computer direkt an eine Active Directory Gruppe zuweisen auf Seite 172
- Active Directory Gruppe in Systemrollen aufnehmen auf Seite 173
- Active Directory Gruppe in den IT Shop aufnehmen auf Seite 174
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 176
- One Identity Manager Benutzer für die Verwaltung einer Active Directory-Umgebung auf Seite 10

Active Directory Benutzerkonten direkt an eine Active Directory Gruppe zuweisen

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

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppe direkt an Benutzerkonten zuweisen.

Um eine Gruppe direkt an Benutzerkonten zuzuweisen

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

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

   Um eine Zuweisung zu entfernen

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

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

Verwandte Themen

- Active Directory Gruppen direkt an ein Active Directory Benutzerkonto zuweisen auf Seite 135
- Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 167
- Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 168
- Active Directory Kontakte direkt an eine Active Directory Gruppe zuweisen auf Seite 171
- Active Directory Computer direkt an eine Active Directory Gruppe zuweisen auf Seite 172
- Active Directory Gruppe in Systemrollen aufnehmen auf Seite 173
- Active Directory Gruppe in den IT Shop aufnehmen auf Seite 174
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 176

- Zulässigkeit von Gruppenmitgliedschaften auf Seite 163
- Allgemeine Stammdaten eines Active Directory Benutzerkontos auf Seite 117

Active Directory Kontakte direkt an eine Active Directory Gruppe zuweisen

Gruppen können direkt oder indirekt an Kontakte zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Gruppen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person einen Kontakt im Active Directory, werden die Gruppen der Rollen an diesen Kontakt vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppe direkt an Kontakte zuweisen.

Um eine Gruppe direkt an Kontakte zuzuweisen

1. Wählen Sie die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Kontakte zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontakte zu.

   - ODER -

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

Verwandte Themen

- Active Directory Gruppen direkt an einen Active Directory Kontakt zuweisen auf Seite 155
- Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 167
- Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 168
- Active Directory Benutzerkonten direkt an eine Active Directory Gruppe zuweisen auf Seite 170
- Active Directory Computer direkt an eine Active Directory Gruppe zuweisen auf Seite 172
- Active Directory Gruppe in Systemrollen aufnehmen auf Seite 173
- Active Directory Gruppe in den IT Shop aufnehmen auf Seite 174
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 176
- Zulässigkeit von Gruppenmitgliedschaften auf Seite 163

Active Directory Computer direkt an eine Active Directory Gruppe zuweisen

Gruppen können direkt oder indirekt an Computer zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung des Gerätes, mit dem ein Computer verbunden ist und der Gruppen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppe direkt an Computer zuweisen.

Um eine Gruppe direkt an Computer zuzuweisen

1. Wählen Sie die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Computer zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Computer zu.

   - ODER -

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

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

Verwandte Themen

- Active Directory Computer direkt an Active Directory Gruppen zuweisen auf Seite 198
- Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 167
- Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 168
- Active Directory Benutzerkonten direkt an eine Active Directory Gruppe zuweisen auf Seite 170
- Active Directory Kontakte direkt an eine Active Directory Gruppe zuweisen auf Seite 171
- Active Directory Gruppe in Systemrollen aufnehmen auf Seite 173
- Active Directory Gruppe in den IT Shop aufnehmen auf Seite 174
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 176
- Zulässigkeit von Gruppenmitgliedschaften auf Seite 163
- Stammdaten eines Active Directory Computers auf Seite 195

Active Directory Gruppe in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

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

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

Um eine Gruppe an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 167
- Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 168
- Active Directory Benutzerkonten direkt an eine Active Directory Gruppe zuweisen auf Seite 170
- Active Directory Kontakte direkt an eine Active Directory Gruppe zuweisen auf Seite 171
- Active Directory Computer direkt an eine Active Directory Gruppe zuweisen auf Seite 172
- Active Directory Gruppe in den IT Shop aufnehmen auf Seite 174
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 176

Active Directory Gruppe in den IT Shop aufnehmen

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

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

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

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

Um eine Gruppe in den IT Shop aufzunehmen

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie im Manager die Kategorie **Berechtigungen | Active Directory Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.

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

Um eine Gruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

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

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

Verwandte Themen

- Allgemeine Stammdaten einer Active Directory Gruppe auf Seite 160
- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 176
- Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 167
- Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 168
- Active Directory Benutzerkonten direkt an eine Active Directory Gruppe zuweisen auf Seite 170
- Active Directory Kontakte direkt an eine Active Directory Gruppe zuweisen auf Seite 171
- Active Directory Computer direkt an eine Active Directory Gruppe zuweisen auf Seite 172
- Active Directory Gruppe in Systemrollen aufnehmen auf Seite 173

Active Directory Gruppen automatisch in den IT Shop aufnehmen

Tabelle 60: Konfigurationsparameter für die automatische Aufnahme von Gruppen in den IT Shop

Konfigurationsparameter	Beschreibung
QER | ITShop | GroupAutoPublish	Präprozessorrelevanter Konfigurationsparameter zur automatischen Übernahme von Gruppen in den IT Shop. Der Konfigurationsparameter legt fest, ob alle Gruppen der Zielsysteme Active Directory und SharePoint automatisch in den IT Shop übernommen werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.
QER | ITShop | GroupAutoPublish | ADSGroupExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Active Directory Gruppen, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`

Um Gruppen automatisch in den IT Shop aufzunehmen

1. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | GroupAutoPublish**.
2. Aktivieren Sie im Designer den Konfigurationsparameter **QER | ITShop | GroupAutoPublish | ADSGroupExcludeList** und legen Sie die Active Directory Gruppen fest, die nicht automatisch in den IT Shop übernommen werden sollen.
3. Kompilieren Sie die Datenbank.

