One Identity Manager 8.0.3

Administrationshandbuch für die Anbindung einer LDAP-Umgebung

Legende

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

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

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

One Identity Manager Administrationshandbuch für die Anbindung einer LDAP-Umgebung
Aktualisiert - März 2019
Version - 8.0.3

Inhalt

Verwalten einer LDAP-Umgebung

Der One Identity Manager gestattet die Administration der in einem LDAP Verzeichnis verwalteten Objekte, wie beispielsweise Personen, Gruppen, organisatorische Einheiten. Die LDAP-Abbildung innerhalb des One Identity Manager ist als Vorschlag zu sehen und wird in den seltensten Fällen der Abbildung der Eigenschaften in einem kundenspezifischen LDAP Verzeichnis entsprechen. Ob und wie die angebotenen Eigenschaften genutzt werden, ist vom jeweils eingesetzten LDAP Schema abhängig und muss kundenspezifisch konfiguriert werden.

Die Standardauslieferung des One Identity Manager konzentriert sich auf die Verwaltung der Personen mit ihren Benutzerkonten, der Benutzergruppen und der organisatorischen Einheiten eines LDAP Verzeichnisses. Im Datenmodell des One Identity Manager ist die Verwaltung von Computern und Servern eines LDAP Verzeichnisses vorgesehen.

Der One Identity Manager liefert Vorlagen für die Synchronisation mit verschiedenen Serversystemen. Die Anbindung an die Synchronisation muss jedoch in jedem Fall kundenspezifisch vorgenommen werden.

Um im One Identity Manager die Personen eines Unternehmens mit den benötigten Benutzerkonten zu versorgen, können unterschiedliche Mechanismen für die Verbindung der Personen mit ihren Benutzerkonten genutzt werden. Ebenso können die Benutzerkonten getrennt von Personen verwaltet und somit administrative Benutzerkonten eingerichtet werden. Um den Benutzern die benötigten Berechtigungen zur Verfügung zu stellen, werden im One Identity Manager LDAP Gruppen administriert. Im One Identity Manager können Sie weiterhin organisatorische Einheiten in einer hierarchischen Struktur verwalten. Organisatorische Einheiten (Geschäftsstellen oder Abteilungen) werden dazu genutzt, Objekte des LDAP Verzeichnisses wie Benutzerkonten und Gruppen logisch zu organisieren und somit die Verwaltung der Objekte zu erleichtern.

Architekturüberblick

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

- LDAP Server

  LDAP Server, der das LDAP Verzeichnis hält. Dieser Server ist ein ausgewählter produktiver Server mit guter Netzwerkanbindung zum Synchronisationsserver. Der Synchronisationsserver verbindet sich gegen diesen Server, um auf die LDAP Objekte zuzugreifen.

- Synchronisationsserver

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

Der LDAP Konnektor wird für die Synchronisation und Provisionierung der LDAP-Umgebung eingesetzt. Der LDAP Konnektor kommuniziert direkt mit einem LDAP Server.

Abbildung 1: Architektur für die Synchronisation

One Identity Manager Benutzer für die Verwaltung einer LDAP-Umgebung

In die Einrichtung und Verwaltung einer LDAP-Umgebung sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	Die Zielsystemadministratoren müssen der Anwendungsrolle **Zielsysteme | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen. • Legen die Zielsystemverantwortlichen fest. • Richten bei Bedarf weitere Anwendungsrollen für

Benutzer	Aufgaben
	Zielsystemverantwortliche ein. • Legen sich fest, welche Anwendungsrollen für Zielsystemverantwortliche sich widersprechen. • Berechtigen weitere Personen als Zielsystemadministratoren. • Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | LDAP** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.
One Identity Manager Administratoren	• Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne.

Benutzer	Aufgaben
	• Erstellen und konfigurieren bei Bedarf Kennwort-richtlinien.
Administratoren für den IT Shop	Die Administratoren müssen der Anwendungsrolle **Request & Fulfillment | IT Shop | Administratoren** zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Weisen Gruppen an IT Shop-Strukturen zu.
Administratoren für 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 einem LDAP Verzeichnis

Der One Identity Manager unterstützt die Synchronisation mit LDAP Version 3 konformen Verzeichnisservern.

HINWEIS: Abhängig vom Schema können weitere Anpassungen bezüglich des Schemas und der Provisionierungsprozesse erforderlich sein.

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

1. Stellen Sie ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von LDAP-Umgebungen sind verfügbar, wenn der Konfigurationsparameter "TargetSystem\LDAP" 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 einem LDAP Verzeichnis auf Seite 12
- Einrichten des Synchronisationsservers auf Seite 14
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer LDAP Domäne auf Seite 18
- Deaktivieren der Synchronisation auf Seite 41

- Anpassen einer Synchronisationskonfiguration auf Seite 32
- Anhang: Konfigurationsparameter für die Verwaltung einer LDAP-Umgebung auf Seite 132
- Anhang: Standardprojektvorlagen für LDAP auf Seite 136

Benutzer und Berechtigungen für die Synchronisation mit einem LDAP Verzeichnis

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

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzer für den Zugriff auf das LDAP Verzeichnis	Es kann keine sinnvolle Minimalkonfiguration für das Benutzerkonto für die Synchronisation empfohlen werden, da die Berechtigungen vom eingesetzten LDAP Verzeichnisdienst abhängen. Die benötigten Berechtigungen entnehmen Sie daher der Dokumentation zum eingesetzten LDAP Verzeichnisdienst.
Benutzerkonto des One Identity Manager Service	Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen (Rechtevergabe, Verzeichnisse und Dateien anlegen und bearbeiten). Das Benutzerkonto muss der Gruppe "Domänen-Benutzer" (Domain Users) angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht "Anmelden als Dienst" (Log on as a service). Das Benutzerkonto benötigt Rechte für den internen Webservice. HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (NT Authority\NetworkService) laufen, so können Sie die Rechte für den internen Webservice über folgenden Kommandozeilenaufruf vergeben: `netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis. In der Standardinstallation wird der One Identity Manager installiert

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

Besonderheiten für die Synchronisation eines Active Directory Lightweight Directory Services

Bei der Einrichtung eines Synchronisationsprojektes mit einem Active Directory Lightweight Directory Service (AD LDS) sind einige Besonderheiten zu beachten.

AD LDS unterstützt verschiedene Authentifizierungswege. Detaillierte Informationen zur AD LDS Authentifizierung finden Sie in der Microsoft TechNet Library.

Abhängig von der gewählten Authentifizierungsmethode ergeben sich unterschiedliche Einstellungen, die bei der Einrichtung eines Synchronisationsprojektes zu beachten sind.

Authentifizierung mittels AD LDS Sicherheitsprinzipal

Für die Authentifizierungsmethode wird ein Benutzerkonto verwendet, das sich direkt im AD LDS befindet.

- Das Benutzerkonto muss Mitglied in der Gruppe "Administratoren" der AD LDS Instanz sein.
- Das Benutzerkonto muss ein Kennwort besitzen.

  Ist kein Kennwort angegeben, erfolgt einen anonyme Authentifizierung. Dies führt dazu, dass das Schema nicht gelesen werden kann und die Einrichtung des Synchronisationsprojektes fehlschlägt.

Für die Einrichtung des Synchronisationsprojektes beachten Sie Folgendes.

- Die Authentifizierung muss mit SSL Verschlüsselung erfolgen.
- Als Authentifizierungsmethode muss "Basic" verwendet werden.
- Der Benutzername des Benutzerkontos für die Anmeldung am AD LDS ist mit dem definierten LDAP Namen (DN) anzugeben.

  Syntaxbeispiel: `CN=Administrator,OU=Users,DC=Doku,DC=Testlab,DC=dd`

Authentifizierung mit Windows Sicherheitsprinzipal

Für die Authentifizierung wird ein Benutzerkonto verwendet, das sich auf einem lokalen Computer oder in einer Active Directory Domäne befindet.

- Das Benutzerkonto muss Mitglied in der Gruppe "Administratoren" der AD LDS Instanz sein.

Für die Einrichtung des Synchronisationsprojektes beachten Sie Folgendes.

- Als Authentifizierungsmethode muss "Negotiate" verwendet werden.
- Erfolgt die Authentifizierung ohne SSL Verschlüsselung, müssen die Nachrichtenvertraulichkeit (Sealing) und die Nachrichtenintegrität (Signing) aktiviert sein.
- Erfolgt die Authentifizierung mit SSL Verschlüsselung, sollten die Nachrichtenvertraulichkeit (Sealing) und die Nachrichtenintegrität (Signing) deaktiviert sein.
- Der Benutzername des Benutzerkonto für die Anmeldung am AD LDS ist mit dem Benutzerprinzipalnamen (User Prinicpal Name) anzugeben.

  Syntaxbeispiel: `Administrator@Doku.Testlab.dd`

Authentifizierung mittels AD LDS Proxyobjekt

Für die Authentifizierung wird ein Benutzerkonto verwendet, das im AD LDS vorhanden ist und als Bindungsumleitung für ein lokales Benutzerkonto oder ein Benutzerkonto in einer Active Directory Domäne dient. Das lokale Benutzerkonto oder das Active Directory Benutzerkonto ist im AD LDS Proxyobjekt als Sicherheits-ID (SID) referenziert.

- Das Benutzerkonto (AD LDS Proxyobjekt) muss Mitglied in der Gruppe "Administratoren" der AD LDS Instanz sein.

Für die Einrichtung des Synchronisationsprojektes beachten Sie Folgendes.

- Die Authentifizierung muss mit SSL Verschlüsselung erfolgen.
- Als Authentifizierungsmethode muss "Basic" verwendet werden.
- Für die Anmeldung am AD LDS ist der Benutzername des AD LDS Proxyobjektes zu verwenden.
- Der Benutzername ist mit dem definierten LDAP Namen (DN) anzugeben.

  Syntaxbeispiel: `CN=Administrator,OU=Users,DC=Doku,DC=Testlab,DC=dd`
- Als Kennwort für die Anmeldung ist das Kennwort des Benutzerkontos anzugeben, auf welches das AD LDS Proxyobjekt verweist.

Einrichten des Synchronisationsservers

Für die Einrichtung der Synchronisation mit einer LDAP-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 (nicht-Itanium 64 bit) ab Service Pack 2
  - Windows Server 2008 R2 (nicht-Itanium 64 bit) ab Service Pack 1
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
- Microsoft .NET Framework Version 4.5.2 oder höher

  HINWEIS: Microsoft .NET Framework Version 4.6.0 wird nicht unterstützt.

  HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.
- Windows Installer
- One Identity Manager Service, LDAP 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 | LDAP directories**.

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 die folgenden Schritte aus.

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

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

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

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

      - ODER -

      Um einen neuen Jobserver zur erstellen, klicken Sie **Hinzufügen**.
   b. Bearbeiten Sie folgende Informationen für den Jobserver.

      Tabelle 3: Eigenschaften eines Jobservers

Eigenschaft	Beschreibung
Server	Bezeichnung des Jobservers.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Beispiel: `<Name des Servers>.<Vollqualifizierter Domänenname>`

      HINWEIS: Über die Option **Erweitert** können Sie weitere Eigenschaften für den Jobserver bearbeiten. Sie können die Eigenschaften auch zu einem späteren Zeitpunkt mit dem Designer bearbeiten.
4. Auf der Seite **Maschinenrollen** legen Sie fest, welche Rolle der Jobserver im One Identity Manager übernimmt. Abhängig von der gewählten Maschinenrolle werden die Installationspakete ermittelt, die auf dem Jobserver installiert werden.

   Wählen Sie mindestens folgende Rollen:

   - LDAP directories

5. Auf der Seite **Serverfunktionen** legen Sie die Funktion des Servers in der One Identity Manager-Umgebung fest. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

   Die Serverfunktionen sind abhängig von den gewählten Maschinenrollen bereits ausgewählt. Sie können die Serverfunktionen hier weiter einschränken.

