One Identity Manager 9.2

Administrationshandbuch für die Anbindung einer LDAP-Umgebung

Legende

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

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

One Identity Manager Administrationshandbuch für die Anbindung einer LDAP-Umgebung
Aktualisiert - 29. September 2023, 04:36 Uhr

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

Inhalt

Über dieses Handbuch

Das *One Identity Manager Administrationshandbuch für die Anbindung einer LDAP-Umgebung* beschreibt, wie Sie die Synchronisation einer LDAP-Umgebung mit dem One Identity Manager einrichten. Sie erfahren, wie Sie mit dem One Identity Manager die Benutzerkonten und die Gruppen einer LDAP-Umgebung verwalten.

Dieses Handbuch wurde als Nachschlagewerk für End-Anwender, Systemadministratoren, Berater, Analysten und andere IT-Fachleute entwickelt.

> HINWEIS: Dieses Handbuch beschreibt die Funktionen des One Identity Manager, die für den Standardbenutzer verfügbar sind. Abhängig von der Systemkonfiguration und den Berechtigungen stehen Ihnen eventuell nicht alle Funktionen zur Verfügung.

Verfügbare Dokumentation

Die One Identity Manager Dokumentation erreichen Sie im Manager und im Designer über das Menü **Hilfe** > **Suchen**. Die Online Version der One Identity Manager Dokumentation finden Sie im Support-Portal unter Online-Dokumentation. Videos mit zusätzlichen Informationen finden Sie unter www.YouTube.com/OneIdentity.

Verwalten einer LDAP-Umgebung

Der One Identity Manager gestattet die Administration der in einem LDAP Verzeichnis verwalteten Objekte, wie beispielsweise Identitäten, 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 Identitäten 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 Identitäten eines Unternehmens mit den benötigten Benutzerkonten zu versorgen, können unterschiedliche Mechanismen für die Verbindung der Identitäten mit ihren Benutzerkonten genutzt werden. Ebenso können die Benutzerkonten getrennt von Identitäten 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.

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

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

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

Konfigurationsparameter für die Verwaltung von LDAP-Umgebungen

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

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

Weitere Informationen finden Sie unter Konfigurationsparameter für die Verwaltung einer LDAP-Umgebung auf Seite 193.

3

Synchronisieren eines LDAP Verzeichnisses

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

HINWEIS:

- Der LDAP Konnektor erfordert, dass sich die Verzeichnisserver RFC-konform verhalten. Insbesondere sind die Anforderung von RFC 4514 (Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names) und RFC 4512 (Lightweight Directory Access Protocol (LDAP): Directory Information Models) zu gewährleisten.
- Auf einigen LDAP Systemen können Schreiboperationen auf Einträge, die nicht RFC-konform sind, Fehlerzustände verursachen.
- Der angebundene LDAP Server sollte die referentielle Integrität von Einträgen selbst verwalten. Ein Beispiel wäre das `Refint`-Plugin von OpenLDAP (Overlays: Referential Integrity). Unterstützt der Server diese Mechanismen nicht oder sind diese nicht aktiviert, können durch Löschung oder Namensänderungen verwaiste Einträge auf Referenzeigenschaften (beispielsweise `Member`) entstehen.

Für den Abgleich der Informationen zwischen der One Identity Manager-Datenbank und einem LDAP Verzeichnis sorgt der One Identity Manager Service.

Informieren Sie sich hier:

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

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

Detaillierte Informationen zum Thema

- Einrichten der Initialsynchronisation mit einem LDAP Verzeichnis auf Seite 16
- Anpassen der Synchronisationskonfiguration für LDAP-Umgebungen auf Seite 39
- Ausführen einer Synchronisation auf Seite 57
- Fehleranalyse auf Seite 64
- Datenfehler bei der Synchronisation ignorieren auf Seite 65

Einrichten der Initialsynchronisation mit einem LDAP Verzeichnis

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

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

HINWEIS: Bei Objekten, die aus verschiedenen Verzeichnisdiensten importiert werden, und in der One Identity Manager-Datenbank den identischen kanonischen Namen und definierten Namen besitzen, kann es zu doppelten Anzeigewerten in laufenden Attestierungen, beispielsweise bei Systemberechtigungen, und in Berichten über Zielsystemobjekten und Zielsystemberechtigungen kommen. Gegebenenfalls müssen kundenspezifische Anpassungen an den Attestierungsverfahren und Berichten vorgenommen werden.

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.

      HINWEIS: Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und

Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.

- Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.

3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Detaillierte Informationen zum Thema

- Benutzer und Berechtigungen für die Synchronisation mit einem LDAP Verzeichnis auf Seite 17
- Besonderheiten für die Synchronisation eines Active Directory Lightweight Directory Services auf Seite 19
- Besonderheiten für die Synchronisation mit Oracle Directory Server Enterprise Edition auf Seite 20
- Einrichten des LDAP Synchronisationsservers auf Seite 21
- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer LDAP Domäne auf Seite 25
- Konfigurationsparameter für die Verwaltung einer LDAP-Umgebung auf Seite 193
- Standardprojektvorlagen für LDAP auf Seite 198
- Einstellungen des LDAP Konnektors V2 auf Seite 202

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

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

Verwandte Themen

- Besonderheiten für die Synchronisation eines Active Directory Lightweight Directory Services auf Seite 19
- Besonderheiten für die Synchronisation mit Oracle Directory Server Enterprise Edition auf Seite 20

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=Domain,DC=com`

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@<domain.com>`

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=Domain,DC=com`
- Als Kennwort für die Anmeldung ist das Kennwort des Benutzerkontos anzugeben, auf welches das AD LDS Proxyobjekt verweist.

Besonderheiten für die Synchronisation mit Oracle Directory Server Enterprise Edition

Oracle Directory Server Enterprise Edition (DSEE) unterstützt keine seitenweise Suche. Aus diesem Grund muss der Konnektor in der Lage sein, die Liste der zu synchronisierenden Objekte eines Schematyps komplett auf einmal zu laden. Bei der Verwendung eines herkömmlichen Oracle DSEE LDAP Benutzers werden in größeren Verzeichnissen serverseitige Limits erreicht, die einen solchen Ladeversuch fehlschlagen lassen.

Mögliche Meldung:

```
Size Limit exceeded

Time Limit exceeded
```

Aus diesem Grund müssen diese Limits für den Synchronisationsbenutzer entfernt werden. Hierzu sind im Verzeichnis am Benutzer für die Synchronisation folgende LDAP Attribute zu setzen:

- `nsTimeLimit`: Maximale Abfragezeit für eine Suchanfrage in Sekunden. Dieser Wert kann je nach Größe des Verzeichnisses erhöht oder verringert werden. (Empfehlung: **7200**)
- `nsSizeLimit`: Maximale Anzahl von Suchergebnissen für eine Suchanfrage. Dieser Wert kann je nach Größe des Verzeichnisses erhöht oder verringert werden. (Empfehlung: **500000**)

Einrichten des LDAP Synchronisationsservers

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

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

Detaillierte Informationen zum Thema

- Systemanforderungen für den LDAP Synchronisationsserver auf Seite 21
- One Identity Manager Service mit LDAP Konnektor installieren auf Seite 22

Systemanforderungen für den LDAP Synchronisationsserver

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 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- Microsoft .NET Framework Version 4.8 oder höher

  | HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.

One Identity Manager Service mit LDAP Konnektor installieren

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.

Tabelle 3: Eigenschaften des Jobservers

Eigenschaft	Wert
Serverfunktion	LDAP Konnektor
Maschinenrolle	Server | Job Server | LDAP directories

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

Um einen Jobserver einzurichten, führen Sie folgende Schritte aus.

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

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

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

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

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

2. Wenn Sie mit einer verschlüsselten One Identity Manager-Datenbank arbeiten, geben Sie dem One Identity Manager Service den Datenbankschlüssel bekannt. Ausführliche Informationen zum Arbeiten mit einer verschlüsselten

One Identity Manager-Datenbank finden Sie im *One Identity Manager Installationshandbuch*.

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

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

1. Starten Sie das Programm Server Installer.

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

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

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

3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.

   a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.

      - ODER -

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

   b. Bearbeiten Sie folgende Informationen für den Jobserver.

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

        Syntax:

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

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

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

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

   Für eine direkte Verbindung zu Datenbank:

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

   Für eine Verbindung zum Anwendungsserver:

   a. Wählen Sie in der Modulliste den Eintrag **Prozessabholung**, klicken Sie die Schaltfläche **Einfügen**.
   b. Wählen Sie **AppServerJobProvider** und klicken Sie **OK**.
   c. Wählen Sie in der Modulliste **Prozessabholung > AppServerJobProvider**.
   d. Klicken Sie auf den Eintrag **Verbindungsparameter** und klicken Sie die Schaltfläche **Bearbeiten**.
   e. Erfassen Sie die Adresse (URL) zum Anwendungsserver und klicken Sie **OK**.
   f. Klicken Sie auf den Eintrag **Authentifizierungsdaten** und klicken Sie die Schaltfläche **Bearbeiten**.
   g. Wählen Sie unter **Authentifizierungsverfahren** das Authentifizierungsmodul für die Anmeldung. Abhängig vom Authentifizierungsmodul können weitere Daten, wie beispielsweise Benutzer und Kennwort erforderlich sein. Ausführliche Informationen zu den One Identity Manager-Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
   h. Klicken Sie **OK**.
7. Zur Konfiguration der Installation, klicken Sie **Weiter**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
9. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
10. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.

- **Computer**: Wählen Sie den Server über die Auswahlliste oder erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.

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

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

Angaben zum One Identity Manager Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service.

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

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

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

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer 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. Ausführliche Informationen zur Einrichtung der Synchronisation finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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

Verwandte Themen

- Benötigte Informationen für die Erstellung eines Synchronisationsprojektes auf Seite 26
- Initiales Synchronisationsprojekt für eine LDAP Domäne mit dem LDAP Konnektor V2 erstellen auf Seite 28

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

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

Tabelle 4: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
DNS Name des LDAP Servers	IP-Adresse oder vollständiger Name des LDAP Servers, gegen den sich der Synchronisationsserver verbindet, um auf die LDAP Objekte zuzugreifen. Syntax: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Authentifizierungsart	Authentifizierungsart für die Verbindung zum Zielsystem. Als Standard wird die Authentifizierungsart **Basic** verwendet. Weitere Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library.
Kommunikationsport auf dem Server	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 17.
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

Angaben	Erläuterungen
	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. • Serverfunktion: **LDAP Konnektor** • Maschinenrolle: **Server | Job Server | LDAP directories** Weitere Informationen finden Sie unter Einrichten des LDAP Synchronisationsservers auf Seite 21.
Verbindungsdaten zur One Identity Manager-Datenbank	• Datenbankserver • Name der Datenbank • SQL Server-Anmeldung und Kennwort • Angabe, ob integrierte Windows-Authentifizierung verwendet wird Die Verwendung der integrierten Windows-Authentifizierung wird nicht empfohlen. Sollten Sie das Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung unterstützt.
Remoteverbindungsserver	Um die Synchronisation mit einem Zielsystem zu konfigurieren, muss der One Identity Manager Daten aus dem Zielsystem auslesen. Dabei kommuniziert der One Identity Manager direkt mit dem Zielsystem. Mitunter ist der direkte Zugriff von der Arbeitsstation, auf welcher der Synchronization Editor installiert ist, nicht möglich, beispielsweise aufgrund der Firewall-Konfiguration oder weil die Arbeitsstation nicht die notwendigen Hard- oder Softwarevoraussetzungen erfüllt. Wenn der direkte Zugriff von der Arbeitsstation nicht möglich ist, kann eine Remoteverbindung eingerichtet werden. Der Remoteverbindungsserver und die Arbeitsstation müssen in der selben Active Directory Domäne stehen. Konfiguration des Remoteverbindungsservers: • One Identity Manager Service ist gestartet • **RemoteConnectPlugin** ist installiert • LDAP Konnektor ist installiert Der Remoteverbindungsserver muss im

Angaben	Erläuterungen
	One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt. TIPP: Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software sowie der Berechtigungen des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie das **RemoteConnectPlugin** zusätzlich installieren. Ausführliche Informationen zum Herstellen einer Remoteverbindung finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Initiales Synchronisationsprojekt für eine LDAP Domäne mit dem LDAP Konnektor V2 erstellen

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

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

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

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

Um ein initiales Synchronisationsprojekt für 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** und klicken Sie **Starten**.

   Der Projektassistent des Synchronization Editors wird gestartet.

1. Auf der Seite **Zielsystem auswählen** wählen Sie **LDAP Konnektor (Version 2)**.
2. Auf der Startseite des Projektassistenten klicken Sie **Weiter**.
3. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.

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

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

4. Auf der Seite **Verbindungsinformationen** erfassen Sie die Verbindungsinformationen für den Zugriff auf das LDAP System. Es wird anschließend versucht eine Verbindung zum Server aufzubauen.
   - **Server**: IP-Adresse oder vollständiger Name des LDAP Servers, gegen den sich der Synchronisationsserver verbindet, um auf die LDAP Objekte zuzugreifen.
   - **Port**: Kommunikationsport auf dem Server. LDAP Standard-Kommunikationsport ist Port **389**.
   - **Authentifizierungsmethode**: Wählen Sie die Authentifizierungsart für die Anmeldung am LDAP System. Zulässig sind:
     - **Basic**: Die Standardauthentifizierung wird verwendet.
     - **Negotiate**: Die Negotiate-Authentifizierung von Microsoft wird verwendet.
     - **Anonymous**: Die Verbindung erfolgt ohne Übergabe von Anmeldeinformationen.
     - **Kerberos**: Die Kerberos-Authentifizierung wird verwendet.
     - **NTLM**: Die Windows NT-Abfrage/Rückmeldung-Authentifizierung wird verwendet.
     - **External**: Als externe Methode wird die zertifikatsbasierte Authentifizierung verwendet.

     Abhängig von der gewählten Authentifizierungsmethode können weitere Informationen für die Anmeldung erforderlich sein.
     - **Benutzername**: Name des Benutzerkontos zur Anmeldung am LDAP.
     - **Kennwort**: Kennwort zum Benutzerkonto.
     - **Sealing aktivieren**: Aktivieren Sie die Option, wenn die gewählte Authentifizierungsmethode die Nachrichtenvertraulichkeit (**Sealing**) unterstützt.
     - **Signing aktivieren**: Aktivieren Sie die Option, wenn die gewählte Authentifizierungsmethode die Nachrichtenintegrität (**Signing**) unterstützt.
     - **Clientzertifikat**: Wählen Sie ein Zertifikat. Die Zertifikate werden aus den Benutzerzertifikaten (Zertifikatsspeicher **Aktueller Benutzer**) des Hosts ermittelt, auf den aktuell verbunden wurde. Dies ist entweder der lokale Computer auf dem der Synchronization Editor gestartet wurde

oder der Jobserver, zu dem eine Remoteverbindung hergestellt wurde.

HINWEIS: Stellen Sie sicher, dass das gewählte Zertifikat auch auf allen Jobservern installiert ist, die sich gegen das LDAP System verbinden sollen.

TIPP: Über neben dem Eingabefeld werden zusätzliche Informationen zum gewählten Zertifikat angezeigt, beispielsweise Subjekt, Zertifizierungsstelle und Gültigkeitszeitraum.

- **Verschlüsselung**: Legen Sie die Verschlüsselung für die Verbindung fest. Zur Auswahl stehen:
  - **None**: Es wird keine Verschlüsselung verwendet.
  - **SSL**: Es wird eine SSL/TLS verschlüsselte Verbindung verwendet.
  - **StartTLS**: Es wird StartTLS zur Verschlüsselung verwendet.
- **Prüfung Serverzertifikat**: Gibt an, ob bei der Verschlüsslung mittels SSL oder StartTLS das Serverzertifikat geprüft werden soll.

  HINWEIS: Das Serverzertifikat muss gültig sein. Das Zertifikat der Stammzertifizierungsstelle muss als Computerzertifikat (Zertifikatsspeicher **Lokaler Computer**) auf dem Host, auf dem der Synchronization Editor gestartet wurde oder auf dem Jobserver, zu dem eine Remoteverbindung hergestellt wurde, vorhanden sein. Stellen Sie sicher, dass das Zertifikat auch auf allen Jobservern installiert ist, die sich gegen das LDAP System verbinden sollen.
- **Protokollversion**: Version des LDAP Protokolls. Standardwert ist **3**.

5. Auf der Seite **Auswahl der Schemaquelle** wählen Sie die Quelle für die Bereitstellung des Schemainformationen. Zur Auswahl stehen:
   - **Load schema from LDAP Server**: Das Schema wird vom LDAP Server geladen. (Standard)
   - **Load schema from given LDIF string**: Falls das Schema des LDAP Servers nicht verfügbar ist, können Sie eine alternative Quelle angeben.

Um das Schema des Servers zu laden (Standard)

1. Wählen Sie in der Auswahlliste **Quelle** den Eintrag **Load schema from LDAP Server**.
2. (Optional) Klicken Sie .
3. (Optional) Um das Schema zu prüfen, klicken Sie .

   Fehler, die beim Analysieren des Schemas gefunden werden, werden im Bereich **Schema Parserfehler** angezeigt.

Um das Schema aus einer LDIF Zeichenkette zu laden

1. Wählen Sie unter **Quelle** den Eintrag **Load schema from given LDIF string**.

2. Erfassen Sie unter **Eindeutige Kennung** eine Bezeichnung für die Schemaquelle.
3. Fügen Sie die Schemadefinition direkt in das Eingabefeld ein.

   - ODER -

   Klicken Sie und wählen Sie die Datei, die das Schema enthält.
4. Um das Schema zu prüfen, klicken Sie .

   Fehler, die beim Analysieren des Schemas gefunden werden, werden im Bereich **Schema Parserfehler** angezeigt. Mit Doppelklick auf eine Fehlermeldung wird zur entsprechenden Stelle in Schema gesprungen.

6. Auf der Seite **Konfigurationsvoreinstellung wählen** legen Sie fest, wie die Vorkonfiguration des Konnektors erfolgen soll. Anhand des erkannten Servers wird bereits eine Vorkonfiguration vorgeschlagen. Alternative können Sie die Konfiguration manuell vornehmen. In diesem Fall konfigurieren Sie Einstellungen für die Suchanfragen, die Änderung von Objekten und das Löschen von Objekten.
   - **Konfigurationsvoreinstellungen verwenden**: Aktivieren Sie diese Option, wenn Sie eine der vorhandenen Konfiguration für den Konnektor verwenden möchten. Anhand des erkannten LDAP Systems wird bereits eine Vorkonfiguration vorgeschlagen. Zur Auswahl stehen:
     - OpenDJ
     - Oracle DSEE
     - Microsoft AD LDS oder Active Directory
     - Novell/NetIQ eDirectory
   - **Manuell konfigurieren**: Aktivieren Sie diese Option, wenn Sie die Konfiguration manuell erstellen möchten. In diesem Fall werden zusätzliche Seiten angeboten, auf denen Sie die Einstellungen für die Suchanfragen, die Änderung von Objekten und das Löschen von Objekten festlegen.

     1. Auf der Seite **Sucheinstellungen** nehmen Sie die Einstellungen für LDAP Suchanfragen vor.

        Die Suchfunktionen sind hierarchisch aufgebaut und werden in der konfigurierten Reihenfolge ausgeführt. Jede Suchfunktion wird auf das Ergebnis der vorherigen Suchfunktion angewendet. Folgende Suchfunktionen stehen zur Verfügung:
        - **Default Searcher**: Standardsucheinstellungen.
          - **Verwende seitenweise Suche**: Gibt an, ob die LDAP Objekte seitenweise geladen werden sollen. Diese Information wird automatisch durch die gewählte Vorkonfiguration ermittelt oder vom LDAP Server abgefragt. Wenn die Option aktiviert ist, erfassen Sie die Seitengröße.