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

- Die Synchronisation sorgt dafür, dass die Gruppen in den IT Shop aufgenommen werden. Bei Bedarf können Sie die Synchronisation im Synchronization Editor sofort starten.
- Gruppen, die im One Identity Manager neu erstellt werden, werden 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 Gruppe ermittelt.

   Für jede Gruppe wird die Leistungsposition geprüft und bei Bedarf angepasst. Die Bezeichnung der Leistungsposition entspricht der Gruppenbezeichnung. Die Leistungsposition wird einer der Standard-Servicekategorien zugeordnet.

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

2. Es wird eine Anwendungsrolle für Produkteigner ermittelt und der Leistungsposition zugeordnet. Die Produkteigner können Bestellungen von Mitgliedschaften in diesen Gruppen genehmigen. Standardmäßig wird der Kontomanager einer Gruppe als Produkteigner ermittelt.

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

   - Ist der Kontomanager der Gruppe bereits Mitglied einer Anwendungsrolle für Produkteigner, dann wird diese Anwendungsrolle der Leistungsposition zugewiesen. Alle Mitglieder dieser Anwendungsrolle werden dadurch Produkteigner der Gruppe.
   - Ist der Kontomanager der Gruppe 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 Gruppe keine Kontomanager wird die Standard-Anwendungsrolle **Request & Fulfillment | IT Shop | Produkteigner | Ohne Eigentümer im AD** verwendet.

3. Die Gruppe 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 Gruppenmitgliedschaften über das Web Portal bestellen.

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

Verwandte Themen

- Active Directory Gruppe in den IT Shop aufnehmen auf Seite 174
- Active Directory Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 167
- Active Directory Gruppe an Geschäftsrollen zuweisen auf Seite 168

- Active Directory Benutzerkonten direkt an eine Active Directory Gruppe zuweisen auf Seite 170
- Active Directory Kontakte direkt an eine Active Directory Gruppe zuweisen auf Seite 171
- Active Directory Computer direkt an eine Active Directory Gruppe zuweisen auf Seite 172
- Active Directory Gruppe in Systemrollen aufnehmen auf Seite 173
- Standardlösungen für die Bestellung von Active Directory Gruppen und Gruppenmitgliedschaften auf Seite 186
- One Identity Manager Administrationshandbuch für IT Shop

Zusätzliche Aufgaben für die Verwaltung von Active Directory Gruppen

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Überblick über die Active Directory Gruppe

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

Um einen Überblick über eine Gruppe zu erhalten

1. Wählen Sie die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die Active Directory Gruppe**.

Active Directory Gruppen in Active Directory Gruppen aufnehmen

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

Um Gruppen direkt an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die der ausgewählten Gruppe untergeordnet sind.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Zulässigkeit von Gruppenmitgliedschaften auf Seite 163

Wirksamkeit von Gruppenmitgliedschaften

Tabelle 61: Konfigurationsparameter für die bedingte Vererbung

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

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

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

HINWEIS:

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

- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.
- Ob die Mitgliedschaft einer ausgeschlossenen Gruppe in einer anderen Gruppe zulässig ist (Tabelle), wird durch den One Identity Manager nicht überprüft.

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

Beispiel für die Wirksamkeit von Gruppenmitgliedschaften

- In einer Domäne ist eine Gruppe A mit Berechtigungen zum Auslösen von Bestellungen definiert. Eine Gruppe B berechtigt zum Anweisen von Zahlungen. Eine Gruppe C berechtigt zum Prüfen von Rechnungen.
- Gruppe A wird über die Abteilung "Marketing", Gruppe B über die Abteilung "Finanzen" und Gruppe C wird über die Geschäftsrolle "Kontrollgruppe" zugewiesen.

Clara Harris hat ein Benutzerkonto in dieser Domäne. Sie gehört primär der Abteilung "Marketing" an. Sekundär sind ihr die Geschäftsrolle "Kontrollgruppe" und die Abteilung "Finanzen" zugewiesen. Ohne Ausschlussdefinition erhält das Benutzerkonto alle Berechtigungen der Gruppen A, B und C.

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

Tabelle 62: Festlegen der ausgeschlossenen Gruppen (Tabelle `ADSGroupExclusion`)

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

Tabelle 63: Wirksame Zuweisungen

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

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

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

Tabelle 64: Ausgeschlossene Gruppen und wirksame Zuweisungen

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

Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherite | GroupExclusion** ist aktiviert.
- Sich ausschließende Gruppen gehören zur selben Domäne.

Um Gruppen auszuschließen

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste eine Gruppe.
3. Wählen Sie die Aufgabe **Gruppen ausschließen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu, die sich mit der gewählten Gruppe ausschließen.

   - ODER -

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

Vererbung von Active Directory Gruppen anhand von Kategorien

Im One Identity Manager können Gruppen selektiv an die Benutzerkonten und Kontakte vererbt werden. Dazu werden die Gruppen und die Benutzerkonten (Kontakte) in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine

Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält die Tabellen, in denen die Benutzerkonten (Kontakte) und die Gruppen abgebildet werden. In der Tabelle für Benutzerkonten (Kontakte) legen Sie Ihre Kategorien für die Benutzerkonten (Kontakte) fest. In Gruppentabelle geben Sie Ihre Kategorien für die Gruppen an. Jede Tabelle enthält die Kategoriepositionen **Position 1** bis **Position 31**.