   Wählen Sie mindestens folgende Serverfunktionen:

   - LDAP Konnektor

6. Auf der Seite **Dienstkonfiguration** prüfen Sie die Konfiguration des One Identity Manager Service.

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

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

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

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

Tabelle 4: Installationsinformationen

Eingabe	Beschreibung
Computer	Server, auf dem der Dienst installiert und gestartet wird. ***Um einen Server auszuwählen*** • Erfassen Sie den Servernamen. -ODER- • Wählen Sie einen Eintrag in der Liste.
Dienstkonto	Angaben zum Benutzerkonto des One Identity Manager Service. ***Um ein Benutzerkonto für den One Identity Manager Service zu erfassen*** • Aktivieren Sie die Option **Lokales Systemkonto**.

Eingabe	Beschreibung
	Damit wird der One Identity Manager Service unter dem Konto "NT AUTHORITY\SYSTEM" gestartet. - ODER- • Erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung.
Installationskonto	Angaben zum administrativen Benutzerkonto für die Installation des Dienstes. ***Um ein administratives Benutzerkonto für die Installation zu erfassen*** • Aktivieren Sie die Option **Erweitert**. • Aktivieren Sie die Option **Angemeldeter Benutzer**. Es wird das Benutzerkonto des aktuell angemeldeten Benutzers verwendet. - ODER- • Geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.

12. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

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

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

    HINWEIS: Der Dienst wird mit der Bezeichnung "One Identity Manager Service" in der Dienstverwaltung des Servers eingetragen.

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer LDAP Domäne

Verwenden Sie den Synchronization Editor, um die Synchronisation zwischen One Identity Manager-Datenbank und LDAP-Umgebung einzurichten. Nachfolgend sind die Schritte für die initiale Einrichtung eines Synchronisationsprojektes beschrieben.

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

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

Tabelle 5: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
DNS Name des LDAP Servers	Vollständiger Name des LDAP Servers, gegen den sich der Synchronisationsserver verbindet, um auf die LDAP Objekte zuzugreifen. Beispiel: `Server.Doku.Testlab.dd`
Authentifizierungsart	Eine Verbindung zum Zielsystem kann nur hergestellt werden, wenn die richtige Authentifizierungsart gewählt wird. Als Standard wird die Authentifizierungsart „Basic" verwendet. Weitere Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library.
Kommunikationsport auf dem Domänen-Controller	LDAP Standard-Kommunikationsport ist Port 389.
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 ausreichend Berechtigungen bereit. Weitere Informationen finden Sie unter Benutzer und Berechtigungen für die Synchronisation mit einem LDAP Verzeichnis auf Seite 12.
Synchronisationsserver für das LDAP	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 LDAP Konnektor installiert sein. Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobservers die folgenden Eigenschaften. **Tabelle 6: Zusätzliche Eigenschaften für den Jobserver** **Eigenschaft** / **Wert** Serverfunktion / LDAP Konnektor Maschinenrolle / Server/Jobserver/LDAP directories

Angaben	Erläuterungen
	Weitere Informationen finden Sie unter Einrichten des Synchronisationsservers auf Seite 14.
Verbindungsdaten zur One Identity Manager Datenbank	SQL Server: • Datenbankserver • Datenbank • Datenbankbenutzer und Kennwort • Angabe, ob integrierte Windows Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows Authentifizierung unterstützt. Oracle: • Angabe, ob der Zugriff direkt oder über Oracle Client erfolgt Die erforderlichen Verbindungsdaten sind abhängig von der Einstellung dieser Option. • Datenbankserver • Port der Oracle Instanz • Service Name • Oracle Datenbankbenutzer und Kennwort • Datenquelle (TNS Alias Name aus der `TNSNames.ora`)
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

Angaben	Erläuterungen
	• RemoteConnectPlugin ist installiert • LDAP Konnektor ist installiert Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software) 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 LDAP Domäne einzurichten

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

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

2. Wählen Sie den Eintrag **Zielsystemtyp LDAP**. Klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors wird gestartet.

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

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

4. Auf der Startseite des Assistenten legen Sie über die Option **Erweiterte Einstellungen konfigurieren (Expertenmodus)** die Einstellungen für den Assistenten fest.
   - Wenn Sie eine Standardprojektvorlage verwenden, lassen Sie die Option deaktiviert. Die Standardvorlagen ermitteln die zu verwendenden Einstellungen automatisch.
   - Für kundenspezifische angepasste LDAP Umgebungen, aktivieren Sie die Option. Für diesen Fall können Sie folgende Einstellungen zusätzlich vornehmen:
     - Definition virtueller Klassen für nicht RFC konforme Abbildungen von Objekten
     - Definition von Hilfsklassen von Typ "Auxiliary"
     - Definition von Systemattributen zur Objektidentifikation, Revisionsattributen und zusätzlichen funktionalen Attributen
     - Definition weiterer Attribute für die Unterstützung dynamischer Gruppen
5. Auf der Seite **Netzwerk** erfassen Sie die Netzwerkeinstellungen für die Verbindung zum LDAP Server.
   - Im Bereich **Host** erfassen Sie die Verbindungsdaten zum LDAP Server.

     Tabelle 7: Verbindungsdaten zum LDAP Server

Eigenschaft	Beschreibung
Server	Vollständiger Name des LDAP Servers, gegen den sich der Synchronisationsserver verbindet, um auf die LDAP Objekte zuzugreifen. Beispiel: `Server.Doku.Testlab.dd`
Port	Kommunikationsport auf dem Server. LDAP Standard-Kommunikationsport ist Port 389.

   - Klicken Sie **Verbindung testen**. Es wird versucht eine Verbindung zum Server aufzubauen.
   - Im Bereich **Zusätzliche Einstellungen** erfassen Sie zusätzliche Einstellungen zur Kommunikation mit dem LDAP Server.

Tabelle 8: Zusätzliche Einstellungen zur Verbindung

Eigenschaft	Beschreibung
Protokollversion	Version des LDAP Protokolls.
Keine Verschlüsselung	Angabe, dass keine Verschlüsselung verwendet wird
SSL/TLS Verschlüsselung	Angabe, ob eine SSL/TLS verschlüsselte Verbindung erfolgt.
Verwende StartTLS	Angabe, ob StartTLS verwendet wird.

6. Auf der Seite **Authentifizierung** erfassen Sie Informationen zur Authentifizierung.
   - Im Bereich **Authentifizierungsmethode** wählen Sie die Authentifizierungsart für die Anmeldung am Zielsystem.
   - Abhängig von der gewählten Authentifizierungsmethode können weitere Informationen erforderlich sein. Diese Informationen erfassen Sie im Bereich **Anmeldeinformationen**.

     Tabelle 9: Anmeldeinformationen

Eigenschaft	Beschreibung
Benutzername	Name des Benutzerkontos zur Anmeldung am LDAP.
Kennwort	Kennwort zum Benutzerkonto.
Sealing aktivieren	Angabe, ob Sealing aktiviert ist. Aktivieren Sie die Option, wenn die gewählte Authentifizierungsmethode die Nachrichtenvertraulichkeit (Sealing) unterstützt.
Signing aktivieren	Angabe, ob Signing aktiviert ist. Aktivieren Sie die Option, wenn die gewählte Authentifizierungsmethode die Nachrichtenintegrität (Signing) unterstützt.

   - Im Bereich **LDAP-Verbindung prüfen** können Sie die erfassten Verbindungsdaten überprüfen. Klicken Sie **Verbindung testen**. Es wird versucht eine Anmeldung am Server durchzuführen.
7. Auf der Seite **LDAP Serverinformationen** werden die Informationen zum LDAP Schema angezeigt.
8. Auf der Seite **Virtuelle Klassen** definieren Sie zusätzliche virtuelle Klassen.

   HINWEIS: Dieser Schritt wird nur angezeigt, wenn Sie die Option **Erweiterte Einstellungen konfigurieren (Expertenmodus)** für den Systemverbindungsassistenten aktiviert haben.

Objekte, die aus mehreren strukturelle Klassen bestehen, können nur in LDAP Systemen erstellt werden, die nicht RFC-konform sind. Sie bestehen aus zwei oder mehr unterschiedlichen Klassen, die nicht voneinander abgeleitet sind, beispielsweise "OrganisationalUnit" und "inetOrgPerson".

Um diese Objekte abzubilden

- Erfassen Sie im Bereich **Konfigurierte virtuelle Klassen** die Bezeichnung der virtuellen Klasse.
- Wählen Sie im Bereich **Strukturelle Klassen wählen** die strukturelle Klassen, die auf die virtuelle Klasse abgebildet werden.

9. Auf der Seite **Suchoptionen** legen Sie Parameter für die Suche nach den zu ladenden LDAP Objekten fest.

Tabelle 10: Suchoptionen

Eigenschaft	Beschreibung
DN des Root-Eintrags	Root-Eintrag (in der Regel die Domäne) für die Synchronisation.
LDAP Schema im lokalen Cache speichern	Angabe, ob das LDAP Schema lokal im Cache gehalten werden soll. Dadurch kann die Synchronisation und Provisionierung von LDAP Objekten beschleunigt werden. Der Cache befindet sich auf dem Computer mit dem die Verbindung hergestellt wird unter `%Appdata%\...\Local\One Identity\One Identity Manager\Cache\GenericLdapConnector\<ConnectionInternalKey>\<Hash>\<Hash>.Cache`
Anfrage Timeout (Sekunden)	Timeout für Anfragen in Sekunden.
Seitenweise Suche verwenden	Angabe, ob die LDAP Objekte seitenweise geladen werden sollen. Wenn Sie die Option aktivieren, erfassen Sie die Seitengröße.
Seitengröße	Anzahl der maximal zu ladenden Objekte pro Seite.

10. Auf der Seite **Einstellungen für schreibende Optionen** geben Sie an, welche Art von Schreiboperationen der LDAP Server unterstützt.
    - Aktivieren Sie die Option **Server unterstützt Umbenennung von Einträgen**, wenn der LDAP Server die Umbenennung von Einträgen unterstützt.

- Aktivieren Sie die Option **Server unterstützt Verschiebung von Einträgen**, wenn der LDAP Server das Verschieben von Einträgen unterstützt.

  HINWEIS: Einige Server unterstützen das Umbenennen von Einträgen nur auf Blattebene. In diesem Fall scheitert die Umbenennung von anderen Knoten mit einer Fehlermeldung.

11. Auf der Seite **Hilfsklassen zuordnen** weisen Sie strukturellen Klassen zusätzliche Hilfsklassen zu.

    HINWEIS: Dieser Schritt wird nur angezeigt, wenn Sie die Option **Erweiterte Einstellungen konfigurieren (Expertenmodus)** für den Systemverbindungsassistenten aktiviert haben.

    Hilfsklassen sind Klassen vom Typ "Auxiliary" und enthalten Attribute, die die strukturelle Klasse erweitern. Die Attribute der Hilfsklassen werden wie optionale Attribute der strukturellen Klassen im Schema angeboten.

    HINWEIS: Um die Attribute der Hilfsklassen im One Identity Manager abzubilden, sind unter Umständen kundenspezifische Erweiterungen des One Identity Manager Schemas erforderlich. Verwenden Sie dazu das Programm Schema Extension.

12. Auf der Seite **Systemattribute** legen Sie fest, welches Attribut des LDAP Systems verwendet werden soll, um die Objekte eindeutig zu identifizieren.

    HINWEIS: Dieser Schritt wird nur angezeigt, wenn Sie die Option **Erweiterte Einstellungen konfigurieren (Expertenmodus)** für den Systemverbindungsassistenten aktiviert haben.

    - Im Bereich **Attribut für die Objektidentifikation** wählen Sie das Attribut, mit dem Objekte eindeutig im LDAP zu identifizieren sind. Das Attribut muss eindeutig sein und an allen Objekten im LDAP vorhanden sein.
    - Im Bereich **Revisionsattribute** legen Sie fest, welche Attribute für Revisionsfilterung genutzt werden.
    - Im Bereich **Zusätzliche funktionale Attribute** legen Sie fest, welche Attribute zusätzlich für die LDAP Objekte ermittelt werden sollen. Funktionale Attribute werden für die Verzeichnisverwaltung verwendet. Die Attribute werden nur ermittelt, wenn sie explizit angegeben sind.