        - **Seitengröße**: Erfassen Sie die Anzahl der maximal zu ladenden Objekte pro Seite. (Standard **500**)
    - **Remove spaces in distinguished names**: Entfernt alle laut RFC nicht erlaubten oder nicht signifikanten Leerzeichen in definierten Namen von Objekten.

      Wenn die Funktion nicht vorhanden ist, werden laut RFC nicht erlaubten oder nicht signifikanten Leerzeichen in definierten Namen nicht entfernt und führen unter Umständen zu Fehlern.
    - **AD (LDS) Search implementation**: Zusätzliche Sucheinstellungen für Active Directory Lightweight Directory Service.
        - **Segmentgröße**: Wenn Attribute mit einer großen Anzahl Werte von einem Microsoft basierenden LDAP Server zurückgegeben werden sollen, sendet der Server nur eine bestimmte Menge der Werte zurück (üblicherweise 1500). Um alle Werte abzufragen, müssen mehrere Abfragen mit einer Bereichseinschränkung gesendet werden.

          Die Segmentgröße bestimmt, wie viele Werte pro Abfrage zurückgeliefert werden sollen. Wenn die gewählte Segmentgröße größer ist, als die Maximalgröße, die der Server verarbeiten kann, wird die Segmentgröße automatisch angepasst.

          Erfassen Sie die zulässige Segmentgröße. (Standard **1000**)

Um eine Suchfunktionen einzufügen

1. Im Bereich **Sucheinstellungen** klicken Sie ✚ .
2. Wählen Sie in der Auswahlliste die gewünschte Suchfunktion und klicken Sie 🖫.

   Über ↑ und ↓ können die Reihenfolge der Suchfunktionen ändern.

Um eine Suchfunktion zu bearbeiten

- Wählen Sie im Bereich **Sucheinstellungen** die Suchfunktion und bearbeiten Sie im unteren Bereich die entsprechende Konfiguration.

Um eine Suchfunktion zu entfernen

- Wählen Sie im Bereich **Sucheinstellungen** die Suchfunktion und klicken Sie 🗑.

2. Auf der Seite **Modifikationseinstellungen** nehmen Sie zusätzliche Einstellungen zur Änderung von Objekten vor. Folgende Funktionen stehen zur Verfügung:

- **Default Modify implementation**: Standardkonfiguration für die Änderung von Objekten.
- **Tolerate 'Attribute already exists' and 'no such attribute' and retry:** Mit dieser Funktion werden bei der Änderung eines Objektes bereits im LDAP System vorhandene oder fehlende Attribute toleriert, beispielsweise bei der Aktualisierung von Gruppenmitgliedschaften. (Standard)

  Wenn die Funktion nicht vorhanden ist, führen Änderungen, die im LDAP System vorhandene oder fehlende Attribute betreffen, zu Fehlern.

Um eine Funktionen einzufügen

1. Im Bereich **Modifikationseinstellungen** klicken Sie ✚ .
2. Wählen Sie in der Auswahlliste die gewünschte Funktion und klicken Sie 💾.

Um eine Funktion zu entfernen

- Wählen Sie im Bereich **Modifikationseinstellungen** die Funktion und klicken Sie 🗑.

3. Auf der Seite **Löscheinstellungen** nehmen Sie zusätzliche Einstellungen für das Löschen von Objekten vor. Folgende Funktion steht zur Verfügung:
   - **Default delete implementation**: Standardkonfiguration für das Löschen von Objekten.
     - **Verwende DeleteTree-Control bei Löschung von Einträgen**: Gibt an, ob der LDAP Server beim Löschen das **DeleteTree**-Control senden soll, um Einträge mit untergeordneten Einträgen zu löschen. Diese Information wird automatisch durch die gewählte Vorkonfiguration ermittelt oder vom LDAP Server abgefragt.

Um eine Funktion zu bearbeiten

- Wählen Sie im Bereich **Löscheinstellungen** die Funktion und bearbeiten Sie im unteren Bereich die entsprechende Konfiguration.

7. Auf der Seite **LDAP Schemaerweiterungen** konfigurieren Sie zusätzliche Schemafunktionen, die beim Laden des Schemas ausgeführt werden.

   Die Schemafunktionen sind hierarchisch aufgebaut. Eine Schemafunktion wird immer auf ihre übergeordnete Schemafunktion angewendet. Der Konnektor verarbeitet die Schemafunktionen hierarchisch von unten nach oben. Folgende Schemafunktionen sind verfügbar:

- **Load schema from LDAP Server/Load schema for LDIF string**: Quelle, aus der das Schema ermittelt wird.
- **Return operational attributes**: Mit dieser Schemafunktion legen Sie fest, welche Attribute zusätzlich für die LDAP Objekte ermittelt werden sollen. Funktionale Attribute werden für die Verzeichnisverwaltung verwendet. Die funktionalen Attribute werden zu jeder Schemaklasse der übergeordneten Funktion hinzugefügt.

  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.
- **Auxillary class assigment**: Mit dieser Schemafunktion weisen Sie strukturellen Klassen zusätzliche Hilfsklassen zu. 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.
- **Switch type of objectclasses**: Mit dieser Schemafunktion können Sie den Typ einer Objektklasse ändern. Dies kann erforderlich sein, wenn ein nicht RFC-konformes LDAP System die Zuweisung mehrerer struktureller Objektklassen zu einem Eintrag zulässt obwohl nur eine strukturelle Klasse erlaubt ist.

  Mehrere zugewiesene strukturelle Klassen führen dazu, dass ein LDAP Eintrag nicht eindeutig einem Schematyp zugeordnet werden kann. Wurden strukturelle Objektklassen definiert, die lediglich als Eigenschaftserweiterungen dienen sollen (also **Auxiliary**-Klassen sein sollten), so kann man den Konnektor mit Hilfe dieser Einstellung dazu veranlassen, diese Objektklasse als **Auxiliary** zu betrachten.

  HINWEIS: Als **Auxiliary** konfigurierte Objektklassen werden dann nicht mehr als eigenständige Schematypen behandelt und können in Folge auch nicht separat synchronisiert werden.
- **Cache Schema**: Mit dieser Schemafunktion wird das LDAP Schema lokal im Cache gehalten. Es wird empfohlen, diese Funktion möglichst nach dem Laden des Schemas anzuordnen. 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\LdapConnector.
  ```

- **Load AD LDS schema extension**: Mit dieser Schemafunktion werden zusätzliche Informationen geladen, die für die Synchronisation eines Active Directory Lightweight Directory Services erforderlich sind.

Um eine Schemafunktion einzufügen

1. Im Bereich **LDAP Schemaerweiterungen** klicken Sie ✚ .
2. Wählen Sie in der Auswahlliste die gewünschte Schemafunktion und klicken Sie 🖫.

   Über 🡅 und 🡇 können die Reihenfolge der Schemafunktionen ändern.

Um eine Schemafunktion zu bearbeiten

- Wählen Sie im Bereich **LDAP Schemaerweiterungen** die Schemafunktion und bearbeiten Sie im unteren Bereich entsprechende Konfiguration.

Um eine Schemafunktion zu entfernen

- Wählen Sie im Bereich **LDAP Schemaerweiterungen** die Schemafunktion und klicken Sie 🗑.

8. Auf der Seite **Suchbasis** legen Sie den Wurzeleintrag (in der Regel die Domäne) fest, der als Basis für die Suchanfragen dient. Wählen Sie in der Auswahlliste **Suchbasis** einen Eintrag aus oder erfassen Sie einen Wurzeleintrag.
9. Auf der letzten Seite des Systemverbindungsassistenten können Sie die Verbindungsdaten speichern.
   - Aktivieren Sie die Option **Verbindung lokal speichern**, um die Verbindungsdaten zu speichern. Diese können Sie bei der Einrichtung weiterer Synchronisationsprojekte nutzen.
   - Um den Systemverbindungsassistenten zu beenden und zum Projektassistenten zurückzukehren, klicken Sie **Fertig**.
10. 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.
11. Der Assistent lädt das Zielsystemschema. Abhängig von der Art des Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.
12. Auf der Seite **Zielsystemzugriff einschränken** legen Sie fest, wie der Systemzugriff erfolgen soll. Zur Auswahl stehen:

Tabelle 5: Zielsystemzugriff festlegen

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

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

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

    a. Klicken Sie , um einen neuen Jobserver anzulegen.

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

    TIPP: Sie können auch einen vorhandenen Jobserver zusätzlich als Synchronisationsserver für dieses Zielsystem einsetzen.

    • Um einen Jobserver auszuwählen, klicken Sie .

Diesem Jobserver wird die passende Serverfunktion automatisch zugewiesen.

c. Klicken Sie **OK**.

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

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

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

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

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

HINWEIS:

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

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

Verwandte Themen

- Benötigte Informationen für die Erstellung eines Synchronisationsprojektes auf Seite 26
- Benutzer und Berechtigungen für die Synchronisation mit einem LDAP Verzeichnis auf Seite 17
- Besonderheiten für die Synchronisation eines Active Directory Lightweight Directory Services auf Seite 19
- Besonderheiten für die Synchronisation mit Oracle Directory Server Enterprise Edition auf Seite 20
- Einrichten des LDAP Synchronisationsservers auf Seite 21
- Synchronisationsprotokoll konfigurieren auf Seite 38
- Anpassen der Synchronisationskonfiguration für LDAP-Umgebungen auf Seite 39
- Erweiterte Schemakonfiguration mit dem LDAP Konnektor V2 auf Seite 45
- Aufgaben nach einer Synchronisation auf Seite 61

- OpenDJ Projektvorlage für den LDAP Konnektor V2 auf Seite 198
- Active Directory Lightweight Directory Services Projektvorlage für den LDAP Konnektor V2 auf Seite 199
- Oracle Directory Server Enterprise Edition Projektvorlage für den LDAP Konnektor V2 auf Seite 200
- Generische Projektvorlage für den LDAP Konnektor V2 auf Seite 200
- Einstellungen des LDAP Konnektors V2 auf Seite 202

Synchronisationsprotokoll konfigurieren

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

Um den Inhalt des Synchronisationsprotokolls für eine Systemverbindung zu konfigurieren

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

   - ODER -

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

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

Um den Inhalt des Synchronisationsprotokolls für einen Synchronisationsworkflow zu konfigurieren

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

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

6. Klicken Sie **OK**.

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 58

Anpassen der Synchronisationskonfiguration für LDAP-Umgebungen

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 primäres System zu nutzen, erstellen Sie einen Workflow mit der Synchronisationsrichtung **In das Zielsystem**.
- Um allgemeingültige Synchronisationskonfigurationen zu erstellen, die erst beim Start der Synchronisation die notwendigen Informationen über die zu synchronisierenden Objekte erhalten, können Variablen eingesetzt werden. Variablen können beispielsweise in den Basisobjekten, den Schemaklassen oder den Verarbeitungsmethoden eingesetzt werden.
- 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.
- Um zusätzliche Schemaeigenschaften zu synchronisieren, aktualisieren Sie das Schema im Synchronisationsprojekt. Nehmen Sie die Schemaerweiterungen in das Mapping auf.

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

Detaillierte Informationen zum Thema

- Synchronisation in die LDAP Domäne konfigurieren auf Seite 40
- Synchronisation verschiedener LDAP Domänen konfigurieren auf Seite 41
- Unterstützung der eduPerson-Objektklasse auf Seite 42
- Einstellungen der Systemverbindung zur LDAP Domäne ändern auf Seite 43
- Schema aktualisieren auf Seite 51
- Beschleunigung der Synchronisation durch Revisionsfilterung auf Seite 52
- Provisionierung von Mitgliedschaften konfigurieren auf Seite 53
- Einzelobjektsynchronisation konfigurieren auf Seite 55
- Beschleunigung der Provisionierung und Einzelobjektsynchronisation auf Seite 56

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

   Es wird ein Workflow mit der Synchronisationsrichtung **In das Zielsystem** angelegt.

4. Erstellen Sie eine neue Startkonfiguration. Nutzen Sie dabei den neu angelegten Workflow.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- Synchronisation verschiedener LDAP Domänen konfigurieren auf Seite 41

Synchronisation verschiedener LDAP Domänen konfigurieren

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

Voraussetzungen

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

Um ein Synchronisationsprojekt für die Synchronisation einer weiteren Domäne anzupassen

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

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

Verwandte Themen

- Synchronisation in die LDAP Domäne konfigurieren auf Seite 40

Unterstützung der eduPerson-Objektklasse

One Identity Manager unterstützt die Objektklasse **eduPerson**. Diese Objektklasse wird vorrangig in Verzeichnissen von Universitäten und Hochschulen verwendet, um die Kommunikation zwischen den Einrichtungen zu erleichtern. Ausführliche Informationen zu **eduPerson** finden Sie unter https://wiki.refeds.org/display/STAN/eduPerson.

Unterstützt werden folgende Schemaeigenschaften:

- EduPersonAffiliation
- EduPersonEntitlement
- EduPersonNickname
- EduPersonOrgDN
- EduPersonOrgUnitDN
- EduPersonPrimaryAffiliation
- EduPersonPrimaryOrgUnitDN
- EduPersonPrincipalName
- EduPersonPrincipalNamePrior
- EduPersonScopedAffiliation
- EduPersonTargetedId
- EduPersonAssurance
- EduPersonUniqueId
- EduPersonOrcId
- EduPersonAnalyticsTag

Die Schemaeigenschaften sind nicht in der Standardvorlage für Synchronisationsprojekte gemappt. Wenn Sie die Objektklasse verwenden möchten, richten Sie das Mapping im Synchronization Editor kundenspezifisch ein. Ausführliche Informationen zum Bearbeiten von Property-Mapping-Regeln im Synchronization Editor finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

Erstellen Sie bei Bedarf kundenspezifische Bildungsregeln und Formatierungsregel. Ausführliche Informationen zur Anpassung des One Identity Manager Schemas finden Sie im *One Identity Manager Konfigurationshandbuch*.

Verwandte Themen

- EduPerson-Erweiterungen für LDAP Benutzerkonten auf Seite 163

Einstellungen der Systemverbindung zur LDAP Domäne ändern

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

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

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

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

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

Detaillierte Informationen zum Thema

- Verbindungsparameter im Variablenset bearbeiten auf Seite 43
- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 44
- Erweiterte Schemakonfiguration mit dem LDAP Konnektor V2 auf Seite 45
- Einstellungen des LDAP Konnektors V2 auf Seite 202

Verbindungsparameter im Variablenset bearbeiten

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

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

Um die Verbindungsparameter in einem spezialisierten Variablenset anzupassen

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

3. Öffnen Sie die Ansicht **Verbindungsparameter**.

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

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

    - ODER -

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

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

Verwandte Themen

- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 44

Eigenschaften der Zielsystemverbindung bearbeiten

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

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

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

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

Um die erweiterten Einstellungen mit dem Systemverbindungsassistenten zu bearbeiten

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

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

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

Verwandte Themen

- Verbindungsparameter im Variablenset bearbeiten auf Seite 43

Erweiterte Schemakonfiguration mit dem LDAP Konnektor V2

Durch die Vorkonfiguration des Konnektors, die Sie im Systemverbindungsassistenten wählen können, sind bereits die erforderlichen Schemakonfigurationen eingerichtet. Sollte es in Ausnahmefällen erforderlich sein, weitere Anpassungen vorzunehmen, können Sie im Systemverbindungsassistenten die Schematypen, Schemaeigenschaften oder Methoden konfigurieren.

WICHTIG: Änderungen an der Schemakonfiguration sollten nur von erfahrenen Benutzern des Synchronization Editors und erfahrenen Systemadministratoren vorgenommen werden.

HINWEIS: Um die erweiterten Einstellungen vorzunehmen, aktivieren Sie auf der Startseite des Systemverbindungsassistenten die Option **Erweiterte Einstellungen anzeigen**.

Auf der Seite **Konnektor Schemakonfiguration** wird ein hierarchisches Metaschema mit den Schematypen, die entstehen werden, angezeigt. Sie können Schemaklassen, Methoden und Schemaeigenschaften bearbeiten, erstellen oder löschen. Die dargestellten Informationen sind an die Informationen im Synchronization Editor angelehnt.

Nutzen Sie diese Einstellungen beispielsweise um:

- festzulegen, welche Schemaeigenschaft für die Revisionsfilterung genutzt werden soll
- festzulegen, über welche Schemaeigenschaft ein Objekt eindeutig identifiziert werden kann
- bei Bedarf virtuelle Schematypen zu definieren

Implementierungen

HINWEIS: Die globalen Einstellungen für die Implementierungen für Lesen und Schreiben sind auf der Seite **Konnektor Schemakonfiguration** am Eintrag **Schema** hinterlegt.

Tabelle 6: Implementierungen

Implementierung	Bedeutung
Implementierung für Abfragen	Implementierung, die für das Abrufen von Einträgen vom LDAP Server verwendet wird. Die `DefaultQueryStrategy`-Implementierung verwendet die konfigurierte LDAP Verbindung zum Abrufen von Einträgen.
Implementierung für Typauslösung	Implementierung die LDAP Einträge inspiziert, die vom LDAP Server zurückgeliefert wurden und versucht, den entsprechenden Konnektor-Schematyp für das resultierende Konnektor-Objekt zu ermitteln. Die `DefaultSchemaTypeResolveStrategy`-Implementierung versucht, die strukturelle Objektklasse des zurückgelieferten Objektes zu bestimmen und anschließend einen Schematyp mit dem gleichen Namen zu finden
Implementierung für Lesen	Implementierung zur Konvertierung von Werten einer Schemaeigenschaft basierend auf einem LDAP Eintrag.
Referenzbehandlung	Implementierung zur Erzeugung oder Auflösung von Referenzwerten einer Schemaeigenschaft eines LDAP Eintrages. Eine Referenz in LDAP ist gewöhnlicherweise eine Eigenschaft, welche über den definierten Namen auf einen anderen Eintrag verweist.
Implementierung für Commit	Implementierung, die verwendet wird, wenn Einträge vom Konnektor auf dem LDAP Server gespeichert werden. Die `DefaultCommitStrategy`-Implementierung führt die Methoden `Insert`, `Update` oder `Delete` in Abhängigkeit vom Objektzustand aus.
Implementierung für Insert-Methode	Implementierung für die `Insert`-Methode der Schematypen. Die `DefaultInsertMethodStrategy`-Implementierung sendet `add`-Anfragen an den LDAP Server um neue Einträge zu erzeugen.
Implementierung für	Implementierung für die `Update`-Methode der Schematypen.

Implementierung	Bedeutung
Update-Methode	Die `DefaultUpdateMethodStrategy`-Implementierung sendet `modify`- und `modifydn`-Anfragen an den LDAP Server um Änderungen an vorhandenen Einträgen zu publizieren.
Implementierung für Delete-Methode	Implementierung für die `Delete`-Methode der Schematypen. Die `DefaultDeleteMethodStrategy`-Implementierung sendet `delete`-Anfragen an den LDAP Server um vorhandene Einträge zu löschen.

Handler für Schemaeigenschaften

Handler	Bedeutung
DNBackLinkPropertyHandler	Handler für Rückwärtsverweise. Der Handler sorgt für die Auslösung von Rückwärtsverweisen zwischen Schemaeigenschaften. Beispiel: Der Handler wird für die Schemaeigenschaft `Member` der Gruppe konfiguriert. Als **Eigenschaft für Rückwärtsverweise** wird die Schemaeigenschaft `MemberOf` ausgewählt. Bei der Zuweisung eines Benutzerkontos an eine Gruppen wird im Zielsystem das Benutzerkonto in der Schemaeigenschaft `Member` der Gruppe eingetragen. Der Handler ermittelt das referenzierte Objekt, in diesem Fall das Benutzerkonto und trägt in der Schemaeigenschaft `MemberOf` den Verweis auf die Gruppe ein.
MirrorPropertyHandler	Handler für Spiegeleigenschaften. Mit diesem Handler werden die Werte und Änderungen der Schemaeigenschaft, für die der Handler definiert ist, auf die unter **Spiegeleigenschaft** ausgewählte Schemaeigenschaft übertragen. Beispiel: Der Handler wird für die Schemaeigenschaft `Member` der Gruppe konfiguriert. Als **Spiegeleigenschaft** wird die Eigenschaft `equivalentToMe` ausgewählt. Bei der Zuweisung eines Benutzerkontos an eine Gruppen wird im Zielsystem das Benutzerkonto in der Schemaeigenschaft `Member` der Gruppe eingetragen. Diese Änderung wird ebenfalls in die Schemaeigenschaft `equivalentToMe` der Gruppe übernommen,

Handler	Bedeutung

RdnPropertyHandler	Der Handler behandelt die virtuelle Schemaeigenschaft `vrtEntryRDN`. Die Schemaeigenschaft `vrtEntryRDN` repräsentiert den relativen definierten Namen eines Eintrages. Der definierte Name setzt sich aus einem oder mehreren Paaren von Attributname-Attributwert-Kombinationen mit der Syntax `<Attributname>=<AttributWert> [+<Attributname>=<AttributWert>]` zusammen.
	
	Beispiele:
	
	`CN=Ben King`
	
	`OU=Sales`
	
	`CN=Clara Harris+UID=char`
	
	Der Handler sorgt beim Setzen eines Wertes für `vrtEntryRDN` dafür, dass die entsprechend referenzierten Eigenschaften des LDAP Eintrages analog gesetzt werden.
	
	Beispiele:
	
	Für den `vrtEntryRDN` mit dem Wert **CN=Ben King** wird Eigenschaft `CN` wird auf den Wert **Ben King** gesetzt.
	
	Für den `vrtEntryRDN` mit dem Wert **OU=Sales** wird die Eigenschaft `OU` wird auf den Wert **Sales** gesetzt.
	
	Für den `vrtEntryRDN` mit dem Wert **CN=Clara Harris+UID=char** wird Eigenschaft `CN` auf den Wert **Clara Harris** gesetzt, die `UID` erhält den Wert **char**.

DefaultValueModificationHandler	Der Handler sorgt dafür, dass immer mindestens ein definierter Standardwert auf eine Schemaeigenschaft geschrieben wird. Dies kann aktuell ein Freitext oder der Distinguished Namen des Objektes sein, an dem der Wert definiert ist, beispielsweise eine Gruppe. Initial und bei Änderung der Schemaeigenschaft, der der Handler zugewiesen wurde, wird eine Operation `CheckForDefaultValueAction` eingestellt. Der Handler sorgt für folgendes Verhalten: • Wenn das Objekt gerade neu angelegt wird , wird geprüft, ob die Schemaeigenschaft einen Wert hat. Ist dies nicht der Fall, wird der Standardwert auf die Schemaeigenschaft geschrieben.

Handler	Bedeutung
	• Handelt es sich um eine Änderung, wird zunächst die Eigenschaft aus dem Zielsystem geladen. Es wird zwischen folgenden Fällen unterschieden: • Im LDAP steht der Standardwert bereits auf der Schemaeigenschaft. Durch die anstehende Änderung wird ein anderer (zusätzlicher) Wert auf die Schemaeigenschaft geschrieben. Der Standardwert wird aus der Schemaeigenschaft im LDAP entfernt und der neue Wert wird auf die Schemaeigenschaft geschrieben. • Im LDAP steht der Standardwert noch nicht auf der Schemaeigenschaft. Durch die anstehende Änderung soll die Schemaeigenschaft geleert werden, beispielsweise der letzte Wert entfernt werden. Der Standardwert wird auf die Schemaeigenschaft im LDAP geschrieben.

Um einen Schematyp zu bearbeiten

- Wählen Sie im Systemverbindungsassistenten auf der Seite **Konnektor Schemakonfiguration** im Bereich **Schema** den Schematyp aus.

  Im rechten Bereich der Ansicht werden die Eigenschaften des Schematyps angezeigt.

Um einen einfachen virtuellen Schematyp zu erstellen

1. Wählen Sie im Systemverbindungsassistenten auf der Seite **Konnektor Schemakonfiguration** im Bereich **Schema** einen Schematyp aus und klicken Sie .
2. Bearbeiten Sie die Eigenschaften des Schematyps.

Um einen virtuellen Schematyp aus mehreren Schemaklassen zu erstellen

1. Wählen Sie im Systemverbindungsassistenten auf der Seite **Konnektor Schemakonfiguration** im Bereich **Schema** die Schemaklassen, die kombiniert werden sollen mittels **Strg + Auswahl** und klicken Sie .
2. Bearbeiten Sie die Eigenschaften des Schematyps.

Um einen virtuellen Schematyp zu löschen

- Wählen Sie im Systemverbindungsassistenten auf der Seite **Konnektor Schemakonfiguration** im Bereich **Schema** einen Schematyp aus und klicken Sie .

Um eine Methode zu bearbeiten

1. Wählen Sie im Systemverbindungsassistenten auf der Seite **Konnektor Schemakonfiguration** im Bereich **Schema** den Schematyp.
2. Wählen Sie unter **Methods** die Methode.

   Im rechten Bereich der Ansicht werden die Eigenschaften der Methode angezeigt.

Um eine Methode zu erstellen

1. Wählen Sie im Systemverbindungsassistenten auf der Seite **Konnektor Schemakonfiguration** im Bereich **Schema** den Schematyp.
2. Wählen Sie den Eintrag **Methods** und klicken Sie .
3. Bearbeiten Sie die Eigenschaften der Methode.

Um eine Methode zu löschen

1. Wählen Sie im Systemverbindungsassistenten auf der Seite **Konnektor Schemakonfiguration** im Bereich **Schema** den Schematyp.
2. Wählen Sie unter **Methods** die Methode und klicken Sie .

Um eine Schemaeigenschaft zu bearbeiten

1. Wählen Sie im Systemverbindungsassistenten auf der Seite **Konnektor Schemakonfiguration** im Bereich **Schema** den Schematyp.
2. Wählen Sie unter **Properties** die Schemaeigenschaft.

   Im rechten Bereich der Ansicht werden die Attribute der Schemaeigenschaft angezeigt.

Um eine virtuelle Schemaeigenschaft zu erstellen

1. Wählen Sie im Systemverbindungsassistenten auf der Seite **Konnektor Schemakonfiguration** im Bereich **Schema** den Schematyp.
2. Wählen Sie den Eintrag **Properties** und klicken Sie .
3. Bearbeiten Sie die Details der Schemaeigenschaft.

Um eine virtuelle Schemaeigenschaft zu löschen

1. Wählen Sie im Systemverbindungsassistenten auf der Seite **Konnektor Schemakonfiguration** im Bereich **Schema** den Schematyp.
2. Wählen Sie unter **Properties** die Schemaeigenschaft und klicken Sie .

Verwandte Themen

- Eigenschaften der Zielsystemverbindung bearbeiten auf Seite 44
- Einstellungen des LDAP Konnektors V2 auf Seite 202

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

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

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

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

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

Um die Revisionsfilterung an einem Workflow zuzulassen

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

Um die Revisionsfilterung an einer Startkonfiguration zuzulassen

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

HINWEIS: 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*.

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 Gruppe (`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. Wählen Sie im Manager die Kategorie **LDAP > Basisdaten zur Konfiguration > Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **LDAP**.
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.
5. Klicken Sie **Merge-Modus**.

HINWEIS:

- Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte `XDateSubItem` hat.
- Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden.

  Beispiel: `LDAPAccountInLDAPGroup`, `LDAPGroupInLDAPGroup` und `LDAPMachineInLDAPGroup`

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. Dabei werden nur die neu eingefügten und gelöschten Zuordnungen verarbeitet. Bei der Provisionierung der Änderungen wird die Mitgliederliste im Zielsystem mit den Einträgen in dieser Tabelle abgeglichen. Damit wird nicht die gesamte Mitgliederliste überschrieben, sondern nur die einzelne geänderte Mitgliedschaft provisioniert.

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

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

Um die originale Bedingung wiederherzustellen

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

HINWEIS: Um in der Bedingung den Bezug zu den eingefügten oder gelöschten Zuordnungen herzustellen, nutzen Sie den Tabellenalias `i`.

Beispiel für eine Bedingung an der Zuordnungstabelle `LDAPAccountInLDAPGroup`:

```
exists (select top 1 1 from LDAPGroup g
     where g.UID_LDAPGroup = i.UID_LDAPGroup
     and <einschränkende Bedingung>)
```

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

Einzelobjektsynchronisation konfigurieren

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

Voraussetzungen

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

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

Um den Pfad zum Basisobjekt der Synchronisation für eine kundenspezifische Tabelle festzulegen

1. Wählen Sie im Manager 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 kundenspezifische Tabelle zu, für die Sie die Einzelobjektsynchronisation nutzen möchten.
5. Speichern Sie die Änderungen.
6. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
7. Wählen Sie die kundenspezifische Tabelle und erfassen Sie den **Pfad zum Basisobjekt**.

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

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

Verwandte Themen

- Einzelobjekte synchronisieren auf Seite 60
- Ausstehende Objekte nachbehandeln auf Seite 61

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

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

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

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

Um die Lastverteilung zu konfigurieren

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

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

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

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

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

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

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

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Detaillierte Informationen zum Thema

- LDAP Jobserver bearbeiten auf Seite 185

Ausführen einer Synchronisation

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

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

Detaillierte Informationen zum Thema

- Synchronisationen starten auf Seite 57
- Synchronisation deaktivieren auf Seite 59
- Synchronisationsergebnisse anzeigen auf Seite 58
- Einzelobjekte synchronisieren auf Seite 60
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 66

Synchronisationen starten

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

Um regelmäßige Synchronisationen auszuführen

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

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

Um die initiale Synchronisation manuell zu starten

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

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

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

Synchronisationsergebnisse anzeigen

Die Ergebnisse der Synchronisation werden im Synchronisationsprotokoll zusammengefasst. Der Umfang des Synchronisationsprotokolls kann für jede Systemverbindung separat festgelegt werden. Der One Identity Manager stellt

verschiedene Berichte bereit, in denen die Synchronisationsergebnisse nach verschiedenen Kriterien aufbereitet sind.

Um das Protokoll einer Synchronisation anzuzeigen

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

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

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

Um das Protokoll einer Provisionierung anzuzeigen

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

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

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

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

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

Verwandte Themen

- Synchronisationsprotokoll konfigurieren auf Seite 38
- Fehleranalyse auf Seite 64

Synchronisation deaktivieren

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

Um regelmäßige Synchronisationen zu verhindern

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

Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Detaillierte Informationen zum Thema

- Erstellen eines Synchronisationsprojektes für die initiale Synchronisation einer LDAP Domäne auf Seite 25
- Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus) auf Seite 66

Einzelobjekte synchronisieren

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

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

Um ein Einzelobjekt zu synchronisieren

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

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

Besonderheiten bei der Synchronisation von Mitgliederlisten

Wenn Sie Änderungen in der Mitgliederliste eines Objekts synchronisieren, führen Sie die Einzelobjektsynchronisation am Basisobjekt der Zuweisung aus. Die Basistabelle einer Zuordnung enthält eine Spalte `XDateSubItem` mit der Information über die letzte Änderung der Mitgliedschaften.

Beispiel:

Basisobjekt für die Zuweisung von Benutzerkonten an Gruppen ist die Gruppe.

Im Zielsystem wurde ein Benutzerkonto an eine Gruppe zugewiesen. Um diese Zuweisung zu synchronisieren, wählen Sie im Manager die Gruppe, der das Benutzerkonto zugewiesen wurde, und führen Sie die Einzelobjektsynchronisation aus. Dabei werden alle Mitgliedschaften für diese Gruppe synchronisiert.

Das Benutzerkonto muss in der One Identity Manager-Datenbank bereits als Objekt vorhanden sein, damit die Zuweisung angelegt werden kann.

Detaillierte Informationen zum Thema

- Einzelobjektsynchronisation konfigurieren auf Seite 55

Aufgaben nach einer Synchronisation

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

- Ausstehende Objekte nachbehandeln auf Seite 61
- Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen auf Seite 63
- LDAP Benutzerkonten über Kontendefinitionen verwalten auf Seite 64

Ausstehende Objekte nachbehandeln

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

Ausstehende Objekte

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

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

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

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

   In der Navigationsansicht werden alle Tabellen angezeigt, die dem Zielsystemtyp **LDAP** als Synchronisationstabellen zugewiesen sind.

2. Öffnen Sie auf dem Formular **Zielsystemabgleich**, in der Spalte **Tabelle/Objekt** den Knoten der Tabelle, für die sie ausstehende Objekte nachbearbeiten möchten.

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

   - Das Synchronisationsprotokoll wurde bereits gelöscht.

     - ODER -

   - Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.

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

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

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

   TIPP:

   Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

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

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

Tabelle 7: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Indirekte Mitgliedschaften können nicht gelöscht werden.

Symbol	Methode	Beschreibung
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung **Ausstehend** wird für das Objekt entfernt. Es wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: • Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen. • Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.
	Zurücksetzen	Die Markierung **Ausstehend** wird für das Objekt entfernt.

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

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

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

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

Um den Fehler zu lokalisieren, muss die Massenverarbeitung der Objekte deaktiviert werden. Die Objekte werden damit nacheinander verarbeitet. Das fehlerhafte Objekt wird in der Fehlermeldung benannt. Alle Änderungen, die bis zum Auftreten des Fehlers vorgenommen wurden, werden gespeichert.

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularsymbolleiste das Symbol .

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

Kundenspezifische Tabellen in den Zielsystemabgleich aufnehmen

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

Um kundenspezifische Tabellen in den Zielsystemabgleich aufzunehmen

1. Wählen Sie im Manager die Kategorie **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.

Verwandte Themen

- Ausstehende Objekte nachbehandeln auf Seite 61

LDAP Benutzerkonten über Kontendefinitionen verwalten

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

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

Detaillierte Informationen zum Thema

- Kontendefinitionen an verbundene LDAP Benutzerkonten zuweisen auf Seite 98

Fehleranalyse

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

- Synchronisation simulieren

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

- Synchronisation analysieren

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

- Meldungen protokollieren

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

- Startinformation zurücksetzen

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

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

Verwandte Themen

- Synchronisationsergebnisse anzeigen auf Seite 58

Datenfehler bei der Synchronisation ignorieren

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

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

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

   Der Systemverbindungsassistent wird gestartet.

4. Auf der Seite **Weitere Einstellungen** aktivieren Sie **Versuche Datenfehler zu ignorieren**.

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

   Fehler in Standardspalten, wie Primärschlüssel oder UID-Spalten, und Pflichteingabespalten können nicht ignoriert werden.

5. Speichern Sie die Änderungen.

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

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

Verarbeitung zielsystemspezifischer Prozesse pausieren (Offline-Modus)

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

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

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

Voraussetzungen

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

- Der Synchronisationsserver wird für kein anderes Basisobjekt als Synchronisationsserver genutzt.
- Wenn dem Basisobjekt eine Serverfunktion zugewiesen ist, darf keiner der Jobserver mit dieser Serverfunktion eine andere Serverfunktion (beispielsweise Aktualisierungsserver) haben.

- Es muss ein dedizierter Synchronisationsserver eingerichtet sein, der ausschließlich die Jobqueue für dieses Basisobjekt verarbeitet. Gleiches gilt für alle Jobserver, die über die Serverfunktion ermittelt werden.

Um den Offline-Modus für ein Basisobjekt zuzulassen

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

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

Die Zahl der nachträglich zu verarbeitenden Prozesse ist abhängig vom Umfang der Änderungen in der One Identity Manager-Datenbank mit Auswirkungen auf das Zielsystem während der Offline-Phase. Um Datenkonsistenz zwischen One Identity Manager-Datenbank und Zielsystem herzustellen, müssen alle anstehenden Prozesse verarbeitet werden, bevor eine Synchronisation gestartet wird.

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

Um ein Zielsystem als offline zu kennzeichnen

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

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

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

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

Verwandte Themen

- Synchronisation deaktivieren auf Seite 59

Managen von LDAP Benutzerkonten und Identitäten

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

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

- Identitäten erhalten ihre Benutzerkonten automatisch über Kontendefinitionen.

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

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

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

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

Verwandte Themen

- Kontendefinitionen für LDAP Benutzerkonten auf Seite 70
- Automatische Zuordnung von Identitäten zu LDAP Benutzerkonten auf Seite 93
- Identitäten manuell mit LDAP Benutzerkonten verbinden auf Seite 99
- Unterstützte Typen von Benutzerkonten auf Seite 99
- Löschverzögerung für LDAP Benutzerkonten festlegen auf Seite 106
- Stammdaten von LDAP Benutzerkonten bearbeiten auf Seite 155

Kontendefinitionen für LDAP Benutzerkonten

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

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

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

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

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

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

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

Detaillierte Informationen zum Thema

- Kontendefinitionen erstellen auf Seite 71
- Kontendefinitionen bearbeiten auf Seite 72
- Stammdaten für Kontendefinitionen auf Seite 72
- Automatisierungsgrade bearbeiten auf Seite 75
- Automatisierungsgrade erstellen auf Seite 76
- Stammdaten für Automatisierungsgrade auf Seite 77
- Abbildungsvorschrift für IT Betriebsdaten erstellen auf Seite 78
- IT Betriebsdaten erfassen auf Seite 80
- IT Betriebsdaten ändern auf Seite 81
- Zuweisen der Kontendefinitionen an Identitäten auf Seite 82
- Kontendefinitionen an LDAP Domänen zuweisen auf Seite 90
- Kontendefinitionen löschen auf Seite 90

Kontendefinitionen erstellen

Erstellen Sie eine oder mehrere Kontendefinitionen für das Zielsystem.

Um eine Kontendefinition zu erstellen

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

Detaillierte Informationen zum Thema

- Stammdaten für Kontendefinitionen auf Seite 72
- Kontendefinitionen bearbeiten auf Seite 72
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 77

Kontendefinitionen bearbeiten

Sie können die Stammdaten der Kontendefinitionen bearbeiten.

Um eine Kontendefinition zu bearbeiten

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

Verwandte Themen

- Stammdaten für Kontendefinitionen auf Seite 72
- Kontendefinitionen erstellen auf Seite 71
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 77

Stammdaten für Kontendefinitionen

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 8: 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	Angabe der vorausgesetzten Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch 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

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

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

Eigenschaft	Beschreibung
	• Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität diese Gruppe nur, wenn die Option aktiviert ist.

Automatisierungsgrade bearbeiten

One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

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

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

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

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

Identitäten berechnet werden. Bestehende Gruppenmitgliedschaften werden dann gelöscht!

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie im Manager die Kategorie **LDAP > Basisdaten zur Konfiguration > Kontendefinitionen > Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
5. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten für Automatisierungsgrade auf Seite 77
- Automatisierungsgrade erstellen auf Seite 76
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 77

Automatisierungsgrade erstellen

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

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

Um einen Automatisierungsgrad zu erstellen

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

Verwandte Themen

- Stammdaten für Automatisierungsgrade auf Seite 77
- Automatisierungsgrade bearbeiten auf Seite 75
- Automatisierungsgrade an Kontendefinitionen zuweisen auf Seite 77

Automatisierungsgrade an Kontendefinitionen zuweisen

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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **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.

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

   Um eine Zuweisung zu entfernen

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

Stammdaten für Automatisierungsgrade

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 9: Stammdaten eines Automatisierungsgrades

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

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

Abbildungsvorschrift für IT Betriebsdaten erstellen

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

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

- LDAP Container
- Gruppen erbbar

- Identität
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

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

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

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

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

Verwandte Themen

- IT Betriebsdaten erfassen auf Seite 80
- IT Betriebsdaten ändern auf Seite 81

IT Betriebsdaten erfassen

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

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

Beispiel:

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

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

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

Um IT Betriebsdaten festzulegen

1. Wählen Sie im Manager in der Kategorie **Organisationen** oder **Geschäftsrollen** die Rolle.
2. Wählen Sie die Aufgabe **IT Betriebsdaten bearbeiten**.
3. Klicken Sie **Hinzufügen** und erfassen Sie die folgenden Daten.

- **Wirksam für**: Legen Sie den Anwendungsbereich der IT Betriebsdaten fest. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.

  Um den Anwendungsbereich festzulegen

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

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

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

  d. Klicken Sie **OK**.

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

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

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

4. Speichern Sie die Änderungen.

Verwandte Themen

- Abbildungsvorschrift für IT Betriebsdaten erstellen auf Seite 78
- IT Betriebsdaten ändern auf Seite 81

IT Betriebsdaten ändern

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

Voraussetzungen

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

  - ODER -

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

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

Um die Bildungsregeln auszuführen

1. Wählen Sie im Manager die Kategorie **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. Es bedeuten:

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

   Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinitionen an Identitäten

Kontendefinitionen werden an die Identitäten des Unternehmens zugewiesen.

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

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

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

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Identitäten

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

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

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

   - ODER -

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

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

Detaillierte Informationen zum Thema

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 84
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 84
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 85

- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 86
- Kontendefinitionen an Systemrollen zuweisen auf Seite 87
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 88

Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen

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

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **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.

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

    Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 84
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 85
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 86
- Kontendefinitionen an Systemrollen zuweisen auf Seite 87
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 88

Kontendefinitionen an Geschäftsrollen zuweisen

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

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

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 84
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 85
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 86
- Kontendefinitionen an Systemrollen zuweisen auf Seite 87
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 88

Kontendefinitionen an alle Identitäten zuweisen

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

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

Um eine Kontendefinition an alle Identitäten zuzuweisen

1. Wählen Sie im Manager die Kategorie **LDAP > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.

3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie die Aufgabe **Automatische Zuweisung zu Identitäten aktivieren**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Speichern Sie die Änderungen.

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

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 84
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 84
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 86
- Kontendefinitionen an Systemrollen zuweisen auf Seite 87
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 88

Kontendefinitionen direkt an Identitäten zuweisen

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

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

Um eine Kontendefinition direkt an Identitäten zuzuweisen

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 84