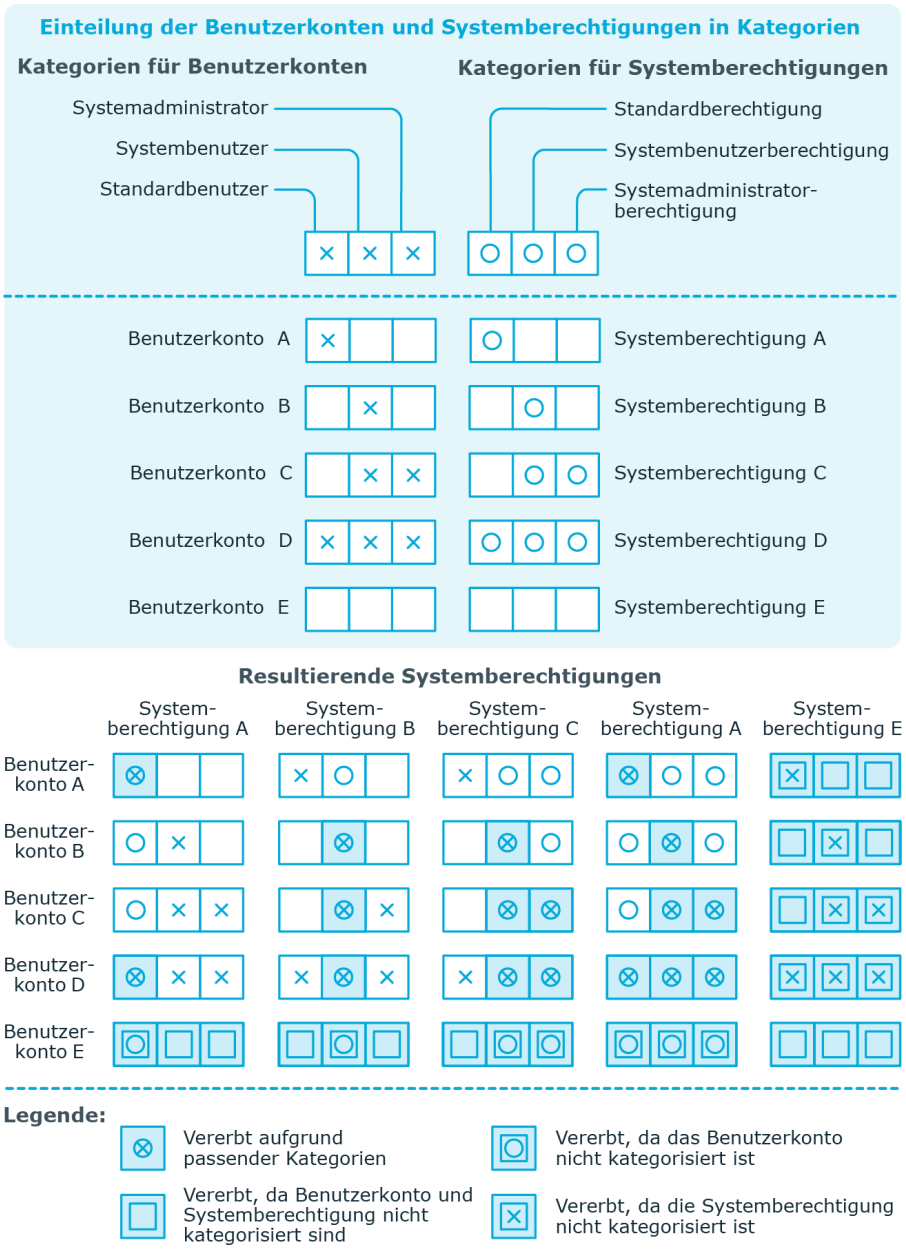
Jedes Benutzerkonto (Kontakt) kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto (Kontakt) und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto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

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

Tabelle 65: Beispiele für Kategorien

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

Abbildung 2: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

- Definieren Sie an der Domäne die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten und Kontakten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Gruppen über ihre Stammdaten zu.

Verwandte Themen

- Festlegen der Kategorien für die Vererbung von Active Directory Gruppen auf Seite 100
- Allgemeine Stammdaten eines Active Directory Benutzerkontos auf Seite 117
- Allgemeine Stammdaten eines Active Directory Kontaktes auf Seite 150
- Allgemeine Stammdaten einer Active Directory Gruppe auf Seite 160

Active Directory Kontenrichtlinien an eine Active Directory Gruppe zuweisen

Für Domänen ab der Funktionsebene **Windows Server 2008 R2** ist es möglich zu den Standardkennwortrichtlinien der Domäne weitere Kontenrichtlinien zu definieren. Somit können einzelne Benutzerkonten und Gruppen mit strengeren Kontenrichtlinien versehen werden, als es die globalen Einstellungen vorsehen.

Um Kontenrichtlinien für eine Gruppe festzulegen

1. Wählen Sie die Kategorie **Active Directory | Gruppe**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Kontenrichtlinien zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Kontenrichtlinien zu.

   - ODER -

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

Verwandte Themen

- Active Directory Kontenrichtlinien für Active Directory Domänen auf Seite 102
- Globale Kontenrichtlinien für eine Active Directory Domäne auf Seite 97
- Active Directory Kontenrichtlinien an ein Active Directory Benutzerkonto zuweisen auf Seite 134

Assistenten an eine Active Directory Gruppe zuweisen

Weisen Sie der Gruppe einen Assistenten zu. Der Assistent wird im Microsoft Outlook in den Eigenschaften eines E-Mail-Empfängers abgebildet.

Um einen Assistenten an eine Gruppe zuzuweisen

1. Wählen Sie die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Assistenten zuweisen**.
4. Wählen Sie im oberen Bereich des Formulars in der Auswahlliste **Tabelle** die Tabelle, welche die Assistenten enthält. Zur Auswahl stehen:
   - Active Directory Benutzerkonten
   - Active Directory Kontakte
   - Active Directory Gruppen
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** den Assistenten zu.

   - ODER -

   Entfernen Sie im Bereich **Zuordnungen entfernen** den Assistenten.
6. Speichern Sie die Änderungen.

Active Directory Gruppe verschieben

HINWEIS: Gruppen können Sie nur innerhalb einer Domäne verschieben.

Um eine Gruppe zu verschieben

1. Wählen Sie die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Active Directory Container ändern**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Container** den neuen Container.
7. Speichern Sie die Änderungen.