      HINWEIS: Um die funktionalen Attribute im One Identity Manager abzubilden, sind unter Umständen kundenspezifische Erweiterungen des One Identity Manager Schemas erforderlich. Verwenden Sie dazu das Programm Schema Extension.

13. Wenn der LDAP Server dynamische Gruppen unterstützt, markieren Sie auf der Seite **Auswahl von Eigenschaften dynamischer Gruppen**, die Attribute, welche die URL mit Suchinformationen enthalten, um die Mitglieder von dynamischen Gruppen zu bestimmen, beispielsweise `memberURL`.

HINWEIS: Dieser Schritt wird nur angezeigt, wenn Sie die Option **Erweiterte Einstellungen konfigurieren (Expertenmodus)** für den Systemverbindungsassistenten aktiviert haben.

14. Auf der Seite **Kennworteinstellungen für Einträge** legen Sie zusätzliche Kennworteinstellungen für Benutzerkonten fest.
    - Erfassen Sie folgende Einstellungen.

Tabelle 11: Kennworteinstellungen

Eigenschaft	Beschreibung
Kennwortattribut	Attribut, welches das Kennwort eines Benutzerkontos repräsentiert, beispielsweise `userPassword`.
Kennwortänderungsmethode	Methode, die verwendet wird, um Kennwörter zu ändern.

Wert	Beschreibung
Default	Standardmethode zum Ändern der Kennwörter. Das Kennwort wird direkt auf das Kennwortattribut geschrieben.
ADLDS	Kennwortänderungsmethode die für Systeme verwendet wird, die auf MicrosoftActive Directory Lightweight Directory Services (AD LDS) basieren.

15. 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.

16. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
17. Auf der Seite **Projektvorlage auswählen** wählen Sie eine Projektvorlage, mit der die Synchronisationskonfiguration erstellt werden soll.

Tabelle 12: Standardprojektvorlagen

Projektvorlage	Beschreibung
OpenDJ Synchronisation	Diese Projektvorlage basiert auf OpenDJ. Verwenden Sie diese Projektvorlage für die initiale Einrichtung des Synchronisationsprojektes. Für kundenspezifische Implementierungen können Sie das Synchronisationsprojekt mit dem Synchronization Editor erweitern.
AD LDS Synchronisation	Diese Projektvorlage basiert auf Active Directory Lightweight Directory Services (AD LDS).

HINWEIS: Eine Standardprojektvorlage sorgt dafür, dass alle benötigten Informationen im One Identity Manager angelegt werden. Dazu gehören beispielsweise die Mappings, Workflows und das Basisobjekt der Synchronisation. Wenn Sie keine Standardprojektvorlage verwenden, müssen Sie das Basisobjekt der Synchronisation selbst im One Identity Manager bekannt geben. Verwenden Sie eine Standardprojektvorlage für die initiale Einrichtung des Synchronisationsprojektes. Für kundenspezifische Implementierungen können Sie das Synchronisationsprojekt mit dem Synchronization Editor erweitern.

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

Tabelle 13: 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:

Option	Bedeutung
	• Die Synchronisationsrichtung ist "In das Zielsystem". • In den Synchronisationsschritten sind die Verarbeitungsmethoden nur für die Synchronisationsrichtung "In das Zielsystem" definiert. • Synchronisationsschritte werden nur für solche Schemaklassen erstellt, deren Schematypen schreibbar sind.

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

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

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

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

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

20. Auf der Seite **Allgemein** erfassen Sie die allgemeinen Einstellungen für das Synchronisationsprojekt.

    HINWEIS: Dieser Schritt wird nur angezeigt, wenn die gewählte Projektvorlage mehrere Skriptsprachen unterstützt.

Tabelle 14: Allgemeine Eigenschaften des Synchronisationsprojekts

Eigenschaft	Beschreibung
Anzeigename	Anzeigename für das Synchronisationsprojekt.
Skriptsprache	Sprache, in der Skripte in diesem Synchronisationsprojekt geschrieben werden. Skripte werden an verschiedenen Stellen in der Synchronisationskonfiguration eingesetzt. Wenn Sie ein leeres Projekt erstellen, legen Sie die Skriptsprache fest. WICHTIG: Die Skriptsprache kann nach dem Speichern des Synchronisationsprojekts nicht mehr geändert werden!

Eigenschaft	Beschreibung
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.

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

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

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

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

   HINWEIS: Einige Inhalte erzeugen besonders viele Protokolldaten!

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

Um regelmäßige Synchronisationen auszuführen

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

Um die initiale Synchronisation manuell zu starten

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

HINWEIS: Im Anschluss an eine Synchronisation werden in der Standardinstallation automatisch für die Benutzerkonten Personen erzeugt. Ist zum Zeitpunkt der Synchronisation noch keine Kontendefinition für 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

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

Detaillierte Informationen zum Thema

- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Verwandte Themen

- Einrichten des Synchronisationsservers auf Seite 14
- Benutzer und Berechtigungen für die Synchronisation mit einem LDAP Verzeichnis auf Seite 12
- Synchronisationsergebnisse anzeigen auf Seite 31
- Anpassen einer Synchronisationskonfiguration auf Seite 32
- Beschleunigung der Synchronisation durch Revisionsfilterung auf Seite 36
- OpenDJ Basisvorlage auf Seite 136
- Standardprojektvorlage für Active Directory Lightweight Directory Services auf Seite 137
- Einrichten von Kontendefinitionen auf Seite 43
- Automatische Zuordnung von Personen zu LDAP Benutzerkonten auf Seite 98

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.

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 LDAP Domäne eingerichtet. Mit diesem Synchronisationsprojekt können Sie LDAP Objekte in die One Identity Manager-Datenbank einlesen. Wenn Sie Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in die LDAP-Umgebung provisioniert.

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

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

- Wenn eine weitere Synchronisation mit derselben Startkonfiguration gestartet wird, wird dieser Prozess gestoppt und erhält den Ausführungsstatus "Frozen". Es wird eine Fehlermeldung in die Protokolldatei des One Identity Manager Service geschrieben.
- Wenn eine weitere Synchronisation mit einer anderen Startkonfiguration gestartet wird, die dasselbe Zielsystem anspricht, kann das zu Synchronisationsfehlern oder Datenverlust führen. Legen Sie an den Startkonfigurationen fest, wie sich der One Identity Manager in diesem Fall verhalten soll. 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 LDAP Domäne konfigurieren auf Seite 33
- Synchronisation verschiedener LDAP Domänen konfigurieren auf Seite 34
- Schema aktualisieren auf Seite 34

Synchronisation in die LDAP 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 LDAP 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 LDAP Domänen konfigurieren auf Seite 34

Synchronisation verschiedener LDAP 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 LDAP 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 LDAP Domäne konfigurieren auf Seite 33

Schema aktualisieren

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

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

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

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

Um das Schema einer Systemverbindung zu aktualisieren

1. 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.

LDAP unterstützt die Revisionsfilterung. Als Revisionszähler werden die Revisionsattribute genutzt, die bei der Einrichtung des Synchronisationsprojektes definiert wurden. In der Standardinstallation werden das Erstellungsdatum und Datum der letzten Änderung der LDAP Objekte genutzt. Jede Synchronisation speichert ihr letztes Ausführungsdatum in der One Identity Manager-Datenbank. (Tabelle `DPRRevisionStore`, Spalte `Value`). Dieser Wert wird als Vergleichswert für die Revisionsfilterung bei der nächsten Synchronisation mit dem selben Workflow genutzt. Beim nächsten Synchronisationslauf werden nur noch jene Objekte gelesen, die sich seit diesem Datum verändert haben. Anhand des Vergleichs werden unnötige Aktualisierungen von Objekten, die sich seit dem letzten Synchronisationslauf nicht verändert haben, vermieden.

Die Revisionsbestimmung erfolgt zu Beginn einer Synchronisation. Objekte, die nach diesem Zeitpunkt geändert werden, werden erst mit der nächsten Synchronisation erfasst.

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

Um die Revisionsfilterung an einem Workflow zuzulassen

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

Um die Revisionsfilterung an einer Startkonfiguration zuzulassen

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

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.

Objekte, die als ausstehend gekennzeichnet wurden,

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

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie die Kategorie **LDAP | Zielsystemabgleich: LDAP**.

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp LDAP als Synchronisationstabellen zugewiesen sind.
2. Wählen Sie in der Navigationsansicht die Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

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

   TIPP:

   Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

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

   b. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.
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 15: 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.

Symbol	Methode	Beschreibung
	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 die Kategorie **LDAP | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp LDAP.
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 LDAP `GroupOfNames`).
- 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. Starten Sie den Manager.
2. Wählen Sie die Kategorie **LDAP | Basisdaten zur Konfiguration | Zielsystemtypen**.
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 `LDAPAccountInLDAPGroup`, `LDAPGroupInLDAPGroup` und `LDAPMachineInLDAPGroup`).

5. Klicken Sie **Änderungen zusammenführen**.
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.

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

Unterstützung bei der Analyse von Synchronisationsproblemen

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

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

Um den Synchronisationsanalysebericht zu erstellen

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

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

Deaktivieren der Synchronisation

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

Um regelmäßige Synchronisationen zu verhindern

- Wählen Sie die Startkonfiguration und deaktivieren Sie den hinterlegten Zeitplan.

  Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das geladene Synchronisationsprojekt zu deaktivieren

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

Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer LDAP Domäne auf Seite 18

3

Basisdaten zur Konfiguration

Für die Verwaltung einer LDAP-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 Anhang: Konfigurationsparameter für die Verwaltung einer LDAP-Umgebung auf Seite 132.

- Kontendefinitionen

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

  Weitere Informationen finden Sie unter Einrichten von Kontendefinitionen auf Seite 43.

- Kennwortrichtlinien

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

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

Weitere Informationen finden Sie unter Kennwortrichtlinien auf Seite 62.

- 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 LDAP Benutzerkonten auf Seite 71.

- 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 73.

- 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 37.

- 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 75.

Einrichten von Kontendefinitionen

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

Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

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

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

Für die 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 die Kategorie **LDAP | 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 44

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 16: 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 LDAP 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.
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.

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

Erstellen der Automatisierungsgrade

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

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

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

- Unmanaged

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

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

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

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

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

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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

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

   - ODER -

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

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

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie die Kategorie **LDAP | 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 48

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 17: 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:

Eigenschaft	Beschreibung	
	Niemals	Die Daten werden nicht aktualisiert.
	Immer	Die Daten werden immer aktualisiert
	Nur initial	Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung beibehalten	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.	
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.	
Gruppen bei dauerhafter Deaktivierung beibehalten	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.	
Benutzerkonten bei dauerhafter Deaktivierung sperren	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.	
Gruppen bei verzögertem Löschen beibehalten	Angabe, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen.	
Benutzerkonten bei verzögertem Löschen sperren	Angabe, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.	
Gruppen bei Sicherheitsgefährdung beibehalten	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.	
Benutzerkonten bei Sicherheitsgefährdung sperren	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.	
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Angabe, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.	

Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

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

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.

- LDAP Container
- Gruppen erbbar
- Identität
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

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

Tabelle 18: Abbildungsvorschrift für IT Betriebsdaten

Eigenschaft	Beschreibung
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.
Quelle	Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen: • Primäre Abteilung • Primärer Standort • Primäre Kostenstelle • Primäre Geschäftsrolle HINWEIS: Verwenden Sie die primäre Geschäftsrolle nur, wenn das Geschäftsrollenmodul vorhanden ist. • keine Angabe Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option **Immer Standardwert verwenden** setzen.
Standardwert	Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
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.

Eigenschaft	Beschreibung
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\LDAP\Accounts\MailTemplateDefaultValues" an.