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 84
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 85
- Kontendefinitionen an Systemrollen zuweisen auf Seite 87
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 88

Kontendefinitionen an Systemrollen zuweisen

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

Mit dieser Aufgabe nehmen Sie eine Kontendefinition in Systemrollen auf.

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 84
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 84
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 85
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 86
- Kontendefinitionen in den IT Shop aufnehmen auf Seite 88

Kontendefinitionen in den IT Shop aufnehmen

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

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

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

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

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

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

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

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

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

1. Wählen Sie im Manager die Kategorie **Berechtigungen > Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

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

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

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

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

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

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

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

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

Verwandte Themen

- Stammdaten für Kontendefinitionen auf Seite 72
- Kontendefinitionen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 84
- Kontendefinitionen an Geschäftsrollen zuweisen auf Seite 84
- Kontendefinitionen an alle Identitäten zuweisen auf Seite 85
- Kontendefinitionen direkt an Identitäten zuweisen auf Seite 86
- Kontendefinitionen an Systemrollen zuweisen auf Seite 87

Kontendefinitionen an LDAP Domänen zuweisen

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **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 Identitäten zu LDAP Benutzerkonten auf Seite 93

Kontendefinitionen löschen

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

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Identitäten.
    a. Wählen Sie im Manager die Kategorie **LDAP > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
    d. Wählen Sie die Aufgabe **Automatische Zuweisung zu Identitäten deaktivieren**.
    e. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
    f. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Identitäten.
    a. Wählen Sie im Manager die Kategorie **LDAP > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **An Identitäten zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Identitäten.
    e. Speichern Sie die Änderungen.
3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorten.
    a. Wählen Sie im Manager die Kategorie **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 im Manager die Kategorie **LDAP > Basisdaten zur Konfiguration > Kontendefinitionen > Kontendefinitionen**.
    b. Wählen Sie in der Ergebnisliste die Kontendefinition.
    c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
    d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
    e. Speichern Sie die Änderungen.
5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden.

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

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

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

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

e. Klicken Sie **OK**.

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

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

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

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

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

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

e. Klicken Sie **OK**.

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

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

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

b. Wählen Sie in der Ergebnisliste die Kontendefinition.

c. Klicken Sie , um die Kontendefinition zu löschen.

Automatische Zuordnung von Identitäten zu LDAP Benutzerkonten

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

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

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

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

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

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

- Wenn Identitäten bei der Synchronisation von Benutzerkonten zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | LDAP | PersonAutoFullsync** und wählen Sie den gewünschte Modus.

- Wenn Identitäten außerhalb der Synchronisation zugeordnet werden sollen, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | LDAP | PersonAutoDefault** und wählen Sie den gewünschten Modus.
- Legen Sie über den Konfigurationsparameter **TargetSystem | LDAP | PersonAutoDisabledAccounts** fest, ob an deaktivierte Benutzerkonten automatisch Identitäten zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
- Weisen Sie der Domäne eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Identitätenzuordnung an der Domäne.

HINWEIS:

Für die Synchronisation gilt:

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

Außerhalb der Synchronisation gilt:

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

HINWEIS:

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

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

Weitere Informationen finden Sie unter LDAP Benutzerkonten über Kontendefinitionen verwalten auf Seite 64.

Verwandte Themen

- Kontendefinitionen erstellen auf Seite 71
- Kontendefinitionen an LDAP Domänen zuweisen auf Seite 90
- Automatisierungsgrade für LDAP Benutzerkonten ändern auf Seite 98
- Kontendefinitionen an verbundene LDAP Benutzerkonten zuweisen auf Seite 98
- Suchkriterien für die automatische Identitätenzuordnung bearbeiten auf Seite 95

Suchkriterien für die automatische Identitätenzuordnung bearbeiten

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

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

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

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

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

Um Kriterien für die Identitätenzuordnung festzulegen

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

   Tabelle 10: Standardsuchkriterien für Benutzerkonten

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

5. Speichern Sie die Änderungen.

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

Verwandte Themen

- Automatische Zuordnung von Identitäten zu LDAP Benutzerkonten auf Seite 93
- Identitäten suchen und direkt an Benutzerkonten zuordnen auf Seite 96

Identitäten suchen und direkt an Benutzerkonten zuordnen

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

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

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

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

Um Suchkriterien auf die Benutzerkonten anzuwenden

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

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

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

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

Um Identitäten direkt an Benutzerkonten zuzuordnen

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

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

  - ODER -

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

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

Um Zuordnungen zu entfernen

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

       Von den ausgewählten Benutzerkonten werden die zugeordneten Identitäten entfernt.

Automatisierungsgrade für LDAP Benutzerkonten ändern

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

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

1. Wählen Sie im Manager 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

- LDAP Benutzerkonten erstellen auf Seite 154

Kontendefinitionen an verbundene LDAP Benutzerkonten zuweisen

An Benutzerkonten im Zustand **Linked** (verbunden) kann nachträglich eine Kontendefinition zugewiesen werden. Das kann beispielsweise der Fall sein, wenn

- Identitäten und Benutzerkonten manuell verbunden wurden
- die automatische Identitätenzuordnung konfiguriert ist, beim Einfügen eines Benutzerkontos jedoch noch keine Kontendefinition an die Domäne zugeordnet ist

Um die Benutzerkonten über Kontendefinitionen zu verwalten

1. Erstellen Sie eine Kontendefinition.
2. Weisen Sie der Domäne die Kontendefinition zu.
3. Weisen Sie den Benutzerkonten im Zustand **Linked** (verbunden) die Kontendefinition zu. Es wird der Standardautomatisierungsgrad der Kontendefinition für das Benutzerkonto übernommen.
    a. Wählen Sie im Manager die Kategorie **LDAP > Benutzerkonten > Verbunden aber nicht konfiguriert > <Domäne>**.
    b. Wählen Sie die Aufgabe **Kontendefinition an verbundene Benutzerkonten zuweisen**.

c. Wählen Sie in der Auswahlliste **Kontendefinition** die Kontendefinition.
d. Wählen Sie die Benutzerkonten, die die Kontendefinition erhalten sollen.
e. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- Kontendefinitionen an LDAP Domänen zuweisen auf Seite 90

Identitäten manuell mit LDAP Benutzerkonten verbinden

Eine Identität kann mit mehreren LDAP Benutzerkonten verbunden werden, beispielsweise um zusätzlich zum Standardbenutzerkonto ein administratives Benutzerkonto zuzuweisen. Darüber hinaus kann eine Identität Standardbenutzerkonten mit verschiedenen Typen nutzen.

Um einer Identität manuell Benutzerkonten zuzuweisen

1. Wählen Sie im Manager die Kategorie **Identitäten > Identitäten**.
2. Wählen Sie in der Ergebnisliste die Identität und führen Sie die Aufgabe **LDAP Benutzerkonten zuweisen**.
3. Weisen Sie die Benutzerkonten zu.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Unterstützte Typen von Benutzerkonten auf Seite 99
- LDAP Benutzerkonten erstellen auf Seite 154

Unterstützte Typen von Benutzerkonten

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

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identitätstyp

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

  Tabelle 11: Identitätstypen von Benutzerkonten

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

- Privilegiertes Benutzerkonto

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

Detaillierte Informationen zum Thema

- Standardbenutzerkonten auf Seite 101
- Administrative Benutzerkonten auf Seite 102
- Administrative Benutzerkonten für eine Identität bereitstellen auf Seite 102
- Administrative Benutzerkonten für mehrere Identitäten bereitstellen auf Seite 103
- Privilegierte Benutzerkonten auf Seite 104

Standardbenutzerkonten

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

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

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

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

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

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

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

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

Verwandte Themen

- Kontendefinitionen für LDAP Benutzerkonten auf Seite 70

Administrative Benutzerkonten

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

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

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

Verwandte Themen

- Administrative Benutzerkonten für eine Identität bereitstellen auf Seite 102
- Administrative Benutzerkonten für mehrere Identitäten bereitstellen auf Seite 103

Administrative Benutzerkonten für eine Identität bereitstellen

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

Voraussetzungen

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

Um ein administratives Benutzerkonto für eine Identität bereitzustellen

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

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

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

Verwandte Themen

- Administrative Benutzerkonten für mehrere Identitäten bereitstellen auf Seite 103
- Ausführliche Informationen zur Abbildung von Identitätstypen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administrative Benutzerkonten für mehrere Identitäten bereitstellen

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

Voraussetzung

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

Um ein administratives Benutzerkonto für mehrere Identitäten bereitzustellen

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

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

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

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

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

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

b. Wählen Sie in der Ergebnisliste das Benutzerkonto.

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

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Identität und doppelklicken Sie .

Verwandte Themen

- Administrative Benutzerkonten für eine Identität bereitstellen auf Seite 102
- Ausführliche Informationen zur Abbildung von Identitätstypen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Privilegierte Benutzerkonten

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

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

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

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

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

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

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

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

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

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

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

- 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** (Spalte `IsPrivilegedAccount`) kennzeichnen. Die Anmeldenamen der Benutzerkonten werden entsprechend der Bildungsregeln umbenannt. Dies erfolgt auch, wenn die Benutzerkonten über den Zeitplan **Ausgewählte Benutzerkonten als privilegiert kennzeichnen** als privilegiert gekennzeichnet werden. Passen Sie bei Bedarf den Zeitplan im Designer an.

Verwandte Themen

- Kontendefinitionen für LDAP Benutzerkonten auf Seite 70

Löschverzögerung für LDAP Benutzerkonten festlegen

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

Sie haben die folgenden Möglichkeiten die Löschverzögerung zu konfigurieren.

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

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

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

  Beispiel:

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

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

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

Managen von Mitgliedschaften in LDAP Gruppen

LDAP Benutzerkonten und LDAP Computer können in LDAP Gruppen zusammengefasst werden, mit denen der Zugriff auf Ressourcen geregelt werden kann.

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

Detaillierte Informationen zum Thema

- Zuweisen von LDAP Gruppen an LDAP Benutzerkonten und LDAP Computer im One Identity Manager auf Seite 108
- Wirksamkeit von Mitgliedschaften in LDAP Gruppen auf Seite 120
- Vererbung von LDAP Gruppen anhand von Kategorien auf Seite 123
- Übersicht aller Zuweisungen auf Seite 125

Zuweisen von LDAP Gruppen an LDAP Benutzerkonten und LDAP Computer im One Identity Manager

LDAP Gruppen können direkt oder indirekt an LDAP Benutzerkonten und LDAP Computer zugewiesen werden. Bei der indirekten Zuweisung werden Identitäten (Arbeitsplätze, Geräte) und LDAP Gruppen in hierarchische Rollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung berechnet sich die Menge der LDAP Gruppen, die einer Identität (einem Arbeitsplatz oder einem Gerät) zugewiesen ist.

- Wenn Sie eine Identität in Rollen aufnehmen und die Identität ein LDAP Benutzerkonto besitzt, dann wird dieses LDAP Benutzerkonto in die LDAP Gruppen

aufgenommen.

- Wenn Sie ein Gerät in Rollen aufnehmen, dann wird der LDAP Computer, der dieses Gerät referenziert, in die LDAP Gruppen aufgenommen.
- Wenn ein Gerät einen Arbeitsplatz besitzt und Sie den Arbeitsplatz in Rollen aufnehmen, dann wird der LDAP Computer, der dieses Gerät referenziert, zusätzlich in alle LDAP Gruppen der Rollen des Arbeitsplatzes aufgenommen.

Des Weiteren können LDAP Gruppen im Web Portal bestellt werden. Dazu werden Identitäten als Kunden in einen Shop aufgenommen. Alle LDAP Gruppen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte LDAP Gruppen werden nach erfolgreicher Genehmigung den Identitäten zugewiesen.

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

Um auf Sonderanforderungen schnell zu reagieren, können Sie die LDAP Gruppen auch direkt an LDAP Benutzerkonten und LDAP Computer zuweisen.

Ausführliche Informationen finden Sie in den folgenden Handbüchern.

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

Detaillierte Informationen zum Thema

- Voraussetzungen für indirekte Zuweisungen von LDAP Gruppen auf Seite 110
- LDAP Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- LDAP Gruppen an Geschäftsrollen zuweisen auf Seite 113
- LDAP Gruppen in Systemrollen aufnehmen auf Seite 114
- LDAP Gruppen in den IT Shop aufnehmen auf Seite 115
- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 117
- LDAP Gruppen direkt an ein LDAP Benutzerkonto zuweisen auf Seite 118
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 118
- LDAP Gruppen direkt an einen LDAP Computer zuweisen auf Seite 119

Voraussetzungen für indirekte Zuweisungen von LDAP Gruppen

Bei der indirekten Zuweisung werden Identitäten und LDAP Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen eingeordnet. Für die indirekte Zuweisung von LDAP Gruppen prüfen Sie folgende Einstellungen und passen Sie die Einstellungen bei Bedarf an.

Voraussetzungen für die indirekte Zuweisung von LDAP Gruppen an die LDAP Benutzerkonten von Identitäten

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Identitäten und LDAP Gruppen erlaubt.
2. Das LDAP Benutzerkonto ist mit einer Identität verbunden.
3. Das LDAP Benutzerkonto ist mit der Option **Gruppen erbbar** gekennzeichnet.

Voraussetzungen für die indirekte Zuweisung von LDAP Gruppen an LDAP Computer

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Geräten und LDAP Gruppen erlaubt.
2. Der LDAP Computer ist mit einem Gerät verbunden.
3. Das Gerät ist als PC oder als Server gekennzeichnet.
4. Der Konfigurationsparameter **TargetSystem | LDAP | HardwareInGroupFromOrg** ist aktiviert.

Voraussetzungen für die indirekte Zuweisung von LDAP Gruppen an LDAP Computer über Arbeitsplätze

1. Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Arbeitsplätzen und LDAP Gruppen erlaubt.
2. Der LDAP Computer ist mit einem Gerät verbunden.
3. Das Gerät ist als PC oder als Server gekennzeichnet ist.
4. Das Gerät besitzt einen Arbeitsplatz.

Um die Zuweisungen zu Rollen einer Rollenklasse zu konfigurieren

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

   - ODER -

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

2. Wählen Sie die Aufgabe **Rollenzuweisungen konfigurieren** und konfigurieren Sie die erlaubten Zuweisungen.
    - Um eine Zuweisung generell zu erlauben, aktivieren Sie die Spalte **Zuweisungen erlaubt**.
    - Um die direkte Zuweisung zu erlauben, aktivieren Sie die Spalte **Direkte Zuweisungen erlaubt**.
3. Speichern Sie die Änderungen.

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

Verwandte Themen

- Stammdaten von LDAP Benutzerkonten bearbeiten auf Seite 155
- Allgemeine Stammdaten für LDAP Benutzerkonten auf Seite 155
- Stammdaten von LDAP Computern bearbeiten auf Seite 174
- Stammdaten für LDAP Computer auf Seite 175

LDAP Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen

Weisen Sie die Gruppe an Abteilungen, Kostenstellen oder Standorte zu, damit die Gruppe über diese Organisationen an Benutzerkonten und Computer zugewiesen wird. Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

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

1. Wählen Sie im Manager 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Organisation und doppelklicken Sie .

5. Speichern Sie die Änderungen.

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

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

   - ODER -

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

   - ODER -

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von LDAP Gruppen auf Seite 110
- LDAP Gruppen an Geschäftsrollen zuweisen auf Seite 113
- LDAP Gruppen in Systemrollen aufnehmen auf Seite 114
- LDAP Gruppen in den IT Shop aufnehmen auf Seite 115
- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 117
- LDAP Gruppen direkt an ein LDAP Benutzerkonto zuweisen auf Seite 118
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 118
- LDAP Gruppen direkt an einen LDAP Computer zuweisen auf Seite 119
- One Identity Manager Benutzer für die Verwaltung einer LDAP-Umgebung auf Seite 11

LDAP Gruppen an Geschäftsrollen zuweisen

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

Weisen Sie die Gruppe an Geschäftsrollen zu, damit die Gruppe über diese Geschäftsrollen an Benutzerkonten und Computer zugewiesen wird. Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

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

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

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

   Um eine Zuweisung zu entfernen

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