Zusatzeigenschaften an eine Active Directory Gruppe zuweisen

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

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie im Manager die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

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

   Um eine Zuweisung zu entfernen

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

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

Löschen von Active Directory Gruppen

Um eine Active Directory Gruppe zu löschen

1. Wählen Sie die Kategorie **Active Directory | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Löschen Sie die Gruppe über die Schaltfläche .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Gruppe wird endgültig aus der One Identity Manager-Datenbank und der Active Directory-Umgebung gelöscht.

HINWEIS: Beim Löschen einer Gruppe wird im One Identity Manager ein Eintrag für die Active Directory SID erzeugt. Weitere Informationen finden Sie unter Active Directory Sicherheits-IDs auf Seite 190.

Standardlösungen für die Bestellung von Active Directory Gruppen und Gruppenmitgliedschaften

Im One Identity Manager werden Standardprodukte und Standard-Entscheidungsworkflows bereitgestellt, um Active Directory Gruppen sowie Mitgliedschaften in diesen Gruppen über den IT Shop zu bestellen. Dadurch werden Berechtigungen in den Zielsystemen über definierte Genehmigungsverfahren vergeben. Produkteigner und

Zielsystemverantwortliche können im Web Portal die Eigenschaften dieser Gruppen bearbeiten und Änderungen beantragen.

Ausführliche Informationen dazu finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

Detaillierte Informationen zum Thema

- Anlegen von Active Directory Gruppen auf Seite 187
- Ändern von Active Directory Gruppen auf Seite 188
- Löschen von Active Directory Gruppen auf Seite 188
- Active Directory Gruppenmitgliedschaften bestellen auf Seite 189

Anlegen von Active Directory Gruppen

Über die Bestellung dieser Standardprodukte können neue Sicherheitsgruppen oder Verteilergruppen im Active Directory angelegt werden. Der Besteller gibt Informationen über Namen, Container und Domäne, soweit bekannt, der Bestellung mit. Anhand dieser Informationen bestimmt der Zielsystemverantwortliche den Container, in dem die Gruppe angelegt werden soll, und genehmigt die Bestellung. Die Gruppe wird im One Identity Manager angelegt und in das Zielsystem publiziert.

Voraussetzung

- Der Anwendungsrolle **Zielsysteme | Active Directory** sind Personen zugewiesen.

Wenn der Konfigurationsparameter **QER | ITShop | GroupAutoPublish** aktiviert ist, wird die Gruppe in den IT Shop aufgenommen und dem Regal **Identity & Access Lifecycle | Active Directory Gruppen** zugewiesen. Die Gruppe wird der Servicekategorie **Sicherheitsgruppe** beziehungsweise **Verteilergruppe** zugeordnet.

Tabelle 66: Standardobjekte für die Bestellung einer Active Directory Gruppe

Produkte:	Anlegen einer Active Directory Sicherheitsgruppe Anlegen einer Active Directory Verteilergruppe
Servicekategorie:	Active Directory Gruppen
Regal:	Identity & Access Lifecycle | Gruppen Lifecycle
Entscheidungsrichtlinie/ Entscheidungsworkflow:	Entscheidung der Bestellungen zur Neuanlage von Active Directory Gruppen

Detaillierte Informationen zum Thema

- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 176

Ändern von Active Directory Gruppen

Produkteigner und Zielsystemverantwortliche können im Web Portal beantragen den Gruppentyp und den Gruppenbereich von Active Directory Gruppen zu ändern. Der Zielsystemverantwortliche muss diese Änderung genehmigen. Die Änderung wird in das Zielsystem publiziert.

Voraussetzungen

- Die Gruppe ist im IT Shop bestellbar.
- Der Anwendungsrolle **Zielsysteme | Active Directory** sind Personen zugewiesen.

Tabelle 67: Standardobjekte für das Ändern einer Active Directory Gruppe

Produkt:	Ändern einer Active Directory Gruppe
Servicekategorie:	nicht zugeordnet
Regal:	Identity & Access Lifecycle | Gruppen Lifecycle
Entscheidungsrichtlinie/ Entscheidungsworkflow:	Entscheidung der Bestellungen von Änderungen an Active Directory Gruppen

Löschen von Active Directory Gruppen

Produkteigner und Zielsystemverantwortliche können im Web Portal beantragen, dass eine Active Directory Gruppe gelöscht wird. Der Produkteigner oder der Zielsystemverantwortliche muss das Löschen genehmigen. Die Gruppe wird im One Identity Manager gelöscht und die Änderung in das Zielsystem publiziert.

Voraussetzungen

- Die Gruppe ist im IT Shop bestellbar.
- Der Anwendungsrolle **Zielsysteme | Active Directory** sind Personen zugewiesen.

Tabelle 68: Standardobjekte für das Löschen einer Active Directory Gruppe

Produkt:	Löschen einer Active Directory Gruppe
Servicekategorie:	nicht zugeordnet
Regal:	Identity & Access Lifecycle | Gruppen Lifecycle
Entscheidungsrichtlinie/ Entscheidungsworkflow:	Entscheidung der Bestellungen zum Löschen von Active Directory Gruppen

Active Directory Gruppenmitgliedschaften bestellen

Tabelle 69: Standardobjekte für das Bestellen von Gruppenmitgliedschaften

Regale:	Identity & Access Lifecycle | Active Directory Gruppen
Entscheidungsrichtlinien/ Entscheidungsworkflows:	Entscheidung der Bestellungen von Active Directory Gruppenmitgliedschaften

Produkteigner und Zielsystemverantwortliche können im Web Portal Mitgliedschaften für die Gruppen in diesem Regal bestellen. Der jeweilige Produkteigner oder Zielsystemverantwortliche muss diese Änderung genehmigen. Die Änderung wird in das Zielsystem publiziert.