4. Speichern Sie die Änderungen.

Verwandte Themen

- Erfassen der IT Betriebsdaten auf Seite 51

Erfassen der IT Betriebsdaten

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

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

Beispiel:

In der Regel erhält jede Person der Abteilung A ein Standardbenutzerkonto 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 in der Kategorie **Organisationen** bzw. **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten** und erfassen Sie folgende Daten.

Tabelle 19: IT Betriebsdaten

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

3. Speichern Sie die Änderungen.

Verwandte Themen

- Erstellen einer Abbildungsvorschrift für IT Betriebsdaten auf Seite 49

Ändern der IT Betriebsdaten

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

Voraussetzungen

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

  - ODER -

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

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

Um die Bildungsregeln auszuführen

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

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

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

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinition an Personen

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

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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

Detaillierte Informationen zum Thema

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 55
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 55
- Kontendefinition an alle Personen zuweisen auf Seite 56
- Kontendefinition direkt an Personen zuweisen auf Seite 57
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 59

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

   - ODER -

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

Verwandte Themen

- Kontendefinition an Geschäftsrollen zuweisen auf Seite 55
- Kontendefinition an alle Personen zuweisen auf Seite 56
- Kontendefinition direkt an Personen zuweisen auf Seite 57

Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

   - ODER -

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 55
- Kontendefinition an alle Personen zuweisen auf Seite 56
- Kontendefinition direkt an Personen zuweisen auf Seite 57

Kontendefinition an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

1. Wählen Sie die Kategorie **LDAP | 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 55
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 55
- Kontendefinition direkt an Personen zuweisen auf Seite 57

Kontendefinition direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

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

   - ODER -

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

Verwandte Themen

- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 55
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 55
- Kontendefinition an alle Personen zuweisen auf Seite 56

Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

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

   - ODER -

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

Kontendefinition in den IT Shop aufnehmen

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

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

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

Um eine Kontendefinition in den IT Shop aufzunehmen

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

   - ODER -

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

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen

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

   - ODER -

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

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

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

   - ODER -

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

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

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

Verwandte Themen

- Stammdaten einer Kontendefinition auf Seite 44
- Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 55
- Kontendefinition an Geschäftsrollen zuweisen auf Seite 55
- Kontendefinition direkt an Personen zuweisen auf Seite 57
- Kontendefinition an Systemrollen zuweisen auf Seite 57

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 in der Kategorie **LDAP | Domänen** die Domäne.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Automatische Zuordnung von Personen zu LDAP Benutzerkonten auf Seite 98

Löschen einer Kontendefinition

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

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

Um eine Kontendefinition zu löschen

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

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

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

e. Speichern Sie die Änderungen.

4. Entfernen Sie die Zuordnung der Kontendefinition zu Geschäftsrollen.

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

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

d. Speichern Sie die Änderungen.

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

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

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

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

e. Speichern Sie die Änderungen.

7. Entfernen Sie die Zuordnung der Kontendefinition zum Zielsystem.

a. Wählen Sie in der Kategorie **LDAP | 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 die Kategorie **LDAP | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Klicken Sie , um die Kontendefinition zu löschen.

Kennwortrichtlinien

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

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

Detaillierte Informationen zum Thema

- Vordefinierte Kennwortrichtlinien auf Seite 62
- Bearbeiten von Kennwortrichtlinien auf Seite 63
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 66
- Ausschlussliste für Kennwörter auf Seite 69
- Prüfen eines Kennwortes auf Seite 69
- Generieren eines Kennwortes testen auf Seite 70
- Zuweisen einer Kennwortrichtlinie auf Seite 70

Vordefinierte Kennwortrichtlinien

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

Kennwortrichtlinie für die Anmeldung am One Identity Manager

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

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

Bei entsprechender Konfiguration wird das zentrale Kennwort einer Person auf die Kennwörter der zielsystemspezifischen Benutzerkonten abgebildet. Die Kennwortrichtlinie "Kennwortrichtlinie für zentrales Kennwort von Personen" definiert die Einstellung für das zentrale Kennwort (`Person.CentralPassword`).

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

Kennwortrichtlinien für Zielsysteme

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

HINWEIS: Bei der Aktualisierung von One Identity Manager Version 7.x auf One Identity Manager Version 8.0.3 werden die Einstellung der Konfigurationsparameter zur Bildung von Kennwörtern auf die zielsystemspezifischen Kennwortrichtlinien umgesetzt.

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

Für LDAP ist die Kennwortrichtlinie "LDAP Kennwortrichtlinie" vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der LDAP Benutzerkonten (`LDAPAccount.UserPassword`) einer LDAP Domäne oder eines LDAP Containers anwenden.

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

Bearbeiten von Kennwortrichtlinien

Um eine Kennwortrichtlinie zu bearbeiten

1. Wählen Sie im Manager die Kategorie **LDAP | 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 64
- Richtlinieneinstellungen auf Seite 64
- Zeichenklassen für Kennwörter auf Seite 65
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 66

Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 20: Stammdaten einer Kennwortrichtlinie

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

Richtlinieneinstellungen

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

Tabelle 21: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wird beim Anlegen im Benutzerkonto selbst kein Kennwort

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

Zeichenklassen für Kennwörter

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

Tabelle 22: 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.

Eigenschaft	Bedeutung
Min. Anzahl Großbuchstaben	Angabe, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Ziffern	Angabe, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Angabe, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.
Zulässige Sonderzeichen	Liste zulässiger Sonderzeichen.
Unzulässige Sonderzeichen	Liste unzulässiger Sonderzeichen.
Max. identische Zeichen insgesamt	Maximale Anzahl identischer Zeichen, die insgesamt im Kennwort vorkommen dürfen.
Max. identische Zeichen aufeinanderfolgend	Maximale Anzahl identischer Zeichen, die nacheinander wiederholt werden können.

Kundenspezifische Skripte für Kennwortanforderungen

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

Detaillierte Informationen zum Thema

- Skript zum Prüfen eines Kennwortes auf Seite 66
- Skript zum Generieren eines Kennwortes auf Seite 68

Skript zum Prüfen eines Kennwortes

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

Syntax für Prüfskripte

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

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Kennwort, das zu prüfen ist

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

Beispiel für ein Skript zum Prüfen eines Kennwortes

Ein Kennwort in darf nicht mit "?" oder "!" beginnen. Das Skript prüft ein gegebenes Kennwort auf Zulässigkeit.

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

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **LDAP | 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 68

Skript zum Generieren eines Kennwortes

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

Syntax für Generierungsskripte

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

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Generiertes Kennwort

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

Beispiel für ein Skript zum Generieren eines Kennwortes

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

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

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **LDAP | 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 66

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 **LDAP | 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 **LDAP | 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.

Zuweisen einer Kennwortrichtlinie

Für LDAP ist die Kennwortrichtlinie "LDAP Kennwortrichtlinie" vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der LDAP Benutzerkonten (`LDAPAccount.UserPassword`) einer LDAP Domäne oder eines LDAP Containers anwenden.

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

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

Um eine Kennwortrichtlinie neu zuzuweisen

1. Wählen Sie im Manager die Kategorie **LDAP | 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 23: Zuweisen einer Kennwortrichtlinie

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

5. Speichern Sie die Änderungen.

Um die Zuweisung einer Kennwortrichtlinie zu ändern

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

Initiales Kennwort für neue LDAP Benutzerkonten

Tabelle 24: Konfigurationsparameter für die Bildung eines initialen Kennwortes für Benutzerkonten

Konfigurationsparameter	Bedeutung
QER\Person\UseCentralPassword	Der Konfigurationsparameter legt

Konfigurationsparameter	Bedeutung
	fest, ob das zentrale Kennwort einer Person in den Benutzerkonten verwendet werden soll. Das zentrale Kennwort der Person wird automatisch auf die Benutzerkonten der Person in allen erlaubten Zielsystemen abgebildet. Ausgenommen sind privilegierte Benutzerkonten; diese werden nicht aktualisiert.
QER\Person\UseCentralPassword\PermanentStore	Der Konfigurationsparameter steuert die Aufbewahrungszeit der zentralen Kennworte. Ist der Parameter aktiviert, wird das zentrale Kennwort der Person dauerhaft gespeichert. Ist der Parameter nicht aktiviert, wird das zentrale Kennwort nur zum Publizieren an bestehende zielsystemspezifische Benutzerkonten benutzt und anschließend in der One Identity Manager-Datenbank gelöscht.
TargetSystem\LDAP\Accounts\ InitialRandomPassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.

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

- Verwenden Sie das zentrale Kennwort der Person. Das zentrale Kennwort der zugeordneten Person wird auf das Kennwort des Benutzerkontos abgebildet.
  - Aktivieren Sie im Designer den Konfigurationsparameter "QER\Person\UseCentralPassword".

    Ist der Konfigurationsparameter "QER\Person\UseCentralPassword" aktiviert, wird das zentrale Kennwort der Person automatisch auf die Benutzerkonten einer Person in den einzelnen Zielsystemen abgebildet. Ausgenommen sind privilegierte Benutzerkonten; diese werden nicht aktualisiert.
  - Aktivieren Sie im Designer den Konfigurationsparameter "QER\Person\UseCentralPassword\PermanentStore" und legen Sie fest, ob das

zentrale Kennwort der Personen dauerhaft oder nur bis zum Publizieren in die Zielsysteme in der One Identity Manager-Datenbank gespeichert wird.

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

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

- Erstellen Sie Benutzerkonten manuell und tragen Sie in den Stammdaten der Benutzerkonten ein Kennwort ein.
- Legen Sie ein initiales Kennwort fest, welches beim Erstellen von Benutzerkonten automatisch verwendet wird.
  - Verwenden Sie zielsystemspezifische Kennwortrichtlinien und tragen Sie in den Kennwortrichtlinien ein initiales Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.
  - Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\LDAP\Accounts\InitialRandomPassword".
  - Verwenden Sie zielsystemspezifische Kennwortrichtlinien und definieren Sie in den Kennwortrichtlinien die Zeichenklassen, die das Kennwort enthalten muss.
  - Legen Sie fest, an welche Person das initiale Kennwort per E-Mail versendet wird.

Verwandte Themen

- Kennwortrichtlinien auf Seite 62
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 73

E-Mail-Benachrichtigungen über Anmeldeinformationen

Tabelle 25: Konfigurationsparameter für Benachrichtigungen über Anmeldeinformationen

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

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

Um Benachrichtigungen über Anmeldeinformationen zu nutzen

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

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

Um die initialen Anmeldeinformationen per E-Mail zu versenden

1. Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\LDAP\Accounts\InitialRandomPassword".
2. Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\LDAP\Accounts\InitialRandomPassword\SendTo" und erfassen Sie als Wert den Empfänger der Benachrichtigung.
3. Aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\LDAP\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\LDAP\Accounts\InitialRandomPassword\SendTo\MailTemplatePassword".

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

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

Zielsystemverantwortliche

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

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

   Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle 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 26: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle **Zielsysteme | LDAP** oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: • Übernehmen die administrativen Aufgaben für das Zielsystem. • Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches 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 | LDAP** .
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 **LDAP | 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 **LDAP | 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.

   - Erfassen Sie die Bezeichnung der Anwendungsrolle und ordnen Sie die übergeordnete Anwendungsrolle **Zielsysteme | LDAP** zu.
   - Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, 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 LDAP-Umgebung auf Seite 8
- Allgemeine Stammdaten einer LDAP Domäne auf Seite 78
- LDAP Containerstrukturen auf Seite 122

LDAP Domänen

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

Um die Stammdaten einer LDAP Domäne zu bearbeiten

1. Wählen Sie die Kategorie **LDAP | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten für eine Domäne.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten einer LDAP Domäne auf Seite 78
- LDAP spezifische Stammdaten einer LDAP Domäne auf Seite 80
- Festlegen der Kategorien für die Vererbung von LDAP Gruppen auf Seite 81

Allgemeine Stammdaten einer LDAP Domäne

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

Tabelle 27: Stammdaten einer Domäne

Eigenschaft	Beschreibung
Domäne	NetBIOS Namen der Domäne.
Vollständiger Domänennamen	Domänennamen der Domäne gemäß DNS Syntax.