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

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

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von LDAP Gruppen auf Seite 110
- LDAP Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- LDAP Gruppen in Systemrollen aufnehmen auf Seite 114
- LDAP Gruppen in den IT Shop aufnehmen auf Seite 115

- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 117
- LDAP Gruppen direkt an ein LDAP Benutzerkonto zuweisen auf Seite 118
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 118
- LDAP Gruppen direkt an einen LDAP Computer zuweisen auf Seite 119
- One Identity Manager Benutzer für die Verwaltung einer LDAP-Umgebung auf Seite 11

LDAP Gruppen in Systemrollen aufnehmen

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

Mit dieser Aufgabe nehmen Sie eine Gruppe in Systemrollen auf.

Wenn Sie eine Systemrolle an Identitäten zuweisen, wird die Gruppe an alle LDAP Benutzerkonten vererbt, die diese Identitäten besitzen.

Wenn Sie die Systemrolle an Arbeitsplätze zuweisen, wird die Gruppe an den LDAP Computer vererbt, der mit diesem Arbeitsplatz verbunden ist.

Diese Aufgabe steht für dynamische Gruppen nicht zur Verfügung.

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

Um eine Gruppe an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- Voraussetzungen für indirekte Zuweisungen von LDAP Gruppen auf Seite 110
- LDAP Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- LDAP Gruppen an Geschäftsrollen zuweisen auf Seite 113
- LDAP Gruppen in den IT Shop aufnehmen auf Seite 115

- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 117
- LDAP Gruppen direkt an ein LDAP Benutzerkonto zuweisen auf Seite 118
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 118
- LDAP Gruppen direkt an einen LDAP Computer zuweisen auf Seite 119

LDAP Gruppen 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 ist keine dynamische Gruppe.
- Die Gruppe muss mit der Option **IT Shop** gekennzeichnet sein.
- Der Gruppe muss eine Leistungsposition zugeordnet sein.

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

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

Um eine Gruppe in den IT Shop aufzunehmen

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

   - ODER -

   Wählen Sie im Manager 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. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Gruppe an die IT Shop Regale zu.
6. Speichern Sie die Änderungen.

Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen

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

   - ODER -

   Wählen Sie im Manager 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. Wählen Sie den Tabreiter **IT Shop Strukturen**.
5. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
6. Speichern Sie die Änderungen.

Um eine Gruppe aus allen Regalen des IT Shops zu entfernen

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

   - ODER -

   Wählen Sie im Manager 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

- Voraussetzungen für indirekte Zuweisungen von LDAP Gruppen auf Seite 110
- Stammdaten für LDAP Gruppen auf Seite 170
- LDAP Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- LDAP Gruppen an Geschäftsrollen zuweisen auf Seite 113
- LDAP Gruppen in Systemrollen aufnehmen auf Seite 114
- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 117
- LDAP Gruppen direkt an ein LDAP Benutzerkonto zuweisen auf Seite 118
- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 118

- LDAP Gruppen direkt an einen LDAP Computer zuweisen auf Seite 119
- One Identity Manager Benutzer für die Verwaltung einer LDAP-Umgebung auf Seite 11

LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen

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

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 Benutzerkonten direkt an eine Gruppe zuzuweisen

1. Wählen Sie im Manager 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- LDAP Gruppen direkt an ein LDAP Benutzerkonto zuweisen auf Seite 118
- LDAP Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- LDAP Gruppen an Geschäftsrollen zuweisen auf Seite 113
- LDAP Gruppen in Systemrollen aufnehmen auf Seite 114
- LDAP Gruppen in den IT Shop aufnehmen auf Seite 115

LDAP Gruppen direkt an ein LDAP Benutzerkonto zuweisen

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

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 im Manager 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- LDAP Benutzerkonten direkt an eine LDAP Gruppe zuweisen auf Seite 117
- LDAP Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- LDAP Gruppen an Geschäftsrollen zuweisen auf Seite 113
- LDAP Gruppen in Systemrollen aufnehmen auf Seite 114
- LDAP Gruppen in den IT Shop aufnehmen auf Seite 115

LDAP Computer direkt an eine LDAP Gruppe zuweisen

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 im Manager 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.

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

   Um eine Zuweisung zu entfernen

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

Verwandte Themen

- LDAP Gruppen direkt an einen LDAP Computer zuweisen auf Seite 119
- LDAP Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- LDAP Gruppen an Geschäftsrollen zuweisen auf Seite 113
- LDAP Gruppen in Systemrollen aufnehmen auf Seite 114
- LDAP Gruppen in den IT Shop aufnehmen auf Seite 115

LDAP Gruppen direkt an einen LDAP Computer zuweisen

Um auf Sonderanforderungen schnell zu reagieren, können Sie einem Computer die Gruppen 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 im Manager 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

Verwandte Themen

- LDAP Computer direkt an eine LDAP Gruppe zuweisen auf Seite 118
- LDAP Gruppen an Abteilungen, Kostenstellen und Standorte zuweisen auf Seite 111
- LDAP Gruppen an Geschäftsrollen zuweisen auf Seite 113
- LDAP Gruppen in Systemrollen aufnehmen auf Seite 114
- LDAP Gruppen in den IT Shop aufnehmen auf Seite 115

Wirksamkeit von Mitgliedschaften in LDAP Gruppen

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

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

HINWEIS:

- Ein wechselseitiger Ausschluss zweier Gruppen kann nicht definiert werden. Das heißt, die Festlegung "Gruppe A schließt Gruppe B aus" UND "Gruppe B schließt Gruppe A aus" ist nicht zulässig.
- Für eine Gruppe muss jede auszuschließende Gruppe einzeln bekannt gegeben werden. Ausschlussdefinitionen werden nicht vererbt.
- Ob die Mitgliedschaft einer ausgeschlossenen Gruppe in einer anderen Gruppe zulässig ist (Tabelle), wird durch den One Identity Manager nicht überprüft.

Die Wirksamkeit der Zuweisungen wird in den Tabellen `LDAPAccountInLDAPGroup` und `BaseTreeHasLDAPGroup` über die Spalte `XIsInEffect` abgebildet.

Beispiel: 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 Identität sowohl Bestellungen auslösen als auch Rechnungen zur Zahlung anweisen kann. Das heißt, die Gruppen A und B schließen sich aus. Eine Identität, die Rechnungen prüft, darf ebenfalls keine Rechnungen zur Zahlung anweisen. Das heißt, die Gruppen B und C schließen sich aus.

Tabelle 12: Festlegen der ausgeschlossenen Gruppen (Tabelle `LDAPGroupExclusion`)

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

Tabelle 13: Wirksame Zuweisungen

Identität	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 Identität ist berechtigt Bestellungen

auszulösen und Rechnungen zu prüfen. Soll das verhindert werden, definieren Sie einen weiteren Ausschluss für die Gruppe C.

Tabelle 14: Ausgeschlossene Gruppen und wirksame Zuweisungen

Identität	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.

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

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

- Sich ausschließende Gruppen gehören zur selben Domäne.

Um Gruppen auszuschließen

1. Wählen Sie im Manager 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 Gruppen selektiv 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 **Position 1** bis **Position 63**.

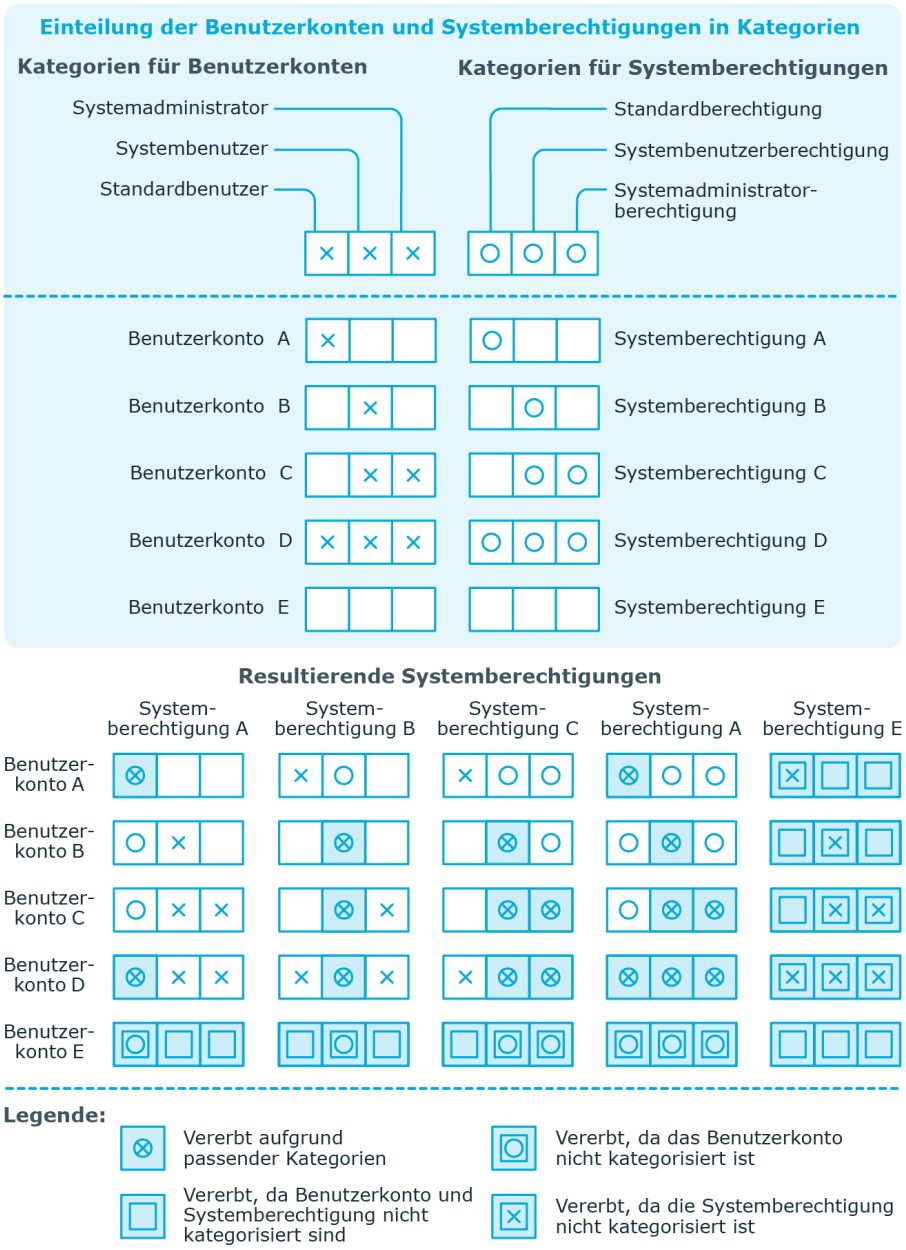
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist 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 15: 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

1. Definieren Sie im Manager an der Domäne die Kategorien.
2. Weisen Sie die Kategorien den Benutzerkonten und Kontakten über ihre Stammdaten zu.
3. Weisen Sie die Kategorien den Gruppen über ihre Stammdaten zu.

Verwandte Themen

- Kategorien für die Vererbung von LDAP Gruppen definieren auf Seite 146
- Allgemeine Stammdaten für LDAP Benutzerkonten auf Seite 155
- Stammdaten für LDAP Gruppen auf Seite 170

Übersicht aller Zuweisungen

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

Beispiele:

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

Um detaillierte Informationen über Zuweisungen anzuzeigen

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

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

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

Abbildung 3: Symbolleiste des Berichts Übersicht aller Zuweisungen

Tabelle 16: 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.

6

Bereitstellen von Anmeldeinformationen für LDAP Benutzerkonten

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

Detaillierte Informationen zum Thema

- Kennwortrichtlinien für LDAP Benutzerkonten auf Seite 127
- Initiales Kennwort für neue LDAP Benutzerkonten auf Seite 139
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 140

Kennwortrichtlinien für LDAP Benutzerkonten

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

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

Detaillierte Informationen zum Thema

- Vordefinierte Kennwortrichtlinien auf Seite 128
- Kennwortrichtlinien anwenden auf Seite 129
- Kennwortrichtlinien bearbeiten auf Seite 131
- Kennwortrichtlinien erstellen auf Seite 131
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 135
- Ausschlussliste für Kennwörter bearbeiten auf Seite 138
- Kennwörter prüfen auf Seite 139
- Generieren von Kennwörtern testen auf Seite 139

Vordefinierte Kennwortrichtlinien

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

Kennwortrichtlinie für die Anmeldung am One Identity Manager

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

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

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Identitäten

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

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

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

Kennwortrichtlinien für Benutzerkonten

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

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

> HINWEIS: Bei der Aktualisierung von One Identity Manager Version 7.x auf One Identity Manager Version 9.2 werden die Einstellung der Konfigurationsparameter zur Bildung von Kennwörtern auf die zielsystemspezifischen Kennwortrichtlinien umgesetzt.

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.

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

Kennwortrichtlinien anwenden

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.

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

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

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

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

Um eine Kennwortrichtlinie neu zuzuweisen

1. Wählen Sie im Manager die Kategorie **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.
    - **Anwenden auf**: Anwendungsbereich der Kennwortrichtlinie.

      Um den Anwendungsbereich festzulegen

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

Um die Zuweisung einer Kennwortrichtlinie zu ändern

1. Wählen Sie im Manager die Kategorie **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.

Kennwortrichtlinien bearbeiten

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

Um eine Kennwortrichtlinie zu bearbeiten

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 132
- Richtlinieneinstellungen auf Seite 132
- Zeichenklassen für Kennwörter auf Seite 134
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 135

Kennwortrichtlinien erstellen

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

Um eine Kennwortrichtlinie zu erstellen

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Kennwortrichtlinien auf Seite 132
- Richtlinieneinstellungen auf Seite 132
- Zeichenklassen für Kennwörter auf Seite 134
- Kundenspezifische Skripte für Kennwortanforderungen auf Seite 135

Allgemeine Stammdaten für Kennwortrichtlinien

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 17: Stammdaten einer Kennwortrichtlinie

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

Richtlinieneinstellungen

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

Tabelle 18: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wenn beim Erstellen eines Benutzerkontos kein Kennwort angegeben wird oder kein Zufallskennwort generiert wird, dann wird das initiale Kennwort benutzt.
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben muss. Ist der Wert **0**, ist kein Kennwort erforderlich.
Max. Länge	Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann. Der maximal zulässige Wert ist **256**.
Max. Fehlanmeldungen	Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Die Anzahl der Fehlanmeldungen wird nur bei der Anmeldung am One Identity Manager berücksichtigt. Ist der Wert **0**, dann wird die Anzahl der Fehlanmeldungen nicht berücksichtigt. Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder identitätenbasierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen überschritten, kann sich die Identität oder der Systembenutzer nicht mehr am One Identity Manager anmelden. Kennwörter gesperrter Identitäten und Systembenutzer können im Kennwortrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im *One Identity Manager Web Designer Web Portal Anwenderhandbuch*.
Max. Tage gültig	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird. Ist der Wert **0**, dann läuft das Kennwort nicht ab.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert **5** eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert. Ist der Wert **0**, dann werden keine Kennwörter in der Kennwortchronik gespeichert.
Min. Kennwortstärke	Gibt an, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert **0** wird die Kennwortstärke nicht geprüft. Die Werte **1**, **2**,

Eigenschaft	Bedeutung
	3 und **4** geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert **1** die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert **4** fordert die höchste Komplexität.
Namensbestandteile unzulässig	Gibt an, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die Option **Enthält Namensbestandteile für die Kennwortprüfung** aktiviert ist. Die Option passen Sie im Designer an der Spaltendefinition an. Ausführliche Informationen finden Sie im *One Identity Manager Konfigurationshandbuch*.

Zeichenklassen für Kennwörter

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

Tabelle 19: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Erforderliche Anzahl von Zeichenklassen	Anzahl der Regeln für Zeichenklassen, die erfüllt sein müssen, damit ein Kennwort der Kennwortrichtlinie entspricht. Berücksichtigt werden die Regeln für **Min. Anzahl Buchstaben**, **Min. Anzahl Kleinbuchstaben**, **Min. Anzahl Großbuchstaben**, **Min. Anzahl Ziffern** und **Min. Anzahl Sonderzeichen**. Es bedeuten: • Wert **0**: Es müssen alle Zeichenklassenregeln erfüllt sein. • Wert **> 0**: Anzahl der Zeichenklassenregeln, die mindestens erfüllt sein müssen. Der Wert kann maximal der Anzahl der Regeln entsprechend, deren Wert **> 0** ist. HINWEIS: Die Prüfung erfolgt nicht für generierte Kennwörter.
Min. Anzahl Buchstaben	Gibt an, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss.
Min. Anzahl Kleinbuchstaben	Gibt an, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Großbuchstaben	Gibt an, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.

Eigenschaft	Bedeutung
Min. Anzahl Ziffern	Gibt an, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Gibt an, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.
Zulässige Sonderzeichen	Liste zulässiger Sonderzeichen.
Max. identische Zeichen insgesamt	Maximale Anzahl identischer Zeichen, die insgesamt im Kennwort vorkommen dürfen.
Max. identische Zeichen aufeinanderfolgend	Maximale Anzahl identischer Zeichen, die nacheinander wiederholt werden können.
Unzulässige Sonderzeichen	Liste unzulässiger Sonderzeichen.
Keine Klein-buchstaben erzeugen	Gibt an, ob ein generiertes Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keinen Großbuch-staben erzeugen	Gibt an, ob ein generiertes Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Keine Ziffern erzeugen	Gibt an, ob ein generiertes Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berück-sichtigt.
Keine Sonderzeichen erzeugen	Gibt an, ob ein generiertes Kennwort Sonderzeichen enthalten darf. Ist die Option aktiviert, sind nur Buchstaben, Zahlen und Leerzeichen in Kennwörtern erlaubt. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.

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 136
- Skript zum Generieren eines Kennwortes auf Seite 137

Skript zum Prüfen eines Kennwortes

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

Syntax für Prüfskripte

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

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Kennwort, das zu prüfen ist

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

Beispiel: Skript zum Prüfen eines Kennwortes

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

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

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **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 137

Skript zum Generieren eines Kennwortes

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

Syntax für Generierungsskripte

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

Mit Parametern:

`policy` = Kennwortrichtlinienobjekt

`spwd` = Generiertes Kennwort

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

Beispiel: Skript zum Generieren eines Kennwortes

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

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

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

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
    a. Wählen Sie im Manager die Kategorie **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 136

Ausschlussliste für Kennwörter bearbeiten

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.

Kennwörter prüfen

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 von Kennwörtern 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.

Initiales Kennwort für neue LDAP Benutzerkonten

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

- Tragen Sie beim Erstellen des Benutzerkontos in den Stammdaten ein Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.
    - Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | 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 Identität das initiale Kennwort per E-Mail versendet wird.

Verwandte Themen

- Kennwortrichtlinien für LDAP Benutzerkonten auf Seite 127
- E-Mail-Benachrichtigungen über Anmeldeinformationen auf Seite 140

E-Mail-Benachrichtigungen über Anmeldeinformationen

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

Um Benachrichtigungen zu nutzen, sind folgende Voraussetzungen zu erfüllen:

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

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

Um die initialen Anmeldeinformationen per E-Mail zu versenden

1. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | 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 **Identität - 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 **Identität - Initiales Kennwort für neues Benutzerkonto** versendet. Die Benachrichtigung enthält das initiale Kennwort für das Benutzerkonto.

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

Abbildung von LDAP Objekten im One Identity Manager

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

Detaillierte Informationen zum Thema

LDAP Domänen

Das Zielsystem der Synchronisation mit einem LDAP Verzeichnis ist die Domäne. Domänen werden als Basisobjekte der Synchronisation im One Identity Manager angelegt. Sie werden genutzt, um Provisionierungsprozesse, die automatische Zuordnung von Identitäten zu Benutzerkonten und die Vererbung von LDAP Gruppen an Benutzerkonten zu konfigurieren.

Detaillierte Informationen zum Thema

- Kategorien für die Vererbung von LDAP Gruppen definieren auf Seite 146
- Synchronisationsprojekt für eine LDAP Domäne bearbeiten auf Seite 147
- Suchkriterien für die automatische Identitätenzuordnung bearbeiten auf Seite 95
- Überblick über LDAP Domänen anzeigen auf Seite 148
- Einzelobjekte synchronisieren auf Seite 60

LDAP Domänen erstellen

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

Um eine LDAP Domäne zu erstellen

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

Verwandte Themen

- Stammdaten von LDAP Domänen bearbeiten auf Seite 143
- Allgemeine Stammdaten für LDAP Domänen auf Seite 144
- LDAP spezifische Stammdaten für LDAP Domänen auf Seite 146
- Kategorien für die Vererbung von LDAP Gruppen definieren auf Seite 146

Stammdaten von LDAP Domänen bearbeiten

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

Um die Stammdaten einer LDAP Domäne zu bearbeiten

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

Verwandte Themen

- LDAP Domänen erstellen auf Seite 143
- Allgemeine Stammdaten für LDAP Domänen auf Seite 144
- LDAP spezifische Stammdaten für LDAP Domänen auf Seite 146
- Kategorien für die Vererbung von LDAP Gruppen definieren auf Seite 146

Allgemeine Stammdaten für LDAP Domänen

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 20: Stammdaten einer Domäne

Eigenschaft	Beschreibung
Domäne	NetBIOS Namen der Domäne.

Vollständiger Domänennamen	Domänennamen der Domäne gemäß DNS Syntax.
	`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 Identitäten zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand **Linked configured**) entstehen sollen. Es wird der Standardautomatisierungsgrad der