Verwandte Themen

- Active Directory Gruppen automatisch in den IT Shop aufnehmen auf Seite 176
- Anlegen von Active Directory Gruppen auf Seite 187

Active Directory Sicherheits-IDs

Die Sicherheits-ID (SID) wird im One Identity Manager verwendet, um Benutzerkonten und Gruppen anderer Domänen zu identifizieren. Dies ist unter anderem für die Synchronisation von Gruppenmitgliedschaften zweier Domänen erforderlich. Des weiteren wird die SID verwendet, um Zugriffsberechtigungen auf Dateisystemebene zu ermitteln.

Beispiel

Die Domäne A wird mit dem One Identity Manager synchronisiert. Mit der Domäne B erfolgt zunächst keine Synchronisation. Die Domänen befinden sich in einer Vertrauensstellung. In den Gruppen der Domäne A sind Benutzerkonten der Domäne A und der Domäne B vorhanden.

Bei der Synchronisation der Domäne A werden die Gruppenmitgliedschaften erkannt. Benutzerkonten der Domäne A können anhand ihrer Bezeichnung zugeordnet werden. Für die Benutzerkonten der Domäne B werden die SIDs ermittelt und im One Identity Manager eingetragen.

Wird die Domäne B zu einem späteren Zeitpunkt synchronisiert, werden die Benutzerkonten anhand ihrer SID erkannt und es erfolgt eine direkte Zuordnung der Benutzerkonten zu den Gruppen der Domäne A. Der Eintrag der SID wird aus der One Identity Manager-Datenbank entfernt.

Um Sicherheits-IDs anzuzeigen:

- Wählen Sie die Kategorie **Active Directory | Active Directory SIDs**.

HINWEIS: Beim Löschen eines Active Directory Objektes wird im One Identity Manager ein Eintrag für die SID erzeugt.

9

Active Directory Containerstrukturen

Die Container werden in einer hierarchischen Baumstruktur dargestellt. Bereits vorhandene Container können durch die Synchronisation aus der Active Directory-Umgebung in die One Identity Manager-Datenbank eingelesen werden. Systemcontainer, welche bei der Synchronisation in die One Identity Manager-Datenbank übernommen wurden, sind entsprechend gekennzeichnet. Die Systemcontainer werden bei der Synchronisation nur beachtet, wenn die entsprechende Konfigurationsoption gesetzt ist.

Einrichten von Active Directory Containern

Um die Stammdaten eines Containers zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Active Directory | Container**.
2. Wählen Sie in der Ergebnisliste den Container und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Detaillierte Informationen zum Thema

- Stammdaten eines Active Directory Containers auf Seite 192

Stammdaten eines Active Directory Containers

Für Container erfassen Sie folgende Stammdaten.

Tabelle 70: Stammdaten eines Containers

Eigenschaft	Beschreibung
Bezeichnung	Name des Containers.
Definierter Name	Definierter Name des Containers. Der definierte Name für den angelegten Container wird per Bildungsregel aus dem Namen des Containers, der Objektklasse, dem übergeordneten Container und der Domäne ermittelt und kann nicht geändert werden.
Strukturelle Objektklasse	Strukturelle Objektklasse, die den Typ des Objektes repräsentiert.
Objektklasse	Liste von Klassen, die die Attribute dieses Objektes definieren. Als Objektklassen werden die Klassen angeboten, die durch die Synchronisation aus der Active Directory-Umgebung in die Datenbank eingelesen wurden. Sie können jedoch zusätzliche Objektklassen in das Eingabefeld eintragen. Abhängig von der Objektklasse können die weiteren Eigenschaften bearbeitet werden. HINWEIS: Neue Container sollten Sie als Organisationseinheiten (Objektklasse `ORGANIZATIONALUNIT`) einrichten. Organisationseinheiten (beispielsweise Geschäftsstellen oder Abteilungen) werden dazu genutzt, Objekte des Active Directory wie Benutzerkonten, Gruppen und Computer logisch zu organisieren und somit die Verwaltung der Objekte zu erleichtern. Die Organisationseinheiten können in einer hierarchischen Containerstruktur verwaltet werden.
Domäne	Domäne des Containers.
Übergeordneter Container	Übergeordneter Container zur Abbildung einer hierarchischen Containerstruktur. Der definierte Name wird dann automatisch durch Bildungsregeln aktualisiert.
Kontomanager	Verantwortlicher für den Container. ***Um einen Kontomanager festzulegen*** 1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, welche die

Eigenschaft	Beschreibung
	Kontomanager abbildet. 3. Wählen Sie unter **Kontomanager** den Verantwortlichen. 4. Klicken Sie **OK**.
Zielsystemverantwortlicher	Anwendungsrolle, in der die Zielsystemverantwortlichen des Containers festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Containers, dem sie zugeordnet sind. Jedem Container können somit andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle, deren Mitglieder verantwortlich für die Administration dieses Containers sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.
Straße	Straße.
Postleitzahl	Postleitzahl.
Standort	Standort.
Bundesland	Bundesland.
Länderkennung	Länderkennung.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Erweiterte Funktion	Filterkriterium in weiteren Darstellungen der Container. Container, die mit der Option gekennzeichnet sind, werden im Active Directory-Benutzerkonto und -Computer Manager nur angezeigt, wenn dort die erweiterte Konsolenstruktur-Ansicht aktiviert wurde.
Schutz vor versehentlichem Löschen	Angabe, ob der Container gegen versehentliches Löschen geschützt werden soll. Ist die Option aktiviert, werden die Löschberechtigungen auf das Container-Objekt entfernt.