Eigenschaft	Beschreibung

	`Name dieser Domäne.Name der übergeordneten Domäne.Name der Stammdomäne`
	Beispiel
	`Doku.Testlab.dd`

LDAP Systemtyp	Typ des LDAP Systems.
Anzeigename	Anzeigename zur Anzeige der Domäne in der Benutzeroberfläche. Initial wird der NetBIOS Name der Domäne übernommen; den Anzeigenamen können Sie jedoch ändern.
Objektklasse	Liste von Klassen, die die Attribute dieses Objektes definieren. Als Objektklasse wird standardmäßig „DOMAIN" vorgegeben. Sie können weitere Objektklassen und Hilfsklassen, die von anderen LDAP- und X.500 Verzeichnisdiensten genutzt werden, über das Eingabefeld hinzufügen.
Definierter Name	Definierter Name der Domäne. Der definierte Name wird per Bildungsregel aus dem vollständigen Domänennamen ermittelt und sollte nicht bearbeitet werden.
Kanonischer Name	Kanonischer Name der Domäne.
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.
Zielsystemverantwortliche	Anwendungsrolle, in der die Zielsystemverantwortlichen der Domäne festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte der Domäne, der sie zugeordnet sind. Jeder Domäne können somit andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieser Domäne sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td>Synchronisiert durch</td><td>HINWEIS: Die Art der Synchronisation können Sie nur festlegen, wenn Sie eine Domäne neu anlegen. Nach dem Speichern sind keine Änderungen möglich.
Beim Erstellen einer Domäne mit dem Synchronization Editor wird "One Identity Manager" verwendet.
Art der Synchronisation, über welche die Daten zwischen der Domäne und dem One Identity Manager synchronisiert werden.
Tabelle 28: Zulässige Werte
<table>
<tr><th>Wert</th><th>Synchronisation durch</th><th>Provisionierung durch</th></tr>
<tr><td>One Identity Manager</td><td>LDAP Konnektor</td><td>LDAP Konnektor</td></tr>
<tr><td>Keine Synchronisation</td><td>keine</td><td>keine</td></tr>
</table>
HINWEIS: Wenn Sie "Keine Synchronisation" festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.</td></tr>
<tr><td>Beschreibung</td><td>Freitextfeld für zusätzliche Erläuterungen.</td></tr>
<tr><td>Strukturelle Objektklasse</td><td>Strukturelle Objektklasse, die den Typ des Objektes repräsentiert.</td></tr>
</table>

Verwandte Themen

- Automatische Zuordnung von Personen zu LDAP Benutzerkonten auf Seite 98
- Zielsystemverantwortliche auf Seite 75

LDAP spezifische Stammdaten einer LDAP Domäne

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

Tabelle 29: Angaben zum LDAP

Eigenschaft	Beschreibung

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

Definierter Name	Definierter Name der Domäne. Der definierte Name wird per Bildungsregel aus dem vollständigen Domänennamen ermittelt und sollte nicht bearbeitet werden.
Strukturelle Objektklasse	Strukturelle Objektklasse, die den Typ des Objektes repräsentiert.
Objektklasse	Liste von Klassen, die die Attribute dieses Objektes definieren. Als Objektklasse wird standardmäßig "DOMAIN" vorgegeben. Sie können weitere Objektklassen und Hilfsklassen, die von anderen LDAP- und X.500 Verzeichnisdiensten genutzt werden, über das Eingabefeld hinzufügen.
Suchmaske	Suchfilter für X.500-Clients.

Festlegen der Kategorien für die Vererbung von LDAP Gruppen

Im One Identity Manager können Gruppenselektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält zwei Tabellen; die Benutzerkontentabelle und die Gruppentabelle. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In der Gruppentabelle geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen an. Jede Tabelle enthält die Kategoriepositionen "Position1" bis "Position 31".

Um Kategorien zu definieren

1. Wählen Sie die Kategorie **LDAP | Domänen**.
2. Wählen Sie in der Ergebnisliste die Domäne.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wechseln Sie auf den Tabreiter **Abbildungsvorschrift Kategorien**.

5. Öffnen Sie den jeweiligen Basisknoten der Benutzerkontentabelle bzw. der Gruppentabelle.
6. Aktivieren Sie die Kategorie per Maus-Doppelklick auf das Symbol .
7. Tragen Sie eine beliebige Benennung der Kategorie für Benutzerkonten und Gruppen in der verwendeten Anmeldesprache ein.
8. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Vererbung von LDAP Gruppen anhand von Kategorien auf Seite 118

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 **LDAP | 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 32

LDAP Benutzerkonten

Mit dem One Identity Manager verwalten Sie die Benutzerkonten einer LDAP-Umgebung. Ein Benutzer kann sich mit seinem Benutzerkonto an der Domäne anmelden und erhält über seine Gruppenmitgliedschaften und Rechte Zugriff auf die Netzwerkressourcen.

Detaillierte Informationen zum Thema

- Benutzerkonten mit Personen verbinden auf Seite 83
- Unterstützte Typen von Benutzerkonten auf Seite 84
- Erfassen der Stammdaten für LDAP Benutzerkonten auf Seite 88

Benutzerkonten mit Personen verbinden

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

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

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

- Personen erhalten ihre Benutzerkonten automatisch über Kontendefinitionen. Hat eine Person noch kein Benutzerkonto in einer LDAP 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.

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

- Beim Einfügen eines Benutzerkontos wird automatisch eine vorhandene Person zugeordnet oder im Bedarfsfall eine neue Person erstellt. Dabei werden die Personenstammdaten anhand vorhandener Benutzerkontenstammdaten erzeugt. Dieser Mechanismus kann eingesetzt werden, wenn eine neues Benutzerkonto manuell oder durch eine Synchronisation erstellt wird. Dieses Vorgehen ist jedoch nicht das Standardverfahren für den One Identity Manager. Für die automatische Personenzuordnung definieren Sie Kriterien, anhand derer die Personen ermittelt werden sollen.

Verwandte Themen

- Erfassen der Stammdaten für LDAP Benutzerkonten auf Seite 88
- Einrichten von Kontendefinitionen auf Seite 43
- Automatische Zuordnung von Personen zu LDAP Benutzerkonten auf Seite 98
- Ausführliche Informationen zu den Grundlagen zur Behandlung und Administration von Personen und Benutzerkonten finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Unterstützte Typen von Benutzerkonten

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

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität (Spalte `IdentityType`)

  Die Identität beschreibt den Typ des Benutzerkontos.

Tabelle 30: Identitäten von Benutzerkonten

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

- Privilegiertes Benutzerkonto (Spalte `IsPrivilegedAccount`)

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

Standardbenutzerkonten

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

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

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

3. Erstellen Sie eine Abbildungsvorschrift für die IT Betriebsdaten.

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

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

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

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

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

5. Weisen Sie die Kontendefinition an die Personen zu.

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

Administrative Benutzerkonten

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

Administrative Benutzerkonten werden durch die Synchronisation in den One Identity Manager eingelesen. Um administrativen Benutzerkonten einen Verantwortlichen zuzuweisen, weisen Sie dem Benutzerkonto im One Identity Manager eine Person zu.

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

Privilegierte Benutzerkonten

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

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

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

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

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

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

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

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

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

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

Um ein Präfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\LDAP\Accounts\PrivilegedAccount\UserID_Prefix" . Um ein Postfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\LDAP\Accounts\PrivilegedAccount\UserID_Postfix" .

Diese Konfigurationsparameter werden in der Standardinstallation ausgewertet, wenn Sie ein Benutzerkonto, mit der Eigenschaft **Privilegiertes Benutzerkonto** (`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.

Erfassen der Stammdaten für LDAP Benutzerkonten

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

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

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

Um die Stammdaten eines Benutzerkontos zu bearbeiten

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

   - ODER -

   Klicken Sie in der Ergebnisliste .

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

Um ein Benutzerkonto für eine Person manuell zuzuweisen oder zu erstellen

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten eines LDAP Benutzerkontos auf Seite 89
- Kontaktinformationen eines LDAP Benutzerkontos auf Seite 93
- Adressinformationen eines LDAP Benutzerkontos auf Seite 94
- Organisatorische Informationen eines LDAP Benutzerkontos auf Seite 95
- Sonstige Informationen eines LDAP Benutzerkontos auf Seite 96

Verwandte Themen

- Unterstützte Typen von Benutzerkonten auf Seite 84
- Einrichten von Kontendefinitionen auf Seite 43

Allgemeine Stammdaten eines LDAP Benutzerkontos

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

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

Eigenschaft	Beschreibung
	Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden.
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.
Domäne	Domäne, in der das Benutzerkonto erzeugt werden soll.
Strukturelle Objektklasse	Strukturelle Objektklasse, die den Typ des Objektes repräsentiert. Standardmäßig werden die Benutzerkonten im One Identity Manager mit der Objektklasse "INETORGPERSON" angelegt.
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.
Objektklasse	Liste von Klassen, die die Attribute dieses Objektes definieren. Standardmäßig werden die Benutzerkonten im One Identity Manager mit der Objektklasse "INETORGPERSON" angelegt. Sie können weitere Objektklassen und Hilfsklassen, die von anderen LDAP- und X.500 Verzeichnisdiensten genutzt werden, über das Eingabefeld hinzufügen.
Bezeichnung	Bezeichnung des Benutzerkontos. Die Bezeichnung wird aus dem Vornamen und dem Nachnamen des Benutzers gebildet.
Anzeigename	Anzeigename des Benutzerkontos. Der Anmeldename wird aus dem Vornamen und dem Nachnamen 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.
Objekt SID (AD)	Sicherheits-ID (SID) des Objektes im Active Directory.
Vorname	Vorname des Benutzers. Haben Sie eine Kontendefinition zugeord-

Eigenschaft	Beschreibung
	net, 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.
Berufsbezeichnung	Berufsbezeichnung. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Anmeldename	Anmeldename. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, der Anmeldename aus dem zentralen Benutzerkonto der Person gebildet.
Kennwort	Kennwort für das Benutzerkonto. Abhängig vom Konfigurationsparameter "Person\UseCentralPassword" wird das zentrale Kennwort der zugeordneten Person auf das Kennwort des Benutzerkontos abgebildet. Wenn Sie ein initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen. HINWEIS: Beim Prüfen eines Benutzerkennwortes werden die One Identity Manager Kennwortrichtlinien beachtet. Stellen Sie sicher, dass die Kennwortrichtlinie nicht gegen die Anforderungen des Zielsystems verstößt.
Kennwortbestätigung	Kennwortwiederholung.
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.
Kontoverfallsdatum	Kontoverfallsdatum. Die Festlegung eines Kontoverfallsdatums bewirkt, dass die Anmeldung für dieses Benutzerkonto 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.
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto.

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt.</td></tr>
<tr><td>Beschreibung</td><td>Freitextfeld für zusätzliche Erläuterungen.</td></tr>
<tr><td>Identität</td><td>Typ der Identität des Benutzerkontos.

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

• Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen.
• Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.</td></tr>
</table>

Eigenschaft	Beschreibung
Benutzerkonto ist deaktiviert	Angabe, ob das Benutzerkonto deaktiviert ist. Wird ein Benutzerkonto vorübergehend nicht benötigt, können Sie das Benutzerkonto über die Option zeitweilig deaktivieren.

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 43
- Kennwortrichtlinien auf Seite 62
- Initiales Kennwort für neue LDAP Benutzerkonten auf Seite 71
- Benutzerkonten mit Personen verbinden auf Seite 83
- Deaktivieren von LDAP Benutzerkonten auf Seite 103

Kontaktinformationen eines LDAP Benutzerkontos

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

Tabelle 33: Kontaktinformationen

Eigenschaft	Beschreibung
Bild	Bild, beispielsweise zur Anzeige in einem internen Telefonbuch. • Laden Sie das Bild über die Schaltfläche . • Über die Schaltfläche können Sie das Bild löschen .
E-Mail-Adresse	E-Mail-Adresse. Haben Sie eine Kontendefinition zugeordnet, wird, abhängig vom Automatisierungsgrad, die E-Mail-Adresse aus der Standard-E-Mail-Adresse der Person gebildet.
Telefon	Telefonnummer.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.
Fax	Faxnummer. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Telefon privat	Private Telefonnummer.