<table>
<tr><th>Eigenschaft</th><th>Beschreibung</th></tr>
<tr><td></td><td>Kontendefinition angewendet.

Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Identität verbunden (Zustand Linked). Dies ist beispielsweise bei der initialen Synchronisation der Fall.</td></tr>
<tr><td>Zielsystemverantwortliche</td><td>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.</td></tr>
<tr><td>Synchronisiert durch</td><td>Art der Synchronisation, über welche die Daten zwischen der Domäne und dem One Identity Manager synchronisiert werden. Sobald Objekte für diese Domäne im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden.

Beim Erstellen einer Domäne mit dem Synchronization Editor wird One Identity Manager verwendet.

Tabelle 21: Zulässige Werte
<table>
<tr><th>Wert</th><th>Synchro-nisation durch</th><th>Provi-sionierung 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 Objekt-klasse</td><td>Strukturelle Objektklasse, die den Typ des Objektes repräsentiert.</td></tr>
</table>

Verwandte Themen

- Kontendefinitionen an LDAP Domänen zuweisen auf Seite 90
- Automatische Zuordnung von Identitäten zu LDAP Benutzerkonten auf Seite 93
- Zielsystemverantwortliche für LDAP auf Seite 182

LDAP spezifische Stammdaten für LDAP Domänen

Erfassen Sie die folgenden Stammdaten zum LDAP.

Tabelle 22: Angaben zum LDAP

Eigenschaft	Beschreibung
Vollständiger Domänennamen	Domänennamen der Domäne gemäß DNS Syntax. `<Name dieser Domäne>.<Name der übergeordneten Domäne>.<Name der Stammdomäne>`
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.

Kategorien für die Vererbung von LDAP Gruppen definieren

Im One Identity Manager können Gruppen selektiv 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 **Position 1** bis **Position 63**.

Um Kategorien zu definieren

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

Detaillierte Informationen zum Thema

- Vererbung von LDAP Gruppen anhand von Kategorien auf Seite 123

Synchronisationsprojekt für eine LDAP Domäne bearbeiten

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

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

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

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

Verwandte Themen

- Anpassen der Synchronisationskonfiguration für LDAP-Umgebungen auf Seite 39

Überblick über LDAP Domänen anzeigen

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

Um einen Überblick über eine Domäne zu erhalten

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

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.

Detaillierte Informationen zum Thema

- LDAP Container erstellen auf Seite 148
- Stammdaten von LDAP Containern bearbeiten auf Seite 149
- Allgemeine Stammdaten für LDAP Container auf Seite 150
- Kontaktinformationen für LDAP Container auf Seite 151
- Adressinformationen für LDAP Container auf Seite 152
- Zusatzeigenschaften an LDAP Container zuweisen auf Seite 152
- Überblick über LDAP Container anzeigen auf Seite 153
- Einzelobjekte synchronisieren auf Seite 60

LDAP Container erstellen

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

Um einen Container zu erstellen

1. Wählen Sie im Manager die Kategorie **LDAP > Container**.
2. Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Containers.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von LDAP Containern bearbeiten auf Seite 149
- Allgemeine Stammdaten für LDAP Container auf Seite 150
- Kontaktinformationen für LDAP Container auf Seite 151
- Adressinformationen für LDAP Container auf Seite 152

Stammdaten von LDAP Containern bearbeiten

Sie können vorhandene Container im One Identity Manager bearbeiten.

Um einen Container zu bearbeiten

1. Wählen Sie im Manager die Kategorie **LDAP > Container**.
2. Wählen Sie in der Ergebnisliste den Container und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Containers.
4. Speichern Sie die Änderungen.

Verwandte Themen

- LDAP Container erstellen auf Seite 148
- Allgemeine Stammdaten für LDAP Container auf Seite 150
- Kontaktinformationen für LDAP Container auf Seite 151
- Adressinformationen für LDAP Container auf Seite 152

Allgemeine Stammdaten für LDAP Container

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 23: 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

Eigenschaft	Beschreibung
	Zielsystemverantwortlichen bearbeiten nur die Objekte des Containers, dem sie zugeordnet sind. Jedem Container können somit andere Zielsystemverantwortliche zugeordnet werden. Wählen Sie die One Identity Manager Anwendungsrolle 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 für LDAP auf Seite 182

Kontaktinformationen für LDAP Container

Erfassen Sie die Daten zur Erreichbarkeit.

Tabelle 24: 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 für LDAP Container

Erfassen Sie die folgenden Adressinformationen.

Tabelle 25: Adressdaten

Eigenschaft	Beschreibung
Name des Gebäudes	Bezeichnung des Gebäudes.
Standortkennzeichen	Standortkennzeichen (Land und Ort).
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 Zustellmethode	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.

Zusatzeigenschaften an LDAP Container zuweisen

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

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

Um Zusatzeigenschaften für einen Container festzulegen

1. Wählen Sie im Manager die Kategorie **LDAP > Container**.
2. Wählen Sie in der Ergebnisliste den Container.

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

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

   Um eine Zuweisung zu entfernen

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

Überblick über LDAP Container anzeigen

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

Um einen Überblick über einen Container zu erhalten

1. Wählen Sie im Manager die Kategorie **LDAP > Container**.
2. Wählen Sie in der Ergebnisliste den Container.
3. Wählen Sie die Aufgabe **Überblick über den LDAP Container**.

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 Berechtigungen Zugriff auf die Netzwerkressourcen.

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

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

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

Verwandte Themen

- Managen von LDAP Benutzerkonten und Identitäten auf Seite 69
- Managen von Mitgliedschaften in LDAP Gruppen auf Seite 108

- Kontendefinitionen für LDAP Benutzerkonten auf Seite 70
- LDAP Benutzerkonten erstellen auf Seite 154
- Stammdaten von LDAP Benutzerkonten bearbeiten auf Seite 155
- Allgemeine Stammdaten für LDAP Benutzerkonten auf Seite 155
- Kontaktinformationen für LDAP Benutzerkonten auf Seite 161
- Adressinformationen für LDAP Benutzerkonten auf Seite 162
- Organisatorische Informationen für LDAP Benutzerkonten auf Seite 162
- EduPerson-Erweiterungen für LDAP Benutzerkonten auf Seite 163
- Sonstige Informationen für LDAP Benutzerkonten auf Seite 165
- Zusatzeigenschaften an LDAP Benutzerkonten zuweisen auf Seite 165
- LDAP Benutzerkonten deaktivieren auf Seite 166
- LDAP Benutzerkonten löschen und wiederherstellen auf Seite 167
- Überblick über LDAP Benutzerkonten anzeigen auf Seite 168
- Einzelobjekte synchronisieren auf Seite 60

LDAP Benutzerkonten erstellen

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

Um ein Benutzerkonto zu erstellen

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

Verwandte Themen

- Stammdaten von LDAP Benutzerkonten bearbeiten auf Seite 155
- Allgemeine Stammdaten für LDAP Benutzerkonten auf Seite 155
- Kontaktinformationen für LDAP Benutzerkonten auf Seite 161
- Adressinformationen für LDAP Benutzerkonten auf Seite 162
- Organisatorische Informationen für LDAP Benutzerkonten auf Seite 162
- EduPerson-Erweiterungen für LDAP Benutzerkonten auf Seite 163
- Sonstige Informationen für LDAP Benutzerkonten auf Seite 165
- Identitäten manuell mit LDAP Benutzerkonten verbinden auf Seite 99

Stammdaten von LDAP Benutzerkonten bearbeiten

Sie können vorhandene Benutzerkonten im One Identity Manager bearbeiten.

Um die Stammdaten eines Benutzerkontos zu bearbeiten

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

Verwandte Themen

- LDAP Benutzerkonten erstellen auf Seite 154
- Allgemeine Stammdaten für LDAP Benutzerkonten auf Seite 155
- Kontaktinformationen für LDAP Benutzerkonten auf Seite 161
- Adressinformationen für LDAP Benutzerkonten auf Seite 162
- Organisatorische Informationen für LDAP Benutzerkonten auf Seite 162
- EduPerson-Erweiterungen für LDAP Benutzerkonten auf Seite 163
- Sonstige Informationen für LDAP Benutzerkonten auf Seite 165
- LDAP Benutzerkonten deaktivieren auf Seite 166
- LDAP Benutzerkonten löschen und wiederherstellen auf Seite 167

Allgemeine Stammdaten für LDAP Benutzerkonten

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 26: Allgemeine Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Identität	Identität, die das Benutzerkonto verwendet. • Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Identität bereits eingetragen. • Wenn Sie die automatische Identitätenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine

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

Eigenschaft	Beschreibung
	aufgrund eines Ausschlusskriteriums nicht mit einer Identität verbunden. Das Benutzerkonto ist beispielsweise in der Ausschlussliste für die automatische Identitätenzuordnung enthalten (Konfigurationsparameter **PersonExcludeList**).
Kontendefinition	Kontendefinition, über die das Benutzerkonto erstellt wurde. Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Identität und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein. HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden. HINWEIS: Über die Aufgabe **Entferne Kontendefinition** am Benutzerkonto können Sie das Benutzerkonto wieder in den Zustand **Linked** zurücksetzen. Dabei wird die Kontendefinition vom Benutzerkonto und von der Identität entfernt. Das Benutzerkonto bleibt über diese Aufgabe erhalten, wird aber nicht mehr über die Kontendefinition verwaltet. Die Aufgabe entfernt nur Kontendefinitionen, die direkt zugewiesen sind (`XOrigin=1`).
Automatisierungsgrad	Automatisierungsgrad des Benutzerkontos. Wählen Sie einen Automatisierungsgrad aus der Auswahlliste. Den Automatisierungsgrad können Sie nur festlegen, wenn Sie auch eine Kontendefinition eingetragen haben. In der Auswahlliste werden alle Automatisierungsgrade der gewählten Kontendefinition angeboten.
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 Identität 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

Eigenschaft	Beschreibung
	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 zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Nachname	Nachname des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Initialen	Initialen des Benutzers. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
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 Identität gebildet.
Kennwort	Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Identität kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Identität finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*. Wenn Sie ein zufällig generiertes initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen. Das Kennwort wird nach dem Publizieren in das Zielsystem aus der Datenbank gelöscht.

Eigenschaft	Beschreibung
	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 Identität als Kontoverfallsdatum übernommen. Ein bereits eingetragenes Kontoverfallsdatum des Benutzerkontos wird dabei überschrieben.
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto. Gruppen können selektiv an die Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Identitätstyp	Typ der Identität des Benutzerkontos. Zulässige Werte sind: • **Primäre Identität**: Standardbenutzerkonto einer Identität. • **Organisatorische Identität**: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • **Persönliche Administratoridentität**: Benutzerkonto mit administrativen Berechtigungen, welches von einer Identität genutzt wird. • **Zusatzidentität**: Benutzerkonto, das für einen spezifischen Zweck benutzt wird, beispielsweise zu Trainingszwecken. • **Gruppenidentität**: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Identitäten

Eigenschaft	Beschreibung
	genutzt wird. Weisen Sie alle Identitäten zu, die das Benutzerkonto nutzen. • **Dienstidentität**: Dienstkonto.
Privilegiertes Benutzerkonto	Gibt an, ob es sich um ein privilegiertes Benutzerkonto handelt.
Gruppen erbbar	Gibt an, ob das Benutzerkonto Gruppen über die verbundene Identität erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen, in denen die Identität Mitglied ist, oder über IT Shop Bestellungen an das Benutzerkonto vererbt. • Wenn Sie eine Identität mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Identität eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Identität diese Gruppe nur, wenn die Option aktiviert ist.
Benutzerkonto ist deaktiviert	Gibt an, ob das Benutzerkonto deaktiviert ist. Wird ein Benutzerkonto vorübergehend nicht benötigt, können Sie das Benutzerkonto über die Option zeitweilig deaktivieren.

Verwandte Themen

- Kontendefinitionen für LDAP Benutzerkonten auf Seite 70
- Kennwortrichtlinien für LDAP Benutzerkonten auf Seite 127
- Initiales Kennwort für neue LDAP Benutzerkonten auf Seite 139
- Managen von LDAP Benutzerkonten und Identitäten auf Seite 69
- Managen von Mitgliedschaften in LDAP Gruppen auf Seite 108
- Voraussetzungen für indirekte Zuweisungen von LDAP Gruppen auf Seite 110
- LDAP Benutzerkonten deaktivieren auf Seite 166

Kontaktinformationen für LDAP Benutzerkonten

Erfassen Sie die Daten zur telefonischen Erreichbarkeit der Identität, die das Benutzerkonto verwendet.

Tabelle 27: 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 Identität 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.
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 für LDAP Benutzerkonten

Erfassen Sie die folgenden Adressinformationen zur Erreichbarkeit der Identität, die das Benutzerkonto verwendet.

Tabelle 28: 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 für LDAP Benutzerkonten

Erfassen Sie die folgenden organisatorischen Stammdaten.

Tabelle 29: Organisatorische Stammdaten

Eigenschaft	Beschreibung
Geschäftsbereich	Geschäftsbereich, dem die Identität zugeordnet ist.
Abteilung	Abteilung der Identität. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automa-

Eigenschaft	Beschreibung
	tisierungsgrad automatisch ausgefüllt.
Standort	Standort der Identität. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Standortkennzeichen	Standortkennzeichen (Land und Ort).
Art der Anstellung	Angaben zur Anstellung.
Personalnummer	Nummer zur Kennzeichnung der Identität zusätzlich zur ID der Identität.
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 Identität. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch ausgefüllt.
Autokennzeichen	Kennzeichen des Fahrzeugs.

EduPerson-Erweiterungen für LDAP Benutzerkonten

Auf dem Tabreiter **Bildung und Forschung** werden folgende Informationen für die Objektklasse **eduPerson** abgebildet.

Tabelle 30: Stammdaten für eduPerson

Eigenschaft	Beschreibung
Benutzerkennung	Ein eindeutiger Bezeichner für eine Identität. Der Bezeichner sollte in der Form "**user@scope**" dargestellt werden. Der Teil **user** ist ein namen-basierter Bezeichner für die Identität. Der Teil **scope** ist die administrative Domäne des Identitätssystems, in dem der Bezeichner erstellt und zugewiesen wurde.
Eindeutiges Pseudonym	Eindeutiger und dauerhafter pseudonymer Bezeichner einer Identität. Dieser Wert ist Anbieter-spezifisch.
Globaler Bezeichner	Eindeutiger, global gültiger Bezeichner für eine Identität.
Nickname	Kurzname der Identität.
Einrichtung	Definierter Name der Einrichtung, zu der die Identität gehört.
Bereich der Einrichtung	Definierter Name des Bereichs der Einrichtung, zu dem die Identität gehört. Es können mehrere Bereiche angegeben werden.
Bereich der Einrichtung (primär)	Definierter Name des primären Bereichs der Einrichtung, zu dem die Identität gehört.
Art der Zugehörigkeit	Kategorie für die Zugehörigkeit der Identität zur Einrichtung wie beispielsweise Student, Lehrkörper, Mitarbeiter, Ehemaliger. Es können mehrere Arten angegeben werden.
Zugehörigkeitsbereich	Kategorie und Einrichtung, zu der die Identität gehört. Es können mehrere Zugehörigkeitsbereiche angegeben werden. Beispiel: student@university.com
Primäre Zugehörigkeit	Primäre Kategorie und Einrichtung, zu der die Identität gehört. Beispiel: student@university.com
Berechtigungen	Berechtigungen, die den Zugriff und die Art des Zugriffs auf bestimmte Ressourcen steuern.
ORCID-IDs	Eindeutige Bezeichner, die primär dazu dienen, eine Identität mit ihren wissenschaftlichen Publikationen in Beziehung zu setzen.
Verlässlichkeitsklasse	Angaben zur Verlässlichkeit einer Identität.
Vorherige Benutzerkennungen	Vorherige Benutzerkennungen, die mit der Identität verknüpft waren. Die Werte dürfen nicht den aktuell gültigen Wert der Benutzerkennung enthalten.
Analyse-Tag	Zeichenkette, die für Berichterstattung oder Analyse genutzt werden kann.

Verwandte Themen

- Unterstützung der eduPerson-Objektklasse auf Seite 42

Sonstige Informationen für LDAP Benutzerkonten

Erfassen Sie die folgenden Stammdaten.

Tabelle 31: Sonstige Stammdaten

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

Zusatzeigenschaften an LDAP Benutzerkonten zuweisen

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

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

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie im Manager die Kategorie **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.

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

   Um eine Zuweisung zu entfernen

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

LDAP Benutzerkonten deaktivieren

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

Szenario: Die Benutzerkonten sind mit Identitäten verbunden und werden über Kontendefinitionen verwaltet.

Benutzerkonten, die über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Identität 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 Identitäten verbunden. Es sind keine Kontendefinitionen zugeordnet.

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

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

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu deaktivieren

1. Wählen Sie im Manager 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: Die Benutzerkonten sind nicht mit Identitäten verbunden.

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

1. Wählen Sie im Manager 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.

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

Verwandte Themen

- Kontendefinitionen für LDAP Benutzerkonten auf Seite 70
- Automatisierungsgrade erstellen auf Seite 76
- LDAP Benutzerkonten löschen und wiederherstellen auf Seite 167

LDAP Benutzerkonten löschen und wiederherstellen

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

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

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

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

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

Um ein Benutzerkonto wiederherzustellen

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

Verwandte Themen

- LDAP Benutzerkonten deaktivieren auf Seite 166
- Löschverzögerung für LDAP Benutzerkonten festlegen auf Seite 106

Überblick über LDAP Benutzerkonten anzeigen

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

Um einen Überblick über ein Benutzerkonto zu erhalten

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

LDAP Gruppen

LDAP Benutzerkonten, Computer und Gruppen können 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 bearbeiten.

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

Verwandte Themen

- Managen von Mitgliedschaften in LDAP Gruppen auf Seite 108
- LDAP Gruppen erstellen auf Seite 169
- Stammdaten von LDAP Gruppen bearbeiten auf Seite 169
- Stammdaten für LDAP Gruppen auf Seite 170
- LDAP Gruppen in LDAP Gruppen aufnehmen auf Seite 172

- Zusatzeigenschaften an LDAP Gruppen zuweisen auf Seite 171
- LDAP Gruppen löschen auf Seite 173
- Überblick über LDAP Gruppen anzeigen auf Seite 173
- Einzelobjekte synchronisieren auf Seite 60

LDAP Gruppen erstellen

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

Um eine Gruppe zu erstellen

1. Wählen Sie im Manager die Kategorie **LDAP > Gruppen**.
2. Klicken Sie in der Ergebnisliste .
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von LDAP Gruppen bearbeiten auf Seite 169
- Stammdaten für LDAP Gruppen auf Seite 170
- LDAP Gruppen löschen auf Seite 173

Stammdaten von LDAP Gruppen bearbeiten

Sie können vorhandene Gruppen im One Identity Manager bearbeiten.

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **LDAP > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
5. Speichern Sie die Änderungen.

Verwandte Themen

- LDAP Gruppen erstellen auf Seite 169
- Stammdaten für LDAP Gruppen auf Seite 170
- LDAP Gruppen löschen auf Seite 173

Stammdaten für LDAP Gruppen

Erfassen Sie die folgenden allgemeinen Stammdaten.

Tabelle 32: 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	Name 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	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 im Bereich von **0** bis **1** ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter **QER | CalculateRiskIndex** aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im *One Identity Manager Administrationshandbuch für Risikobewertungen*.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.

Eigenschaft	Beschreibung
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Bedingung	LDAP Filter für die Bestimmung der Mitgliedschaften einer dynamische Gruppe.
Dynamische Gruppe	Gibt an, ob es sich um eine dynamische Gruppe handelt.
IT Shop	Gibt an, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Gibt an, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal 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 123
- LDAP Gruppen in den IT Shop aufnehmen auf Seite 115

Zusatzeigenschaften an LDAP Gruppen zuweisen