Verwandte Themen

- Zielsystemverantwortliche auf Seite 79

Zusätzliche Aufgaben zur Verwaltung von Active Directory Containern

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Überblick über den Active Directory Container

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

Um einen Überblick über einen Container zu erhalten

1. Wählen Sie die Kategorie **Active Directory | Container**.
2. Wählen Sie in der Ergebnisliste den Container.
3. Wählen Sie die Aufgabe **Überblick über den Active Directory Container**.

Active Directory Container verschieben

HINWEIS: Container können Sie nur innerhalb einer Domäne verschieben.

Um einen Container zu verschieben

1. Wählen Sie die Kategorie **Active Directory | Container**.
2. Wählen Sie in der Ergebnisliste den Container.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Active Directory Container ändern**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Container** den neuen Container.
7. Speichern Sie die Änderungen.

Active Directory Computer

Durch die Synchronisation werden die Computer und Server in den One Identity Manager eingelesen.

Um die Stammdaten eines Computers zu bearbeiten

1. Wählen Sie die Kategorie **Active Directory | Computer**.
2. Wählen Sie in der Ergebnisliste den Computer und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

   Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten für einen Computer.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten eines Active Directory Computers auf Seite 195
- Bearbeiten eines Servers auf Seite 81

Stammdaten eines Active Directory Computers

Für einen Computer erfassen Sie die folgenden Stammdaten.

Tabelle 71: Stammdaten eines Computers

Eigenschaft	Beschreibung
Gerät	Gerät, mit dem der Computer verbunden ist. Legen Sie über die Schaltfläche neben der Auswahlliste ein neues Gerät an. Ausführliche Informationen zur Geräteverwaltung finden Sie im *One*

Eigenschaft	Beschreibung
	Identity Manager Administrationshandbuch für das Identity Management Basismodul.
Bezeichnung	Bezeichnung des Computers.
Domäne	Domäne, in der der Computer erzeugt werden soll.
Container	Container, in dem der Computer erzeugt werden soll. Bei der Auswahl des Containers wird per Bildungsregel der definierte Name für den Computer ermittelt.
Primäre Gruppe	Primäre Gruppe des Computers. Es stehen dabei nur die Gruppen zur Auswahl, die dem Computer bereits zugewiesen wurden.
Kontomanager	Verantwortlicher für den Computer. ***Um einen Kontomanager festzulegen*** 1. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld. 2. Wählen Sie unter **Tabelle** die Tabelle, welche die Kontomanager abbildet. 3. Wählen Sie unter **Kontomanager** den Verantwortlichen. 4. Klicken Sie **OK**.
Computername (pre Win2000)	Prä-Windows 2000 Computername. Computername für die Vorgängerversion von Windows 2000.
DNS Hostname	DNS-Name des Computers.
Funktion	Funktion des Computers im Netzwerk. Es stehen die Funktionen **Workstation**, **Server** und **Domain Controller** zur Auswahl.
Betriebssystem	Bezeichnung des Betriebssystems.
Version Betriebssystem	Version des Betriebssystems.
Servicepack Betriebssystem	Bezeichnung des Servicepacks.
Hotfix Betriebssystem	Bezeichnung des Hotfixes.

Zusätzliche Aufgaben für die Verwaltung von Active Directory Computern

Nachdem Sie die Stammdaten erfasst haben, können Sie die folgenden Aufgaben ausführen.

Überblick über den Active Directory Computer

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

Um einen Überblick über einen Computer zu erhalten

1. Wählen Sie die Kategorie **Active Directory | Computer**.
2. Wählen Sie in der Ergebnisliste den Computer.
3. Wählen Sie die Aufgabe **Überblick über die Active Directory Computer**.

Active Directory Computer verschieben

HINWEIS: Computer können Sie nur innerhalb einer Domäne verschieben.

Um einen Computer zu verschieben

1. Wählen Sie die Kategorie **Active Directory | Computer**.
2. Wählen Sie in der Ergebnisliste den Computer.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Active Directory Container ändern**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Wählen Sie auf dem Tabreiter **Allgemein** in der Auswahlliste **Container** den neuen Container.
7. Speichern Sie die Änderungen.

Active Directory Computer direkt an Active Directory Gruppen zuweisen

Gruppen können direkt oder indirekt an Computer zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung des Gerätes, mit dem ein Computer verbunden ist und der Gruppen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen.

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Computer die Gruppen auch direkt zuweisen.

Um einen Computer direkt an Gruppen zuzuweisen

1. Wählen Sie die Kategorie **Active Directory | Computer**.
2. Wählen Sie in der Ergebnisliste den Computer.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppen zu.

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

   Um eine Zuweisung zu entfernen

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

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

Verwandte Themen

- Active Directory Gruppe an Active Directory Benutzerkonten, Active Directory Kontakte und Active Directory Computer zuweisen auf Seite 166
- Zulässigkeit von Gruppenmitgliedschaften auf Seite 163
- Stammdaten eines Active Directory Computers auf Seite 195

Diagnose eines Computers ausführen

Bei Erreichbarkeit des Computers im Netz und mit ausreichenden Zugriffsberechtigungen können Sie über die folgenden Aufgaben eine Diagnose durchführen.

Tabelle 72: Aufgaben für die Diagnose

Aufgabe	Beschreibung
Diagnose - Browse	Es wird ein Fenster des Windows Explorers geöffnet. Angezeigt werden alle Freigaben des ausgewählten Computers.
Diagnose - Windows Diagnose	Es werden die Systeminformationen (`winmsd.exe` oder `msinfo32.exe`) des Computers geöffnet.
Windows Computerverwaltung	Es wird die Microsoft Management Konsole zur Computerverwaltung für den ausgewählten Computer geöffnet. Hier können Sie beispielsweise das Ereignisprotokoll oder die lokale Benutzerverwaltung einsehen.

Um Diagnosen für einen Computer auszuführen

1. Wählen Sie die Kategorie **Active Directory | Computer**.
2. Wählen Sie in der Ergebnisliste den Computer und führen Sie die gewünschte Aufgabe zur Diagnose aus.