Eigenschaft	Beschreibung
Telefon privat (2)	Weitere private Telefonnummer.
Internationale ISDN Nummer	Internationale ISDN Nummer.
Weitere E-Mail-Adressen	Weitere E-Mail-Adresse.
X.121-Adresse	Adressierung als X.121-Adresse.
X400-Adresse	Adressierung im X400-Format.

Adressinformationen eines LDAP Benutzerkontos

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

Tabelle 34: Adressdaten

Eigenschaft	Beschreibung
Raum	Raum. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Hausanschrift	Postanschrift.
Adresse	Postanschrift.
Postanschrift privat	Private Postanschrift.
Postfach	Postfach. 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.
Postleitzahl	Postleitzahl. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Bundesland	Bundesland. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.

Organisatorische Informationen eines LDAP Benutzerkontos

Auf dem Tabreiter **Organisatorisch** erfassen Sie die folgenden organisatorischen Stammdaten.

Tabelle 35: Organisatorische Stammdaten

Eigenschaft	Beschreibung
Geschäftsbereich	Geschäftsbereich, dem die Person zugeordnet ist.
Abteilung	Abteilung der Person. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Standort	Standort der Person. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Standortkennzeichen	Standortkennzeichen (Land und Ort) für Telegrammdienst.
Art der Anstellung	Angaben zur Anstellung.
Personennummer	Nummer zur Kennzeichnung der Person zusätzlich zur Personenkennung.
Titel	Akademischer Titel des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Position im Unternehmen	Angabe zur Position im Unternehmen, beispielsweise Geschäftsführer oder Abteilungsleiter.
Büro	Büro. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Bevorzugte Sprache	Bevorzugte Sprache. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Kontomanager	Verantwortlicher für das Benutzerkonto.
Assistent	Benutzerkonto des Assistenten.
Länderkennung	Länderkennung.
Firma	Firma der Person. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Autokennzeichen	Kennzeichen des Fahrzeugs.

Sonstige Informationen eines LDAP Benutzerkontos

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

Tabelle 36: Sonstige Stammdaten

Eigenschaft	Beschreibung
Siehe auch	Verweis auf ein anderes LDAP Objekt.
Stamm-PC	Arbeitsstation des Benutzers.
Benutzer-ID	Identifikationsnummer oder Ausweisnummer des Benutzers.

Zusätzliche Aufgaben für die Verwaltung von LDAP Benutzerkonten

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

Überblick über das LDAP 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 **LDAP | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Überblick über das LDAP Benutzerkonto**.

Ändern des Automatisierungsgrades an einem LDAP 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 die Kategorie **LDAP | 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 LDAP Benutzerkonten auf Seite 88

LDAP Gruppen direkt an ein LDAP 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 LDAP, werden die Gruppen der Rollen an dieses Benutzerkonto vererbt.

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

HINWEIS: Benutzerkonten können nicht manuell in dynamische Gruppen aufgenommen werden. Die Mitgliedschaften in einer dynamischen Gruppe werden über die Bedingung der dynamischen Gruppe ermittelt.

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

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

   - ODER -

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

Verwandte Themen

- LDAP Gruppe an LDAP Benutzerkonten und LDAP Computer zuweisen auf Seite 108

Zusatzeigenschaften an ein LDAP 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 die Kategorie **LDAP | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   - ODER -

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

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

Automatische Zuordnung von Personen zu LDAP Benutzerkonten

Tabelle 37: Konfigurationsparameter für die automatische Personenzuordnung

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

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\LDAP\PersonAutoFullsync" und wählen Sie den gewünschte Modus.
- Wenn Personen außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter "TargetSystem\LDAP\PersonAutoDefault" und wählen Sie den gewünschte Modus.
- Legen Sie über den Konfigurationsparameter "TargetSystem\LDAP\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

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

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

Verwandte Themen

- Erstellen einer Kontendefinition auf Seite 44
- Zuweisen der Kontendefinition an ein Zielsystem auf Seite 59
- Bearbeiten der Suchkriterien für die automatische Personenzuordnung auf Seite 100

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 `LDAPDomain` 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 **LDAP | 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 38: Standardsuchkriterien für Benutzerkonten

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
LDAP Benutzerkonten	Zentrales Benutzerkonto (CentralAccount)	Anmeldename (UserID)

5. Speichern Sie die Änderungen.

Direkte Zuordnung von Personen an Benutzerkonten anhand einer Vorschlagsliste

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

Tabelle 39: Ansichten zur manuellen Zuordnung

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

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 LDAP Benutzerkonten auf Seite 98

Deaktivieren von LDAP Benutzerkonten

Tabelle 40: Konfigurationsparameter für das Deaktivieren von Benutzerkonten

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

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

Szenario:

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

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

Szenario:

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

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

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

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu sperren

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

Szenario:

- Benutzerkonten sind nicht mit Personen verbunden.

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

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

Verwandte Themen

- Einrichten von Kontendefinitionen auf Seite 43
- Erstellen der Automatisierungsgrade auf Seite 47
- Löschen und Wiederherstellen von LDAP Benutzerkonten auf Seite 104
- Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Löschen und Wiederherstellen von LDAP Benutzerkonten

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 **LDAP | 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 **LDAP | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Klicken Sie in der Ergebnisliste die Schaltfläche **Löschen rückgängig machen**.

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 LDAPAccount.

Verwandte Themen

- Deaktivieren von LDAP Benutzerkonten auf Seite 103

LDAP Gruppen

Im LDAP-Verzeichnis können Benutzerkonten, Kontakte, Computer und Gruppen in Gruppen zusammengefasst werden, mit denen der Zugriff auf Ressourcen geregelt werden kann. Im One Identity Manager können Sie neue Gruppen einrichten oder bereits vorhandene Gruppen editieren.

Um Benutzer in Gruppen aufzunehmen, können Sie die Gruppen direkt an die Benutzer zuweisen. Sie können Gruppen an Abteilungen, Kostenstellen, Standorte, Geschäftsrollen oder den IT Shop zuweisen.

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie die Kategorie **LDAP | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.

   - ODER -

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

Detaillierte Informationen zum Thema

- Stammdaten einer LDAP Gruppe auf Seite 106
- LDAP Gruppe an LDAP Benutzerkonten und LDAP Computer zuweisen auf Seite 108

Stammdaten einer LDAP Gruppe

Erfassen Sie die folgenden Stammdaten.

Tabelle 41: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Definierter Name	Definierter Name der Gruppe. Der definierte Name wird per Bildungsregel aus dem Namen der Gruppe und dem Container ermittelt und sollte nicht bearbeitet werden.
Bezeichnung	Bezeichnung der Gruppe.
Anzeigename	Anzeigename zur Anzeige der Gruppe in der Benutzeroberfläche der One Identity Manager Werkzeuge.
Domäne	Domäne in der die Gruppe angelegt werden soll.
Container	Container, in dem die Gruppe angelegt werden soll.
Administrator	Administrator der Gruppe.
Leistungsposition	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Geschäftsbereich	Geschäftsbereich, dem die Gruppe zugeordnet ist.
Siehe auch	Verweis auf ein anderes LDAP Objekt.
Strukturelle Objektklasse	Strukturelle Objektklasse, die den Typ des Objektes repräsentiert. Standardmäßig werden die Gruppen im One Identity Manager mit der Objektklasse "GROUPOFNAMES" angelegt.
Objektklasse	Liste von Klassen, die die Attribute dieses Objektes definieren. Standardmäßig werden die Gruppen im One Identity Manager mit der Objektklasse "GROUPOFNAMES" angelegt. Sie können weitere Objektklassen und Hilfsklassen, die von anderen LDAP- und X.500 Verzeichnisdiensten genutzt werden, über das Eingabefeld hinzufügen.
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 zur Risikobewertung finden Sie im One Identity Manager Administrationshandbuch für Risikobewertungen.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Über die Auswahlliste ordnen Sie die Gruppe einer oder mehreren Kategorien zu.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Bedingung	LDAP Filter für die Bestimmung der Mitgliedschaften einer dynamische Gruppe.
Dynamische	Angabe, ob es sich um eine dynamische Gruppe handelt.

Eigenschaft	Beschreibung
Gruppe	
IT Shop	Angabe, ob die Gruppe über den IT Shop bestellbar ist. Die Gruppe kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Die Gruppe kann über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.

Verwandte Themen

- Vererbung von LDAP Gruppen anhand von Kategorien auf Seite 118
- Ausführliche Informationen zur Vorbereitung der Gruppen für die Bestellung über den IT Shop finden Sie im One Identity Manager Administrationshandbuch für IT Shop.

LDAP Gruppe an LDAP Benutzerkonten und LDAP 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 besitzt, dann wird dieses Benutzerkonto 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 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\LDAP\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 über IT Shop-Bestellungen an Personen zugewiesen werden. Damit Gruppen über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Gruppen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Gruppen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

Detaillierte Informationen zum Thema

- LDAP Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 109
- LDAP Gruppe an Geschäftsrollen zuweisen auf Seite 110
- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 111
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 112
- LDAP Gruppe in Systemrollen aufnehmen auf Seite 113
- LDAP Gruppe in den IT Shop aufnehmen auf Seite 114
- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

LDAP 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 die Kategorie **LDAP | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.

4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
    - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
    - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
    - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

    - ODER -

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

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

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

    - ODER -

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

    - ODER -

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

    - ODER -

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

Verwandte Themen

- LDAP Gruppe an Geschäftsrollen zuweisen auf Seite 110
- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 111
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 112
- LDAP Gruppe in Systemrollen aufnehmen auf Seite 113
- LDAP Gruppe in den IT Shop aufnehmen auf Seite 114
- One Identity Manager Benutzer für die Verwaltung einer LDAP-Umgebung auf Seite 8

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

   - ODER -

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

Um Gruppen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

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

   - ODER -

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

Verwandte Themen

- LDAP Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 109
- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 111
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 112
- LDAP Gruppe in Systemrollen aufnehmen auf Seite 113
- LDAP Gruppe in den IT Shop aufnehmen auf Seite 114
- One Identity Manager Benutzer für die Verwaltung einer LDAP-Umgebung auf Seite 8

LDAP Benutzerkonten direkt an eine LDAP 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 LDAP, werden die Gruppen der Rollen an dieses Benutzerkonto vererbt.

Um auf Sonderanforderungen schnell zu reagieren, können Sie die Gruppe direkt an Benutzerkonten zuweisen.

HINWEIS: Benutzerkonten können nicht manuell in dynamische Gruppen aufgenommen werden. Die Mitgliedschaften in einer dynamischen Gruppe werden über die Bedingung der dynamischen Gruppe ermittelt.

Um eine Gruppe direkt an Benutzerkonten zuzuweisen

1. Wählen Sie die Kategorie **LDAP | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Benutzerkonten zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Benutzerkonten zu.

   - ODER -

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

Verwandte Themen

- LDAP Gruppen direkt an ein LDAP Benutzerkonto zuweisen auf Seite 97
- LDAP Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 109
- LDAP Gruppe an Geschäftsrollen zuweisen auf Seite 110
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 112
- LDAP Gruppe in Systemrollen aufnehmen auf Seite 113
- LDAP Gruppe in den IT Shop aufnehmen auf Seite 114

LDAP Computer direkt an eine LDAP 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.

HINWEIS: Computer können nicht manuell in dynamische Gruppen aufgenommen werden. Die Mitgliedschaften in einer dynamischen Gruppe werden über die Bedingung der dynamischen Gruppe ermittelt.