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

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

Um Zusatzeigenschaften für eine Gruppe festzulegen

1. Wählen Sie im Manager 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.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Zusatzeigenschaft und doppelklicken Sie ✓.

5. Speichern Sie die Änderungen.

LDAP Gruppen in LDAP Gruppen aufnehmen

Mit dieser Aufgabe nehmen Sie eine Gruppe in andere Gruppen auf. Damit können die Gruppen hierarchisch strukturiert werden.

Um Gruppen als Mitglieder an eine Gruppe zuzuweisen

1. Wählen Sie im Manager die Kategorie **LDAP > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Wählen Sie den Tabreiter **Hat Mitglieder**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die untergeordneten Gruppen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie ✓.

6. Speichern Sie die Änderungen.

Um eine Gruppe als Mitglied in andere Gruppen aufzunehmen

1. Wählen Sie im Manager die Kategorie **LDAP > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Gruppen zuweisen**.
4. Wählen Sie den Tabreiter **Ist Mitglied in**.
5. Weisen Sie im Bereich **Zuordnungen hinzufügen** die übergeordneten Gruppen zu.

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

   Um eine Zuweisung zu entfernen

   - Wählen Sie die Gruppe und doppelklicken Sie ✓.

6. Speichern Sie die Änderungen.

LDAP Gruppen löschen

Die Gruppe wird endgültig aus der One Identity Manager-Datenbank und der LDAP-Umgebung gelöscht.

Um eine Gruppe zu löschen

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

Überblick über LDAP Gruppen anzeigen

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 im Manager die Kategorie **LDAP > Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Überblick über die LDAP Gruppe**.

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.

Verwandte Themen

- LDAP Computer erstellen auf Seite 174
- Stammdaten von LDAP Computern bearbeiten auf Seite 174
- Stammdaten für LDAP Computer auf Seite 175
- Überblick über LDAP Computer anzeigen auf Seite 175
- Managen von Mitgliedschaften in LDAP Gruppen auf Seite 108
- Einzelobjekte synchronisieren auf Seite 60

LDAP Computer erstellen

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

Um einen Computer zu erstellen

1. Wählen Sie im Manager die Kategorie **LDAP > Computer**.
2. Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten für einen Computer.
4. Speichern Sie die Änderungen.

Verwandte Themen

- Stammdaten von LDAP Computern bearbeiten auf Seite 174
- Stammdaten für LDAP Computer auf Seite 175

Stammdaten von LDAP Computern bearbeiten

Sie können vorhandene Computer im One Identity Manager bearbeiten.

Um die Stammdaten eines Computers zu bearbeiten

1. Wählen Sie im Manager die Kategorie **LDAP > Computer**.
2. Wählen Sie in der Ergebnisliste den Computer und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten für einen Computer.
4. Speichern Sie die Änderungen.

Verwandte Themen

- LDAP Computer erstellen auf Seite 174
- Stammdaten für LDAP Computer auf Seite 175

Stammdaten für LDAP Computer

Für einen Computer erfassen Sie die folgenden Stammdaten.

Tabelle 33: Stammdaten eines Computers

Eigenschaft	Beschreibung
Gerät	Gerät, mit dem der Computer verbunden ist. Legen Sie über die Schaltfläche neben der Auswahlliste ein neues Gerät an. Ausführliche Informationen zu Geräten finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
Bezeichnung	Bezeichnung des Computers.
Domäne	Domäne, in der der Computer erzeugt werden soll.
Container	Container in dem der Computer erzeugt werden soll. Bei der Auswahl des Containers wird per Bildungsregel der definierte Name für den Computer ermittelt.
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

- Voraussetzungen für indirekte Zuweisungen von LDAP Gruppen auf Seite 110

Überblick über LDAP Computer anzeigen

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

Um einen Überblick über einen Computer zu erhalten

1. Wählen Sie im Manager die Kategorie **LDAP > Computer**.
2. Wählen Sie in der Ergebnisliste den Computer.
3. Wählen Sie die Aufgabe **Überblick über den Computer**.

Berichte über LDAP Objekte

One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen Objekten der One Identity Manager-Datenbank aufbereitet sind. Für LDAP stehen folgende Berichte zur Verfügung.

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

Tabelle 34: Berichte zur Datenqualität eines Zielsystems

Bericht	Bereitgestellt für	Beschreibung
Übersicht anzeigen	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Herkunft)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto und die Herkunft der zugewiesenen Berechtigungen.
Übersicht anzeigen (inklusive Historie)	Benutzerkonto	Der Bericht zeigt einen Überblick über das Benutzerkonto einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Benutzerkonten anzeigen (inklusive Historie)	Container	Der Bericht zeigt alle Benutzerkonten des Containers mit ihren Berechtigungen einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Systemberechtigungen anzeigen (inklusive Historie)	Container	Der Bericht zeigt die Systemberechtigungen des Containers mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min.**

Bericht	Bereitgestellt für	Beschreibung
		Datum). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Container	Der Bericht ermittelt alle Rollen, in denen sich Identitäten befinden, die im ausgewählten Container mindestens ein Benutzerkonto besitzen.
Übersicht aller Zuweisungen	Gruppe	Der Bericht ermittelt alle Rollen, in denen sich Identitäten befinden, welche die ausgewählte Systemberechtigung besitzen.
Übersicht anzeigen	Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und ihre Zuweisungen.
Übersicht anzeigen (inklusive Herkunft)	Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung und die Herkunft der zugewiesenen Benutzerkonten.
Übersicht anzeigen (inklusive Historie)	Gruppe	Der Bericht zeigt einen Überblick über die Systemberechtigung einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Abweichende Systemberechtigungen anzeigen	Domäne	Der Bericht enthält alle Systemberechtigungen, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten anzeigen (inklusive Historie)	Domäne	Der Bericht liefert alle Benutzerkonten mit ihren Berechtigungen einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.

Bericht	Bereitgestellt für	Beschreibung
Benutzerkonten mit einer überdurchschnittliche Anzahl an Systemberechtigungen anzeigen	Domäne	Der Bericht enthält alle Benutzerkonten, die eine überdurchschnittliche Anzahl an Systemberechtigungen besitzen.
Identitäten mit mehreren Benutzerkonten anzeigen	Domäne	Der Bericht zeigt alle Identitäten, die mehrere Benutzerkonten besitzen. Der Bericht enthält eine Risikoeinschätzung.
Systemberechtigungen anzeigen (inklusive Historie)	Domäne	Der Bericht zeigt die Systemberechtigungen mit den zugewiesenen Benutzerkonten einschließlich eines historischen Verlaufs. Wählen Sie das Datum, bis zu dem die Historie angezeigt werden soll (**Min. Datum**). Ältere Änderungen und Zuordnungen, die vor diesem Datum entfernt wurden, werden in dem Bericht nicht dargestellt.
Übersicht aller Zuweisungen	Domäne	Der Bericht ermittelt alle Rollen, in denen sich Identitäten befinden, die im ausgewählten Zielsystem mindestens ein Benutzerkonto besitzen.
Ungenutzte Benutzerkonten anzeigen	Domäne	Der Bericht enthält alle Benutzerkonten, die in den letzten Monaten nicht verwendet wurden.
Unverbundene Benutzerkonten anzeigen	Domäne	Der Bericht zeigt alle Benutzerkonten, denen keine Identität zugeordnet ist.

Tabelle 35: Zusätzliche Berichte für das Zielsystem

Bericht	Beschreibung
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 125

8

Behandeln von LDAP Objekten im Web Portal

Der One Identity Manager bietet seinen Benutzern die Möglichkeit, verschiedene Aufgaben unkompliziert über ein Web Portal zu erledigen.

- Managen von Benutzerkonten und Identitäten

  Mit der Zuweisung einer Kontendefinition an ein IT Shop Regal kann die Kontendefinition von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Identität, beispielsweise einen Manager, wird das Benutzerkonto angelegt.

- Managen von Zuweisungen von Gruppen

  Mit der Zuweisung einer Gruppe an ein IT Shop Regal kann die Gruppe von den Kunden des Shops im Web Portal bestellt werden. Die Bestellung durchläuft ein definiertes Genehmigungsverfahren. Erst nach der Zustimmung durch eine autorisierte Identität wird die Gruppe zugewiesen.

  Manager und Administratoren von Organisationen können im Web Portal Gruppen an die Abteilungen, Kostenstellen oder Standorte zuweisen, für die sie verantwortlich sind. Die Gruppen werden an alle Identitäten vererbt, die Mitglied dieser Abteilungen, Kostenstellen oder Standorte sind.

  Wenn das Geschäftsrollenmodul vorhanden ist, können Manager und Administratoren von Geschäftsrollen im Web Portal Gruppen an die Geschäftsrollen zuweisen, für die sie verantwortlich sind. Die Gruppen werden an alle Identitäten vererbt, die Mitglied dieser Geschäftsrollen sind.

  Wenn das Systemrollenmodul vorhanden ist, können Verantwortliche von Systemrollen im Web Portal Gruppen an die Systemrollen zuweisen. Die Gruppen werden an alle Identitäten vererbt, denen diese Systemrollen zugewiesen sind.

- Attestierung

  Wenn das Modul Attestierung vorhanden ist, kann die Richtigkeit der Eigenschaften von Zielsystemobjekten und von Gruppenmitgliedschaften regelmäßig oder auf Anfrage bescheinigt werden. Dafür werden im Manager Attestierungsrichtlinien konfiguriert. Die Attestierer nutzen das Web Portal, um Attestierungsvorgänge zu entscheiden.

- Governance Administration

  Wenn das Modul Complianceregeln vorhanden ist, können Regeln definiert werden, die unzulässige Gruppenmitgliedschaften identifizieren und deren Risiken bewerten. Die Regeln werden regelmäßig und bei Änderungen an den Objekten im One Identity Manager überprüft. Complianceregeln werden im Manager definiert. Verantwortliche nutzen das Web Portal, um Regelverletzungen zu überprüfen, aufzulösen und Ausnahmegenehmigungen zu erteilen.

  Wenn das Modul Unternehmensrichtlinien vorhanden ist, können Unternehmensrichtlinien für die im One Identity Manager abgebildeten Zielsystemobjekte definiert und deren Risiken bewertet werden. Unternehmensrichtlinien werden im Manager definiert. Verantwortliche nutzen das Web Portal, um Richtlinienverletzungen zu überprüfen und Ausnahmegenehmigungen zu erteilen.

- Risikobewertung

  Über den Risikoindex von Gruppen kann das Risiko von Gruppenmitgliedschaften für das Unternehmen bewertet werden. Dafür stellt der One Identity Manager Standard-Berechnungsvorschriften bereit. Im Web Portal können die Berechnungsvorschriften modifiziert werden.

- Berichte und Statistiken

  Das Web Portal stellt verschiedene Berichte und Statistiken über die Identitäten, Benutzerkonten, deren Berechtigungen und Risiken bereit.

Ausführliche Informationen zu den genannten Themen finden Sie unter Managen von LDAP Benutzerkonten und Identitäten auf Seite 69, Managen von Mitgliedschaften in LDAP Gruppen auf Seite 108 und in folgenden Handbüchern:

- *One Identity Manager Web Designer Web Portal Anwenderhandbuch*
- *One Identity Manager Administrationshandbuch für Attestierungen*
- *One Identity Manager Administrationshandbuch für Complianceregeln*
- *One Identity Manager Administrationshandbuch für Unternehmensrichtlinien*
- *One Identity Manager Administrationshandbuch für Risikobewertungen*

Basisdaten für die Verwaltung einer LDAP-Umgebung

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

- Kontendefinitionen

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

  Weitere Informationen finden Sie unter Kontendefinitionen für LDAP Benutzerkonten auf Seite 70.

- Kennwortrichtlinien

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

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

  Weitere Informationen finden Sie unter Kennwortrichtlinien für LDAP Benutzerkonten auf Seite 127.

- Zielsystemtypen

  Zielsystemtypen werden für die Konfiguration des Zielsystemabgleichs benötigt. An den Zielsystemtypen werden die Tabellen gepflegt, die ausstehende Objekte enthalten können. Es werden Einstellungen für die Provisionierung von Mitgliedschaften und die Einzelobjektsynchronisation vorgenommen. Zusätzlich dient der Zielsystemtyp zur Abbildung der Objekte im Unified Namespace.

  Weitere Informationen finden Sie unter Ausstehende Objekte nachbehandeln auf Seite 61.

- Zielsystemverantwortliche

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

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

  Weitere Informationen finden Sie unter Zielsystemverantwortliche für LDAP auf Seite 182.

- Server

  Für die Verarbeitung der zielsystemspezifischen Prozesse im One Identity Manager muss der Synchronisationsserver mit seinen Serverfunktionen bekannt sein.

  Weitere Informationen finden Sie unter Jobserver für LDAP-spezifische Prozessverarbeitung auf Seite 185.

Zielsystemverantwortliche für LDAP

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

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

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

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

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

Tabelle 36: 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. • Bearbeiten Kennwortrichtlinien für das Zielsystem. • Bereiten Gruppen zur Aufnahme in den IT Shop vor. • Können Identitäten anlegen, die nicht den Identitätstyp **Primäre Identität** haben. • Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager. • Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation. • Berechtigen innerhalb ihres Verantwortungsbereiches weitere Identitäten als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Identitäten als Zielsystemadministrator festzulegen

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

Um initial Identitäten in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

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

Um als Zielsystemverantwortlicher weitere Identitäten als Zielsystemverantwortliche zu berechtigen

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

Um Zielsystemverantwortliche für einzelne Domänen festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **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.

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

   b. Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Identitäten zu, die berechtigt sind, die Domäne im One Identity Manager zu bearbeiten.

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 11
- Allgemeine Stammdaten für LDAP Domänen auf Seite 144
- LDAP Containerstrukturen auf Seite 148

Jobserver für LDAP-spezifische Prozessverarbeitung

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

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

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

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

Verwandte Themen

- Systemanforderungen für den LDAP Synchronisationsserver auf Seite 21
- LDAP Jobserver bearbeiten auf Seite 185

LDAP Jobserver bearbeiten

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

Um einen Jobserver und seine Funktionen zu bearbeiten

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

Detaillierte Informationen zum Thema

- Allgemeine Stammdaten für Jobserver auf Seite 186
- Festlegen der Serverfunktionen auf Seite 189
- One Identity Manager Service mit LDAP Konnektor installieren auf Seite 22

Allgemeine Stammdaten für Jobserver

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

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

Tabelle 37: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS-Syntax. Syntax: `<Name des Servers>.<Vollqualifizierter Domänenname>`
Zielsystem	Zielsystem des Computerkontos.
Sprache	Sprache des Servers.
Server ist Cluster	Gibt an, ob der Server einen Cluster abbildet.
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften **Server ist Cluster** und **Server gehört zu Cluster** schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme `Robocopy` und `rsync` unterstützt. Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausge-

Eigenschaft	Bedeutung
	führt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm `Robocopy` und zwischen Servern mit einem Linux Betriebssystem mit dem Programm `rsync`. Unterscheiden sich die Betriebssysteme des Quellservers und des Zielservers, so ist für eine erfolgreiche Replikation die Angabe der zulässigen Kopierverfahren zwingend erforderlich. Es wird das Kopierverfahren eingesetzt, das beide Server unterstützen.
Kopierverfahren (Zielserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Ziel einer Kopieraktion ist.
Codierung	Codierung des Zeichensatzes mit der Dateien auf dem Server geschrieben werden.
Übergeordneter Jobserver	Bezeichnung des übergeordneten Jobservers.
Ausführender Server	Bezeichnung des ausführenden Servers. Eingetragen wird der Name des physisch vorhandenen Servers, auf dem die Prozesse verarbeitet werden. Diese Angabe wird bei der automatischen Aktualisierung des One Identity Manager Service ausgewertet. Verarbeitet ein Server mehrere Queues, wird mit der Auslieferung von Prozessschritten solange gewartet, bis alle Queues, die auf demselben Server abgearbeitet werden, die automatische Aktualisierung abgeschlossen haben.
Queue	Bezeichnung der Queue, welche die Prozessschritte verarbeitet. Mit dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte **Win32**, **Windows**, **Linux** und **Unix**. Ist die Angabe leer, wird **Win32** angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto,

Eigenschaft	Bedeutung
	die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	Gibt an, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur `QBM_PJobQueueLoad` aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Gibt an, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Berechtigungen im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im *One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche*.
Pausiert wegen Nichtverfügbarkeit eines Zielsystems	Gibt an, ob die Verarbeitung von Aufträgen für diese Queue angehalten wurde, weil das Zielsystem, für den dieser Jobserver der Synchronisationsserver ist, vorübergehend nicht erreichbar ist. Sobald das Zielsystem wieder erreichbar ist, wird die Verarbeitung gestartet und alle anstehenden Aufträge werden ausgeführt. Ausführliche Informationen zum Offline-Modus finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
Kein automatisches Softwareupdate	Gibt an, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Gibt an, ob gerade eine Softwareaktualisierung ausgeführt wird.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- Festlegen der Serverfunktionen auf Seite 189

Festlegen der Serverfunktionen

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

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

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

Tabelle 38: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
CSV Konnektor	Server, auf dem der CSV Konnektor für die Synchronisation installiert ist.
Domänen-Controller	Active Directory Domänen-Controller. Server, die nicht als Domänen-Controller gekennzeichnet sind, werden als Memberserver betrachtet.
Druckserver	Server, der als Druckserver arbeitet.
Generischer Server	Server für die generische Synchronisation mit einem kundendefinierten Zielsystem.
Homeserver	Server zur Anlage von Homeverzeichnissen für Benutzerkonten.
LDAP Konnektor	Server, auf dem der LDAP Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem LDAP aus.
LDAP Store	Server, der den LDAP Store hält.
Aktualisierungsserver	Der Server führt die automatische Softwareaktualisierung aller anderen Server aus. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Der Server kann SQL Aufträge ausführen. Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.

Serverfunktion	Anmerkungen
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Der Server benötigt eine direkte Verbindung zum Datenbankserver, auf dem die One Identity Manager-Datenbank installiert ist. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente `ScriptComponent` verarbeiten.
Generischer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.
One Identity Manager-Datenbankkonnektor	Server, auf dem der One Identity Manager Konnektor installiert ist. Dieser Server führt die Synchronisation mit dem Zielsystem One Identity Manager aus.
One Identity Manager Service installiert	Server, auf dem ein One Identity Manager Service installiert werden soll.
Primärer Domänen-Controller	Primärer Domänen-Controller.
Profilserver	Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten.
SAM Synchronisationsserver	Server für die Synchronisation mit einem SMB-basierten Zielsystem.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtsserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell Konnektor	Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen.

Verwandte Themen

- Allgemeine Stammdaten für Jobserver auf Seite 186

Anhang A

Fehlerbehebung

Mögliche Fehler bei der Synchronisation einer OpenDJ-Umgebung

Problem

Bei der Synchronisation einer OpenDJ-Umgebung tritt ein Fehler auf, wenn ein Kennwort mit einer öffnenden geschweiften Klammer beginnt.

Ursache

Der LDAP Server interpretiert ein generiertes Kennwort in der Form `{<abc>}<def>` als Hashwert. Der LDAP Server lässt die Übergabe von gehashten Kennwörtern jedoch nicht zu.

Lösung

LDAP Server können so konfiguriert werden, dass ein bereits gehashtes Kennwort in der Form `{<Algorithmus>}Hash` übergeben wird.

- Auf dem LDAP Server: Erlauben Sie die Übergabe von bereits gehashten Kennwörtern.
- Im Synchronisationsprojekt: Übergeben Sie nur gehashte Kennwörter. Nutzen Sie Skripteigenschaften für das Mapping von Schemaeigenschaften, die Kennwörter enthalten. Erzeugen Sie im Skript den Hashwert der Kennwörter.

Fehler beim mehrfachen Anbinden von LDAP Systemen mit dem gleichen definierten Namen

Probleme

Beim Erstellen mehrerer Synchronisationsprojekte für die Anbindung einer LDAP Domäne oder bei der Anbindung von Instanzen mit identischer Bezeichnung tritt eine Fehlermeldung auf.