11

Active Directory Drucker

Bei der Synchronisation werden alle freigegebenen Drucker einer Domäne in den One Identity Manager eingelesen.

Um Drucker anzuzeigen

1. Wählen Sie die Kategorie **Active Directory | Drucker**.
2. Wählen Sie in der Ergebnisliste einen Drucker und wählen Sie die Aufgabe **Stammdaten bearbeiten**.

Folgende Informationen zu einem Drucker werden abgebildet.

Tabelle 73: Stammdaten eines Druckers

Eigenschaft	Beschreibung
Druckername	Bezeichnung des Druckers.
Treiber	Bezeichnung des Druckertreibers.
Active Directory Computer	Computer oder Server, mit dem der Drucker verbunden ist.
Vollständiger Server-name	Vollständiger Name des Servers, mit dem der Drucker verbunden ist.
Server	Kurzbezeichnung des Servers.
Port	Anschluss des Druckers.
UNC Name	Universal Naming Convention (UNC) Adresse des Druckers.
Standortbeschreibung	Freitextfeld für zusätzliche Erläuterungen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Duplex	Abgabe, ob beidseitiges Drucken unterstützt wird.
Farbe	Angabe, ob Farbdruck unterstützt wird.
Sortierer unterstützt	Angabe, ob der Drucker eine Sortierung unterstützt.

Eigenschaft	Beschreibung
Seite pro Minute	Druckergeschwindigkeit in Seiten pro Minute.
Max. Auflösung [dpi]	Maximale Druckerauflösung in dpi.
Max. Auflösung horizontal	Maximale Druckerauflösung entlang der X-Achse (Breite).
Max. Auflösung vertikal	Maximale Druckerauflösung entlang der Y-Achse (Höhe).
Freies Feld Nr. 01 ... Freies Feld Nr. 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

12

Active Directory Standorte

Standorte sind eine Gruppierung von Computern anhand von Netzwerkinformationen. Im Active Directory werden die Standortinformationen verwendet, um die Replikation zwischen Domänencontrollern zu steuern.

Die Informationen zu Active Directory Standorten werden durch die Synchronisation in den One Identity Manager eingelesen und können nicht bearbeitet werden.

Um Informationen zu einem Standort anzuzeigen

1. Wählen Sie die Kategorie **Active Directory | Standort**.
2. Wählen Sie in der Ergebnisliste einen Standort.
3. Um die Server eines Standortes anzuzeigen, wählen Sie die Aufgabe **Überblick über den Standort**.
4. Um die Stammdaten eines Standortes anzuzeigen, wählen Sie die Aufgabe **Stammdaten bearbeiten** .

Folgende Informationen werden zu einem Standort abgebildet.

Tabelle 74: Stammdaten eines Standortes

Eigenschaft	Beschreibung
Bezeichnung	Name des Standortes.
Kanonischer Name	Kanonischer Name des Standortes.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Standortbeschreibung	Freitextfeld für zusätzliche Erläuterungen.
Gesamtstruktur	Name der Gesamtstruktur, zu der dieser Standort gehört.
Subnetze	Bereiche von IP-Adressen am Standort.

Verwandte Themen

- Informationen zur Active Directory Gesamtstruktur auf Seite 100

13

Berichte über Active Directory Objekte

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

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

Tabelle 75: Berichte für das Zielsystem

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

Bericht	Beschreibung
Systemberechtigungen anzeigen	manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen anzeigen	Der Bericht enthält alle Benutzerkonten der Domäne, die eine überdurchschnittliche Anzahl an Gruppenmitgliedschaften besitzen.
Active Directory Benutzerkonten- und Gruppenverteilung	Der Bericht enthält eine Zusammenfassung zur Benutzerkonten- und Gruppenverteilung aller Domänen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**.
Datenqualität der Active Directory Benutzerkonten	Der Bericht enthält verschiedenen Auswertungen zur Datenqualität der Benutzerkonten aller Domänen. Den Bericht finden Sie in der Kategorie **Mein One Identity Manager**.

Verwandte Themen

- Übersicht aller Zuweisungen auf Seite 204

Übersicht aller Zuweisungen

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

Beispiele

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

- Wird der Bericht für eine Geschäftsrolle erstellt, werden alle Rollen ermittelt, in denen die Personen der gewählten Geschäftsrolle ebenfalls Mitglied sind.

Um detaillierte Informationen über Zuweisungen anzuzeigen

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

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.
- Mit einem Maus-Doppelklick auf das Steuerelement einer Rolle zeigen Sie alle untergeordneten Rollen der ausgewählten Rolle an.
- Mit einem einfachen Mausklick auf die Schaltfläche im Steuerelement einer Rolle zeigen Sie alle Personen dieser Rolle an, die das Basisobjekt besitzen.
- Über den Pfeil rechts neben der Schaltfläche starten Sie einen Assistenten, mit dem Sie die Liste der angezeigten Personen zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Personen werden der Geschäftsrolle zugeordnet.