Um eine Gruppe direkt an Computer zuzuweisen

1. Wählen Sie die Kategorie **LDAP | 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.

Verwandte Themen

- LDAP Computer direkt an LDAP Gruppen zuweisen auf Seite 127
- LDAP Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 109
- LDAP Gruppe an Geschäftsrollen zuweisen auf Seite 110
- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 111
- LDAP Gruppe in Systemrollen aufnehmen auf Seite 113
- LDAP Gruppe in den IT Shop aufnehmen auf Seite 114

LDAP 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 die Kategorie **LDAP | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Systemrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Systemrollen zu.

   - ODER -

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

Verwandte Themen

- LDAP Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 109
- LDAP Gruppe an Geschäftsrollen zuweisen auf Seite 110
- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 111
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 112
- LDAP Gruppe in den IT Shop aufnehmen auf Seite 114

LDAP 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.
- 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 die Kategorie **LDAP | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

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

Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **LDAP | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | LDAP Gruppen** (bei rollenbasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.

3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Um eine Gruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **LDAP | Gruppen** (bei nicht-rollenbasierter Anmeldung).

   - ODER -

   Wählen Sie die Kategorie **Berechtigungen | LDAP 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

- Stammdaten einer LDAP Gruppe auf Seite 106
- LDAP Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 109
- LDAP Gruppe an Geschäftsrollen zuweisen auf Seite 110
- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 111
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 112
- LDAP Gruppe in Systemrollen aufnehmen auf Seite 113

Zusätzliche Aufgaben für die Verwaltung von LDAP Gruppen

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

Überblick über die LDAP 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 **LDAP | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die LDAP Gruppe**.

Wirksamkeit von Gruppenmitgliedschaften

Tabelle 42: 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, wird durch den One Identity Manager nicht überprüft.

Die Wirksamkeit der Zuweisungen wird in den Tabellen LDAPAccountInLDAPGroup und BaseTreeHasLDAPGroup 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 43: Festlegen der ausgeschlossenen Gruppen (Tabelle LDAPGroupExclusion)

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

Tabelle 44: 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 45: 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 die Kategorie **LDAP | 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 LDAP Gruppen anhand von Kategorien

Im One Identity Manager können Gruppenselektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Die Kategorien sind frei wählbar und werden über eine Abbildungsvorschrift festgelegt. Jede der Kategorien erhält innerhalb dieser Abbildungsvorschrift eine bestimmte Position. Die Abbildungsvorschrift enthält zwei Tabellen; die Benutzerkontentabelle und die Gruppentabelle. In der Benutzerkontentabelle legen Sie Ihre Kategorien für die zielsystemabhängigen Benutzerkonten fest. In der Gruppentabelle geben Sie Ihre Kategorien für die zielsystemabhängigen Gruppen an. Jede Tabelle enthält die Kategoriepositionen "Position1" bis "Position 31".

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

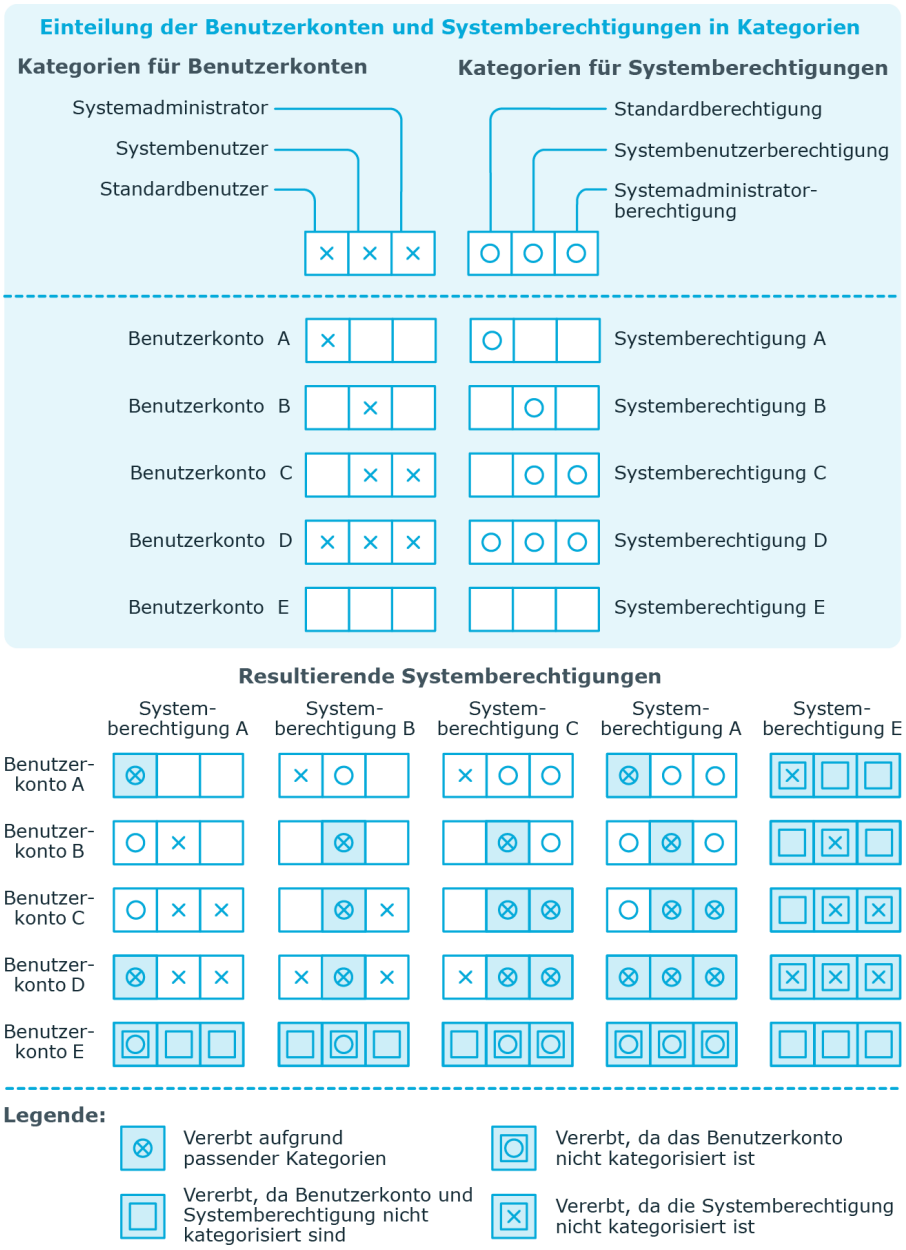
Benutzerkonto nicht in Kategorien eingestuft, dann wird die Gruppe ebenfalls an das Benutzerkonto vererbt.

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

Tabelle 46: 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 LDAP Gruppen auf Seite 81
- Allgemeine Stammdaten eines LDAP Benutzerkontos auf Seite 89
- Stammdaten einer LDAP Gruppe auf Seite 106

Zusatzeigenschaften an eine LDAP 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 die Kategorie **LDAP | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Zusatzeigenschaften zu.

   - ODER -

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

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

Löschen von LDAP Gruppen

Um eine Gruppe zu löschen

1. Wählen Sie die Kategorie **LDAP | 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 LDAP-Umgebung gelöscht.

LDAP Containerstrukturen

Die LDAP Container werden in einer hierarchischen Baumstruktur dargestellt. Container werden häufig dazu genutzt Organisationseinheiten wie beispielsweise Geschäftsstellen oder Abteilungen abzubilden, die Objekte des LDAP Verzeichnisses wie Benutzerkonten, Gruppen und Computer logisch zu organisieren und somit die Verwaltung der Objekte zu erleichtern. Die Container eines LDAP Verzeichnisses werden durch die Synchronisation in die One Identity Manager-Datenbank eingelesen.

Um die Stammdaten eines Containers zu bearbeiten

1. Wählen Sie die Kategorie **LDAP | 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

- Allgemeine Stammdaten eines LDAP Containers auf Seite 122
- Kontaktinformationen eines LDAP Containers auf Seite 124
- Adressinformationen eines LDAP Containers auf Seite 124

Allgemeine Stammdaten eines LDAP Containers

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

Tabelle 47: Stammdaten eines Containers

Eigenschaft	Beschreibung
Anzeigename	Anzeigename zur Anzeige des Containers.
Domäne	Domäne des Containers.
Übergeordneter Container	Übergeordneter Container zur Abbildung einer hierarchischen Containerstruktur. Der definierte Name wird dann automatisch durch Bildungsregeln aktualisiert.
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 sollte nicht geändert werden.
Geschäftsbereich	Geschäftsbereich, dem der Container zugeordnet ist.
Link (Bezeichnetes URI-Format)	Angabe von Links im bezeichneten Uniform Resource Identifier (URI) Format; bestehend aus einer Bezeichnung sowie einem Uniform Resource Locator (URL).
Suchmaske	Suchfilter für X.500-Clients.
Siehe auch	Verweis auf ein anderes LDAP Objekt.
Bundesland	Bundesland.
Strukturelle Objektklasse	Strukturelle Objektklasse, die den Typ des Objektes repräsentiert. Standardmäßig werden die Container im One Identity Manager mit der Objektklasse "ORGANIZATIONALUNIT" angelegt.
Objektklasse	Liste von Klassen, die die Attribute dieses Objektes definieren. Standardmäßig werden die Container im One Identity Manager mit der Objektklasse "ORGANIZATIONALUNIT" angelegt. Sie können weitere Objektklassen und Hilfsklassen, die von anderen LDAP- und X.500 Verzeichnisdiensten genutzt werden, über das Eingabefeld hinzufügen.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
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.

Eigenschaft	Beschreibung
	Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieses Container sind. Über die Schaltfläche neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.

Verwandte Themen

- Zielsystemverantwortliche auf Seite 75

Kontaktinformationen eines LDAP Containers

Auf dem Tabreiter **Kontaktdaten** erfassen Sie die Daten zur Erreichbarkeit.

Tabelle 48: Kontaktinformationen

Eigenschaft	Beschreibung
Fax	Faxnummer.
Internationale ISDN Nummer	Internationale ISDN Nummer.
Telefon	Telefonnummer.
Teletex-ID	Teletex-Terminal Identifizierung.
Telex	Telex-Nummer.
Kennwort	Kennwort.
Kennwortbestätigung	Kennwortwiederholung.

Adressinformationen eines LDAP Containers

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

Tabelle 49: Adressdaten

Eigenschaft	Beschreibung
Name des Gebäudes	Bezeichnung des Gebäudes.
Standortkennzeichen	Standortkennzeichen (Land und Ort) für Telegrammdienst.
Büro	Büro.
Adresse	Postanschrift.
Postleitzahl	Postleitzahl. 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.
Bevorzugte Zustell-methode	Bevorzugte Zustellmethode.
Hausanschrift	Postanschrift.
Straße	Straße. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
X.121-Adresse	Adressierung als X.121-Adresse.

8

LDAP Computer

Im Datenmodell des One Identity Manager ist die Verwaltung von Computern und Servern eines LDAP Verzeichnisses vorgesehen. Um diese Daten mit der LDAP-Umgebung zu synchronisieren, passen Sie Ihr Synchronisationsprojekt entsprechend an.

Um die Stammdaten eines Computers zu bearbeiten

1. Wählen Sie die Kategorie **LDAP | 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.

Detaillierte Informationen zum Thema

- Stammdaten eines LDAP Computers auf Seite 126

Verwandte Themen

- One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation

Stammdaten eines LDAP Computers

Für einen Computer erfassen Sie die folgenden Stammdaten.

Tabelle 50: 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.

Eigenschaft	Beschreibung
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.
Strukturelle Objektklasse	Strukturelle Objektklasse, die den Typ des Objektes repräsentiert.
Objektklasse	Liste von Klassen, die die Attribute dieses Objektes definieren. Sie können weitere Objektklassen und Hilfsklassen, die von anderen LDAP- und X.500 Verzeichnisdiensten genutzt werden, über das Eingabefeld hinzufügen.

Verwandte Themen

- One Identity Manager Administrationshandbuch für das Identity Management Basismodul

LDAP Computer direkt an LDAP 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.