Abbildung 3: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 76: Bedeutung der Symbole in der Symbolleiste des Berichts

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

Anhang A

Konfigurationsparameter für die Verwaltung einer Active Directory-Umgebung

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

Tabelle 77: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
QER | ITShop | GroupAutoPublish	Präprozessorrelevanter Konfigurationsparameter zur automatischen Übernahme von Gruppen in den IT Shop. Der Konfigurationsparameter legt fest, ob alle Gruppen der Zielsysteme Active Directory und SharePoint automatisch in den IT Shop übernommen werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.
QER | ITShop | GroupAutoPublish | ADSGroupExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Gruppen, für die keine automatische Zuordnung zum IT Shop erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
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.
TargetSystem | ADS | Accounts	Der Konfigurationsparameter erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem | ADS | Accounts |	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben

Konfi-gurationsparameter	Beschreibung
InitialRandomPassword	wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.
TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo	Der Konfigurationsparameter enthält die Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Geschäftsrolle, Verantwortlicher der Person oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter **TargetSystem | ADS | DefaultAddress** hinterlegte Adresse versandt.
TargetSystem | ADS | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Der Konfigurationsparameter enthält den Namen 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	Der Konfigurationsparameter enthält den Namen 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	Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Person - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | ADS | Accounts | NotRequirePassword	Der Konfigurationsparameter legt fest, ob beim Anlegen eines neuen Benutzerkontos die Option **Kein Kennwort erforderlich** in der Active Directory-Umgebung aktiviert wird.
TargetSystem | ADS | Accounts | Privi-legedAccount	Der Konfigurationsparameter erlaubt die Konfiguration der Einstellungen für privilegierte Active Directory Benutzerkonten.
TargetSystem | ADS | Accounts | PrivilegedAccount | SAMAccountName_ Postfix	Der Konfigurationsparameter enthält das Postfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | ADS |	Der Konfigurationsparameter enthält das Präfix zur Bildung des

Konfigurationsparameter	Beschreibung
Accounts | PrivilegedAccount | SAMAccountName_ Prefix	Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | ADS | Accounts | ProfileFixedString	Der Konfigurationsparameter enthält eine feste Zeichenkette, die an den Standardprofilpfad eines Benutzerprofils angehängt wird.
TargetSystem | ADS | Accounts | TransferJPegPhoto	Der Konfigurationsparameter legt fest, 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	Der Konfigurationsparameter legt fest, ob die Historie einer SID aus dem Zielsystem gelesen werden soll.
TargetSystem | ADS | Accounts | TSProfileFixedString	Der Konfigurationsparameter enthält eine feste Zeichenkette, die an den Standardprofilpfad eines Benutzerprofils auf einem Terminalserver angehängt wird.
TargetSystem | ADS | Accounts | UnlockByCentralPassword	Der Konfigurationsparameter legt fest, ob das Active Directory Benutzerkonto der Person bei der Synchronisation des zentralen Kennworts ebenfalls entsperrt wird.
TargetSystem | ADS | Accounts | UserMustChangePassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten die Option **Kennwort bei der nächsten Anmeldung ändern** gesetzt wird.
TargetSystem | ADS | AuthenticationDomains	Der Konfigurationsparameter enthält eine durch 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 Handbuch zur Autorisierung und Authentifizierung*.
TargetSystem | ADS | AutoCreateDepartment	Der Konfigurationsparameter legt fest, ob beim Synchronisieren oder Ändern von Benutzerkonten automatisch

Konfi-gurationsparameter	Beschreibung
	Abteilungen erzeugt werden.
TargetSystem | ADS | AutoCreateLocality	Der Konfigurationsparameter legt fest, ob beim Synchronisieren oder Ändern von Benutzerkonten automatisch Standorte erzeugt werden.
TargetSystem | ADS | AutoCreateHardwaretype	Der Konfigurationsparameter legt fest, ob für importierte Druckerobjekte automatisch entsprechende Gerätetypen in der Datenbank erzeugt werden.
TargetSystem | ADS | AutoCreateServers	Der Konfigurationsparameter gibt an, ob bei der Synchronisation der Benutzerkonten automatisch Einträge für fehlende Homeserver und Profileserver erstellt werden.
TargetSystem | ADS | AutoCreateServers | PreferredLanguage	Der Konfigurationsparameter enthält die Sprache der automatisch angelegten Server.
TargetSystem | ADS | DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | ADS | HardwareInGroupFromOrg	Der Konfigurationsparameters legt fest, ob Computer aufgrund von Gruppenzuordnung zu Rollen in Gruppen aufgenommen werden.
TargetSystem | ADS | MaxFullsyncDuration	Der Konfigurationsparameter enthält die maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.
TargetSystem | ADS | MembershipAssignCheck	Der Konfigurationsparameter legt fest, 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	Der Konfigurationsparameter enthält die Anzahl von Active Directory Objekten pro Container, bei deren Überschreitung eine Warnmail gesendet werden soll.
TargetSystem | ADS |	Der Konfigurationsparameter enthält die Anzahl von Active

Konfi-gurationsparameter	Beschreibung
MemberShipRestriction | Group	Directory Objekten pro Gruppe, bei deren Überschreitung eine Warnmail gesendet werden soll.
TargetSystem | ADS | MemberShipRestriction | MailNotification	Der Konfigurationsparameter enthält die Standard-Mailadresse zum Versenden von Warnmails.
TargetSystem | ADS | PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | ADS | PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | ADS | PersonAutoFullSync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem | ADS | PersonExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe (|) getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: `ADMINISTRATOR|GUEST|KRBTGT|TSINTERNETUSER|IUSR_.*|IWAM_.*|SUPPORT_.*|.* | $`
TargetSystem | ADS | PersonUpdate	Der Konfigurationsparameter legt fest, 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	Der Konfigurationsparameter dient zur 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	Der Konfigurationsparameter legt fest, 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 Active Directory

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

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

Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 78: Abbildung der Active Directory Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Active Directory	Tabelle im One Identity Manager Schema
builtInDomain	ADSContainer
computer	ADSMachine
contact	ADSContact
container	ADSContainer
domainDNS	ADSDomain
forest (Virtueller Schematyp)	ADSForest
group	ADSGroup
inetOrgPerson	ADSAccount
msDS-PasswordSettings	ADSPolicy
organizationalUnit	ADSContainer
printQueue	ADSPrinter

Schematyp im Active Directory	Tabelle im One Identity Manager Schema
serverInSite	ADSMachineInADSSite
site	ADSSite
trustedDomain	DomainTrustsDomain
user	ADSAccount

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

B

E

F

G

H

I

J

K

L

M

O

P

R

S

Z