HINWEIS: Computer können nicht manuell in dynamische Gruppen aufgenommen werden. Die Mitgliedschaften in einer dynamischen Gruppe werden über die Bedingung der dynamischen Gruppe ermittelt.

Um einen Computer direkt an Gruppen zuzuweisen

1. Wählen Sie die Kategorie **LDAP | 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.

   - ODER -

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

Verwandte Themen

- LDAP Gruppe an LDAP Benutzerkonten und LDAP Computer zuweisen auf Seite 108

9

Berichte über LDAP 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 LDAP stehen folgende Berichte zur Verfügung.

HINWEIS: Abhängig von den vorhandenen Modulen können weitere Berichte zur Verfügung stehen.

Tabelle 51: 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 Systemberechtigungen anzeigen	Der Bericht enthält alle Gruppen der Domäne, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity

Bericht	Beschreibung
	Manager.
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen anzeigen	Der Bericht enthält alle Benutzerkonten der Domäne, die eine überdurchschnittliche Anzahl an Gruppenmitgliedschaften besitzen.
LDAP 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 LDAP 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 130

Übersicht aller Zuweisungen

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

Beispiele

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

Um detaillierte Informationen über Zuweisungen anzuzeigen

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

  Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol in der Symbolleiste des Berichtes.
- Mit einem Maus-Doppelklick auf das Steuerelement einer Rolle zeigen Sie alle untergeordneten Rollen der ausgewählten Rolle an.
- Mit einem einfachen Mausklick auf die Schaltfläche im Steuerelement einer Rolle zeigen Sie alle Personen dieser Rolle an, die das Basisobjekt besitzen.
- Über den Pfeil rechts neben der Schaltfläche starten Sie einen Assistenten, mit dem Sie die Liste der angezeigten Personen zur Nachverfolgung speichern können. Dabei wird eine neue Geschäftsrolle erstellt und die Personen werden der Geschäftsrolle zugeordnet.

Abbildung 3: Symbolleiste des Berichts "Übersicht aller Zuweisungen"

Tabelle 52: Bedeutung der Symbole in der Symbolleiste des Berichts

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

Anhang: Konfigurationsparameter für die Verwaltung einer LDAP-Umgebung

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

Tabelle 53: Konfigurationsparameter für die Synchronisation mit einem LDAP-Verzeichnis

Konfigurationsparameter	Beschreibung
TargetSystem\LDAP	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung des Zielsystems LDAP. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.
TargetSystem\LDAP\Accounts	Der Konfigurationsparameter erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem\LDAP\Accounts \InitialRandomPassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.
TargetSystem\LDAP\Accounts\ InitialRandomPassword\SendTo	Der Konfigurationsparameter enthält die Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der

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

Konfigurationsparameter	Beschreibung
TargetSys-tem\LDAP\Authentication\Authentication	Der Konfigurationsparameter legt den Authentifizierungsmechanismus fest. Gültige Werte sind "Secure", "Encryption", "SecureSocketsLayer", "ReadonlyServer", "Anonymous", "FastBind", "Signing", "Sealing", "Delegation" und "ServerBind". Die Werte können mit Komma (,) kombiniert werden. Ausführliche Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library. Standard ist ServerBind.
TargetSystem\LDAP\Authentication\Port	Port des LDAP Servers. Standard ist Port 389.
TargetSystem\LDAP\Authentication\RootDN	Der Konfigurationsparameter enthält den Distinguished Name der Root-Domäne. Syntax: `dc=MyDomain`
TargetSystem\LDAP\Authentication\Server	Der Konfigurationsparameter enthält den Namen des LDAP Servers.
TargetSystem\LDAP\DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem\LDAP\ HardwareInGroupFromOrg	Der Konfigurationsparameters legt fest. ob Computer aufgrund von Gruppenzuordnung zu Rollen in Gruppen aufgenommen werden.
TargetSystem\LDAP\ 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\LDAP\ PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische

Konfigurationsparameter	Beschreibung
	Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\LDAP\ PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem\LDAP\ PersonAutoFullSync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.

Anhang: Standardprojektvorlagen für LDAP

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.

Detaillierte Informationen zum Thema

- OpenDJ Basisvorlage auf Seite 136
- Standardprojektvorlage für Active Directory Lightweight Directory Services auf Seite 137

OpenDJ Basisvorlage

Diese Projektvorlage basiert auf OpenDJ. Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 54: Abbildung der Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im LDAP	Tabelle im One Identity Manager Schema
domain	LDPDomain
organization	LDAPContainer
organizationalUnit	LDAPContainer

Schematyp im LDAP	Tabelle im One Identity Manager Schema
locality	LDAPContainer
container	LDAPContainer
groupOfNames	LDAPGroup
groupOfUniqueNames	LDAPGroup
groupOfURLs	LDAPGroup
inetOrgPerson	LDAPAccount

Standardprojektvorlage für Active Directory Lightweight Directory Services

Diese Projektvorlage basiert auf Active Directory Lightweight Directory Services (AD LDS). Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 55: Abbildung der Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im AD LDS	Tabelle im One Identity Manager Schema
container	LDAPContainer
country	LDAPContainer
domainDNS	LDAPContainer
foreignSecurityPrincipal	LDAPAccount
group	LDAPGroup
groupOfNames	LDAPGroup
inetOrgPerson	LDAPAccount
organization	LDAPContainer
organizationalUnit	LDAPContainer
user	LDAPAccount
userProxy	LDAPAccount
userProxyFull	LDAPAccount

Anhang: Authentifizierungsmodule für die Anmeldung am One Identity Manager

Mit der Installation des Moduls sind zusätzlich die folgenden Authentifizierungsmodule zur Anmeldung am One Identity Manager verfügbar.

LDAP Benutzerkonto (dynamisch)

Anmeldeinformationen	Anmeldenamen, Bezeichnung, definierter Name oder Benutzer-ID eines LDAP Benutzerkontos. Kennwort des LDAP Benutzerkontos.
Voraussetzungen	Die Person ist in der One Identity Manager-Datenbank vorhanden. Das LDAP Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen. Die Konfigurationsdaten zur dynamischen Ermittlung des Systembenutzers sind an der Anwendung definiert. Somit kann beispielsweise einer Person, in Abhängigkeit ihrer Abteilungszugehörigkeit, dynamisch ein Systembenutzer zugeordnet werden.
Aktiviert im Standard	nein
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	Bei der Anmeldung über den Anmeldenamen, die Bezeichnung oder die Benutzer-ID wird über die Domäne des Containers das

entsprechende Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Erfolgt die Anmeldung über den definierten Namen, wird dieser direkt verwendet. Der One Identity Manager ermittelt die Person, die dem LDAP Benutzerkonto zugeordnet ist.

Besitzt eine Person mehrere Identitäten, wird über den Konfigurationsparameter "QER\Person\MasterIdentity\UseMasterForAuthentication" gesteuert, welche Person zur Authentifizierung verwendet wird.

- Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.
- Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt.

Über die Konfigurationsdaten der Anwendung wird ein Systembenutzer ermittelt und der Person dynamisch zugeordnet. Die Benutzeroberfläche und die Bearbeitungsrechte werden über den Systembenutzer geladen, der der angemeldeten Person dynamisch zugeordnet ist.

Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.

Für den Einsatz des Authentifizierungsmoduls passen Sie im Designer die folgenden Konfigurationsparameter an.

Tabelle 56: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
TargetSystem\LDAP\Authentication	Der Konfigurationsparameter erlaubt die Konfiguration der LDAP Authentifizierungsmodule.
TargetSystem\LDAP\Authentication\Authentication	Der Konfigurationsparameter legt den Authentifizierungsmechanismus fest. Gültige Werte sind "Secure", "Encryption", "SecureSocketsLayer", "ReadonlyServer", "Anonymous", "FastBind", "Signing", "Sealing", "Delegation" und "ServerBind". Die Werte können mit Komma (,) kombiniert werden. Ausführliche Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library. Standard ist ServerBind.
TargetSystem\LDAP\Authentication\Port	Port des LDAP Servers. Standard ist

Konfigurationsparameter	Bedeutung
	Port 389.
TargetSystem\LDAP\Authentication\RootDN	Der Konfigurationsparameter enthält den Distinguished Name der Root-Domäne. Syntax: `dc=MyDomain`
TargetSystem\LDAP\Authentication\Server	Der Konfigurationsparameter enthält den Namen des LDAP Servers.

LDAP Benutzerkonto (rollenbasiert)

Anmeldeinformationen	Anmeldenamen, Bezeichnung, definierter Name oder Benutzer-ID eines LDAP Benutzerkontos. Kennwort des LDAP Benutzerkontos.
Voraussetzungen	Die Person ist in der One Identity Manager-Datenbank vorhanden. Die Person ist mindestens einer Anwendungsrolle zugewiesen. Das LDAP Benutzerkonto ist in der One Identity Manager-Datenbank vorhanden und in den Stammdaten des Benutzerkontos ist die Person eingetragen. Die Konfigurationsdaten zur dynamischen Ermittlung des Systembenutzers sind an der Anwendung definiert. Somit kann beispielsweise einer Person, in Abhängigkeit ihrer Abteilungszugehörigkeit, dynamisch ein Systembenutzer zugeordnet werden.
Aktiviert im Standard	nein
Single Sign-on	nein
Anmeldung am Frontend möglich	ja
Anmeldung am Web Portal möglich	ja
Bemerkungen	Bei der Anmeldung über den Anmeldenamen, die Bezeichnung oder die Benutzer-ID wird über die Domäne des Containers das entsprechende Benutzerkonto in der One Identity Manager-Datenbank ermittelt. Erfolgt die Anmeldung über den definierten Namen, wird dieser direkt verwendet. Der One Identity Manager ermittelt die Person, die dem LDAP Benutzerkonto zugeordnet ist. Besitzt eine Person mehrere Identitäten, wird über den

Konfigurationsparameter "QER\Person\MasterIdentity\UseMasterForAuthentication" gesteuert, welche Person zur Authentifizierung verwendet wird.

- Ist der Konfigurationsparameter aktiviert, wird die Hauptidentität der Person für die Authentifizierung genutzt.
- Ist der Parameter deaktiviert, wird die Subidentität der Person für die Authentifizierung genutzt.

Es wird ein dynamischer Systembenutzer aus den Anwendungsrollen der Person ermittelt. Die Benutzeroberfläche und die Bearbeitungsrechte werden über diesen Systembenutzer geladen.

Datenänderungen werden dem angemeldeten Benutzerkonto zugeordnet.

Für den Einsatz des Authentifizierungsmoduls passen Sie im Designer die folgenden Konfigurationsparameter an.

Tabelle 57: Konfigurationsparameter für das Authentifizierungsmodul

Konfigurationsparameter	Bedeutung
TargetSystem\LDAP\Authentication	Der Konfigurationsparameter erlaubt die Konfiguration der LDAP Authentifizierungsmodule.
TargetSystem\LDAP\Authentication\Authentication	Der Konfigurationsparameter legt den Authentifizierungsmechanismus fest. Gültige Werte sind "Secure", "Encryption", "SecureSocketsLayer", "ReadonlyServer", "Anonymous", "FastBind", "Signing", "Sealing", "Delegation" und "ServerBind". Die Werte können mit Komma (,) kombiniert werden. Ausführliche Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library. Standard ist ServerBind.
TargetSystem\LDAP\Authentication\Port	Port des LDAP Servers. Standard ist Port 389.
TargetSystem\LDAP\Authentication\RootDN	Der Konfigurationsparameter enthält den Distinguished Name der Root-Domäne. Syntax: `dc=MyDomain`

Konfigurationsparameter	Bedeutung
TargetSystem\LDAP\Authentication\Server	Der Konfigurationsparameter enthält den Namen des LDAP Servers.

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 besuchen Sie https://www.oneidentity.com/company/contact-us.aspx oder rufen Sie + 1-800-306-9329 an.

Technische Supportressourcen

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

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

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

Index

L

M

O

P

R

S

Z