```
Die Domäne mit dem definierten Namen '{0}' wird bereits im
Synchronisationsprojekt '{1}' verwendet. Je Domäne und Konnektor ist nur ein
Synchronisationsprojekt zulässig.
```

Ursache

Dieses Problem tritt auf, wenn die Synchronisationsprojekte mit einer älteren One Identity Manager Version erstellt wurden.

Zur Suche von LDAP Domänen in der Datenbank wird die Bezeichnung der Domäne (`Ident_Domain`) verwendet. In Synchronisationsprojekten, die mit einer älteren One Identity Manager Version erstellt wurden, wurde die Bezeichnung der LDAP Domänen in der Form `<DN Bestandteil 1>` gebildet.

Lösung

- Mit neu erstellten Synchronisationsprojekten wird die Bezeichnung der LDAP Domänen in der Form `<DN Bestandteil 1> (<Server aus Verbindungsparametern>)` gebildet.
- Für bestehende Synchronisationsprojekte, die mit dem generischen LDAP Konnektor erstellt wurden, wenden Sie den Patch **VPR#33513** an. Damit wird eine Variable samt Wert für `$IdentDomain$` in allen Variablensets erzeugt und der Scope auf `DistinguishedName = '$CP_RootEntry$' and Ident_Domain='$IdentDomain$'` geändert.

  Ausführliche Informationen zum Anwenden von Patches finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.
- Bereits in der Datenbank vorhandene LDAP Domänen werden nicht umbenannt. Passen Sie die Bezeichnung der LDAP Domänen (`Ident_Domain`) gegebenenfalls manuell an. Weitere Informationen finden Sie unter LDAP Domänen auf Seite 142.

HINWEIS: Bei Objekten, die aus verschiedenen Verzeichnisdiensten importiert werden, und in der One Identity Manager-Datenbank den identischen kanonischen Namen und definierten Namen besitzen, kann es zu doppelten Anzeigewerten in laufenden Attestierungen, beispielsweise bei Systemberechtigungen, und in Berichten über Zielsystemobjekten und Zielsystemberechtigungen kommen. Gegebenenfalls müssen kundenspezifische Anpassungen an den Attestierungsverfahren und Berichten vorgenommen werden.

Anhang B

Konfigurationsparameter für die Verwaltung einer LDAP-Umgebung

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

Tabelle 39: 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. Wenn Sie den Konfigurationsparameter zu einem späteren Zeitpunkt deaktivieren, werden die nicht benötigten Modellbestandteile und Skripte deaktiviert. SQL Prozeduren und Trigger werden weiterhin ausgeführt. Ausführliche Informationen zum Verhalten präprozessorrelevanter Konfigurationsparameter und zur bedingten Kompilierung finden Sie im *One Identity Manager Konfigurationshandbuch*.
TargetSystem | LDAP | Accounts	Erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem | LDAP | Accounts | InitialRandomPassword	Gibt an, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.
TargetSystem | LDAP | Accounts | InitialRandomPassword |	Identität, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Geschäftsrolle,

Konfigurationsparameter	Beschreibung
SendTo	Verantwortlicher der Identität oder `XUserInserted`). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter **TargetSystem | LDAP | DefaultAddress** hinterlegte Adresse versandt.
TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo | MailTemplateAccountName	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage **Identität - Erstellung neues Benutzerkonto** verwendet.
TargetSystem | LDAP | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword	Name der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage **Identität - Initiales Kennwort für neues Benutzerkonto** verwendet.
TargetSystem | LDAP | Accounts | MailTemplateDefaultValues	Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage **Identität - Erstellung neues Benutzerkonto mit Standardwerten** verwendet.
TargetSystem | LDAP | Accounts | PrivilegedAccount	Erlaubt die Konfiguration der Einstellungen für privilegierte LDAP Benutzerkonten.
TargetSystem | LDAP | Accounts | PrivilegedAccount | UserID_ Postfix	Postfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | LDAP | Accounts | PrivilegedAccount | UserID_ Prefix	Präfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem | LDAP | Authentication	Erlaubt die Konfiguration der LDAP Authentifizierungsmodule. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
TargetSystem | LDAP | Authentication | Authentication	Authentifizierungsmechanismus. Gültige Werte sind **Secure**, **Encryption**, **SecureSocketsLayer**, **ReadonlyServer**, **Anonymous**, **FastBind**, **Signing**,

Konfigurationsparameter	Beschreibung
	Sealing, **Delegation** und **ServerBind**. Die Werte können mit Komma (,) kombiniert werden. Ausführliche Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library. Standard: **ServerBind**
TargetSystem | LDAP | Authentication | Port	Kommunikationsport auf dem Server. Standard: **389**

TargetSystem | LDAP | Authentication | RootDN	Pipe (|) getrennte Liste von Root-Domänen, in denen das Benutzerkonto zur Authentifizierung gesucht werden soll.
	Syntax:
	`DC=<MyDomain>|DC=<MyOtherDomain>`
	Beispiel:
	`DC=Root1,DC=com|DC=Root2,DC=de`

TargetSystem | LDAP | Authentication | Server	Name des LDAP Servers.
TargetSystem | LDAP | AuthenticationV2	Erlaubt die Konfiguration der LDAP Authentifizierungsmodule. Ausführliche Informationen zu den One Identity Manager Authentifizierungsmodulen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.
TargetSystem | LDAP | AuthenticationV2 | AcceptSelfSigned	Gibt an, ob selbstsignierte Zertifikate akzeptiert werden.
TargetSystem | LDAP | AuthenticationV2 | Authentication	Authentifizierungsmethode zur Anmeldung am LDAP System. Zulässig sind: • **Basic**: Die Standardauthentifizierung wird verwendet. • **Negotiate**: Die Negotiate-Authentifizierung von Microsoft wird verwendet. • **Kerberos**: Die Kerberos-Authentifizierung wird verwendet. • **NTLM**: Die Windows NT-Abfrage/Rückmeldung-Authentifizierung wird verwendet. Standard: **Basic**

Konfigurationsparameter	Beschreibung
	Weitere Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library.
TargetSystem | LDAP | AuthenticationV2 | ClientTimeout	Client-Timeout in Sekunden.
TargetSystem | LDAP | AuthenticationV2 | Port	Kommunikationsport auf dem Server. Standard: **389**
TargetSystem | LDAP | AuthenticationV2 | ProtocolVersion	Version des LDAP Protokolls. Zulässig sind die Werte **2** und **3**. Standard: **3**

TargetSystem | LDAP | AuthenticationV2 | RootDN	Pipe (|) getrennte Liste von Root-Domänen, in denen das Benutzerkonto zur Authentifizierung gesucht werden soll.
	Syntax:
	`DC=<MyDomain>|DC=<MyOtherDomain>`
	Beispiel:
	`DC=Root1,DC=com|DC=Root2,DC=de`

TargetSystem | LDAP | AuthenticationV2 | Security	Sicherheit der Verbindung. Zulässige Werte sind **None**, **SSL** und **STARTTLS**.
TargetSystem | LDAP | AuthenticationV2 | Server	Name des LDAP Servers.
TargetSystem | LDAP | AuthenticationV2 | UseSealing	Gibt an, ob die Nachrichtenvertraulichkeit aktiviert ist.
TargetSystem | LDAP | AuthenticationV2 | UseSigning	Gibt an, ob Nachrichtenintegrität aktiviert ist.
TargetSystem | LDAP | AuthenticationV2 | VerifyServerCertificate	Gibt an, ob bei Verschlüsselung mit SSL das Serverzertifikat geprüft werden soll.
TargetSystem | LDAP | DefaultAddress	Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem | LDAP | HardwareInGroupFromOrg	Gibt an, ob Computer aufgrund von Gruppenzuordnung zu Rollen in Gruppen aufgenommen werden.
TargetSystem | LDAP | MaxFullsyncDuration	Maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der

Konfigurationsparameter	Beschreibung
	festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.
TargetSystem | LDAP | PersonAutoDefault	Modus für die automatische Identitätenzuordnung für Benutzerkonten, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem | LDAP | PersonAutoDisabledAccounts	Gibt an, ob an deaktivierte Benutzerkonten automatisch Identitäten zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem | LDAP | PersonAutoFullSync	Modus für die automatische Identitätenzuordnung für Benutzerkonten, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.

Anhang C

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 Projektvorlage für den LDAP Konnektor V2 auf Seite 198
- Active Directory Lightweight Directory Services Projektvorlage für den LDAP Konnektor V2 auf Seite 199
- Oracle Directory Server Enterprise Edition Projektvorlage für den LDAP Konnektor V2 auf Seite 200
- Generische Projektvorlage für den LDAP Konnektor V2 auf Seite 200

OpenDJ Projektvorlage für den LDAP Konnektor V2

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

Tabelle 40: Abbildung der Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im LDAP	Tabelle im One Identity Manager Schema
container	LDAPContainer

Schematyp im LDAP	Tabelle im One Identity Manager Schema
country	LDAPContainer
domain	LDPDomain
GroupOfEntries	LDAPGroup
groupOfNames	LDAPGroup
groupOfUniqueNames	LDAPGroup
groupOfURLs	LDAPGroup
inetOrgPerson	LDAPAccount
locality	LDAPContainer
organization	LDAPContainer
organizationalUnit	LDAPContainer

Active Directory Lightweight Directory Services Projektvorlage für den LDAP Konnektor V2

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

Tabelle 41: Abbildung der Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im AD LDS	Tabelle im One Identity Manager Schema
domainDNS	LDAPContainer
country	LDAPContainer
locality	LDAPContainer
organization	LDAPContainer
container	LDAPContainer
organizationalUnit	LDAPContainer
inetOrgPerson	LDAPAccount
user	LDAPAccount
userProxy	LDAPAccount

Schematyp im AD LDS	Tabelle im One Identity Manager Schema
userProxyFull	LDAPAccount
foreignSecurityPrincipal	LDAPAccount
group	LDAPGroup
groupOfNames	LDAPGroup

Oracle Directory Server Enterprise Edition Projektvorlage für den LDAP Konnektor V2

Diese Projektvorlage basiert auf Oracle Directory Server Enterprise Edition (DSEE). Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 42: Abbildung der Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im LDAP	Tabelle im One Identity Manager Schema
country	LDAPContainer
domain	LDPDomain
groupOfNames	LDAPGroup
groupOfUniqueNames	LDAPGroup
groupOfURLs	LDAPGroup
inetOrgPerson	LDAPAccount
locality	LDAPContainer
organization	LDAPContainer
organizationalUnit	LDAPContainer

Generische Projektvorlage für den LDAP Konnektor V2

Diese Vorlage kann als Basisvorlage verwendet werden, wenn keine systemspezifische Vorlage vorhanden ist. Es können weitere Anpassungen können erforderlich sein.

HINWEIS: Prüfen Sie das Projekt und korrigieren Sie mögliche Fehler bevor Sie das Synchronisationsprojekt verwenden.

Die Projektvorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 43: Abbildung der Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im LDAP	Tabelle im One Identity Manager Schema
container	LDAPContainer
country	LDAPContainer
domain	LDPDomain
GroupOfEntries	LDAPGroup
groupOfNames	LDAPGroup
groupOfUniqueNames	LDAPGroup
groupOfURLs	LDAPGroup
inetOrgPerson	LDAPAccount
locality	LDAPContainer
organization	LDAPContainer
organizationalUnit	LDAPContainer

Anhang D

Einstellungen des LDAP Konnektors V2

Für die Systemverbindung mit dem LDAP Konnektor V2 werden die folgenden Einstellungen konfiguriert.

HINWEIS: Einige der Einstellungen können Sie nur setzen, wenn Sie auf der Startseite des Systemverbindungsassistenten die Option **Erweiterte Einstellungen anzeigen** aktivieren.

Tabelle 44: Einstellungen des LDAP Konnektors V2

Einstellung	Bedeutung
Server	IP-Adresse oder vollständiger Name des LDAP Servers, gegen den sich der Synchronisationsserver verbindet, um auf die LDAP Objekte zuzugreifen. Variable: `CP_SdspLdapDriverDescriptorServer`
Port	Kommunikationsport auf dem Server. Standard: **389** Variable: `CP_SdspLdapDriverDescriptorPort`
Authentifizierungsart	Authentifizierungsmethode zur Anmeldung am LDAP System. Zulässig sind: • **Basic**: Die Standardauthentifizierung wird verwendet. • **Negotiate**: Die Negotiate-Authentifizierung von Microsoft wird verwendet. • **Anonymous**: Die Verbindung erfolgt ohne Übergabe von Anmeldeinformationen. • **Kerberos**: Die Kerberos-Authentifizierung wird verwendet. • **NTLM**: Die Windows NT-Abfrage/Rückmeldung-Authentifizierung wird verwendet. • **External**: Als externe Methode wird die

Einstellung	Bedeutung
	zertifikatsbasierte Authentifizierung verwendet. Standard: **Basic** Variable: `CP_SdspLdapDriverDescriptorAuthenticationType` Weitere Informationen zu den Authentifizierungsarten finden Sie in der MSDN Library.
Benutzername	Name des Benutzerkontos zur Anmeldung am LDAP. Variable: `CP_SdspLdapDriverDescriptorUsername`
Kennwort	Kennwort zum Benutzerkonto. Variable: `CP_SdspLdapDriverDescriptorPassword`
Sealing verwenden	Gibt an, ob die Nachrichtenvertraulichkeit aktiviert ist. Variable: `CP_SdspLdapDriverDescriptorUseSealing`
Signing verwenden	Gibt an, ob Nachrichtenintegrität aktiviert ist. Variable: `CP_SdspLdapDriverDescriptorUseSigning`
SSL verwenden	Gibt an, ob eine SSL/TLS verschlüsselte Verbindung verwendet wird. Variable: `CP_SdspLdapDriverDescriptorUseSsl`
StartTLS verwenden	Gibt an, ob eine StartTLS zur Verschlüsselung verwendet wird. Variable: `CP_SdspLdapDriverDescriptorUseStartTls`
Prüfung Serverzertifikat	Gibt an, ob bei der Verschlüsslung mittels SSL oder StartTLS das Serverzertifikat geprüft werden soll. HINWEIS: Das Serverzertifikat muss gültig sein. Das Zertifikat der Stammzertifizierungsstelle muss als Computerzertifikat (Zertifikatsspeicher **Lokaler Computer**) auf dem Host, auf dem der Synchronization Editor gestartet wurde oder auf dem Jobserver, zu dem eine Remoteverbindung hergestellt wurde, vorhanden sein. Stellen Sie sicher, dass das Zertifikat auch auf allen Jobservern installiert ist, die sich gegen das LDAP System verbinden sollen. Variable: `CP_SdspLdapDriverDescriptorVerifyServerCertificate`
Protokollversion	Version des LDAP Protokolls. Standard: **3** Variable: `CP_SdspLdapDriverDescriptorProtocolVersion`
Suchbasis	Basis für die Suchanfragen, in der Regel die LDAP Domäne.

Einstellung	Bedeutung
	Variable: `CP_LdapContextDescriptorBaseDn`
Anfrage Timeout	Timeout für LDAP Anfragen in Sekunden. Standard: **3600** Variable: `CP_SdspLdapDriverDescriptorClientTimeout`
UID der LDAP Domäne	Eindeutige Kennung für die LDAP Domäne in der Tabelle `LDPDomain`. Variable: `UID_LDPDomain`
Default Searcher: Verwende seitenweise Suche	Gibt an, ob die LDAP Objekte seitenweise geladen werden sollen. Diese Information wird automatisch durch die gewählte Vorkonfiguration ermittelt oder vom LDAP Server abgefragt. Wenn die Option aktiviert ist, erfassen Sie die Seitengröße. Variable: `CP_SdspDefaultSearchDescriptorUsePagedSearch`
Default Searcher: Seitengröße	Anzahl der maximal zu ladenden Objekte pro Seite. Standard: **500** Variable: `CP_SdspDefaultSearchDescriptorPageSize`
AD (LDS) Search implementation: Segmentgröße	Wenn Attribute mit einer großen Anzahl Werte von einem Microsoft basierenden LDAP Server zurückgegeben werden sollen, sendet der Server nur eine bestimmte Menge der Werte zurück (üblicherweise 1500). Um alle Werte abzufragen, müssen mehrere Abfragen mit einer Bereichseinschränkung gesendet werden. Die Segmentgröße bestimmt, wie viele Werte pro Abfrage zurückgeliefert werden sollen. Wenn die gewählte Segmentgröße größer ist, als die Maximalgröße, die der Server verarbeiten kann, wird die Segmentgröße automatisch angepasst. Standard: **1000** Variable: `CP_AdLdsSearchFeatureDescriptorChunkSize`
Default delete implementation: Verwende DeleteTree-Control bei Löschung von Einträgen	Gibt an, ob der LDAP Server beim Löschen das **DeleteTree**-Control senden soll, um Einträge mit untergeordneten Einträgen zu löschen. Diese Information wird automatisch durch die gewählte Vorkonfiguration ermittelt oder vom LDAP Server abgefragt. Variable:`CP_SdspDefaultDeleteDescriptorUseDeleteTree`
Load schema from LDAP Server	Das Schema wird vom LDAP Server geladen. (Standard)
Load schema from given	Alternative Quelle, aus der das Schema geladen wird, falls das

Einstellung	Bedeutung
LDIF string	Schema des LDAP Servers nicht verfügbar ist. Die LDIF Zeichenkette wird in der Systemverbindung (`DPRSystemConnection.ConnectionParameter`) gespeichert. Damit muss keine `*.ldif`-Datei verteilt werden.
Remove spaces in distinguished names	Die Funktion entfernt alle laut RFC nicht erlaubten oder nicht signifikanten Leerzeichen in definierten Namen von Objekten. Wenn die Funktion nicht vorhanden ist, werden laut RFC nicht erlaubte oder nicht signifikante Leerzeichen in definierten Namen nicht entfernt und führen unter Umständen zu Fehlern. Standard: **False**
Tolerate 'Attribute already exists' and 'no such attribute' and retry	Mit dieser Funktion werden bei der Änderung eines Objektes bereits im LDAP System vorhandene oder fehlende Attribute toleriert, beispielsweise bei der Aktualisierung von Gruppenmitgliedschaften. Wenn die Funktion nicht vorhanden ist, führen Änderungen, die im LDAP System vorhandene oder fehlende Attribute betreffen, zu Fehlern. Standard: **True**
Return operational attributes	Mit dieser Schemafunktion legen Sie fest, welche Attribute zusätzlich für die LDAP Objekte ermittelt werden sollen. Funktionale Attribute werden für die Verzeichnisverwaltung verwendet. Die funktionalen Attribute werden zu jeder Schemaklasse der übergeordneten Funktion hinzugefügt. 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.
Auxillary class assigment	Mit dieser Schemafunktion weisen Sie strukturellen Klassen zusätzliche Hilfsklassen zu. 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.
Switch type of objectclasses	Mit dieser Schemafunktion können Sie den Typ einer Objektklasse ändern. Dies kann erforderlich sein, wenn ein

Einstellung	Bedeutung
	nicht RFC-konformes LDAP System die Zuweisung mehrerer struktureller Objektklassen zu einem Eintrag zulässt obwohl nur eine strukturelle Klasse erlaubt ist. Mehrere zugewiesene strukturelle Klassen führen dazu, das ein LDAP Eintrag nicht eindeutig einem Schematyp zugeordnet werden kann. Wurden strukturelle Objektklassen definiert, die lediglich als Eigenschaftserweiterungen dienen sollen (also **Auxiliary**-Klassen sein sollten), so kann man den Konnektor mit Hilfe dieser Einstellung dazu veranlassen, diese Objektklasse als **Auxiliary** zu betrachten. HINWEIS: Als **Auxiliary** konfigurierte Objektklassen werden dann nicht mehr als eigenständige Schematypen behandelt und können in Folge auch nicht separat synchronisiert werden.

Cache Schema	Mit dieser Schemafunktion wird das LDAP Schema lokal im Cache gehalten. Es wird empfohlen, diese Funktion möglichst nach dem Laden des Schemas anzuordnen. 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\LdapConnector.`

Load AD LDS schema extension	Mit dieser Schemafunktion werden zusätzliche Informationen geladen, die für die Synchronisation eines Active Directory Lightweight Directory Services erforderlich sind.
Treiber	Treiber, der zum Zugriff auf das LDAP System verwendet werden soll. Standard: **LDAP via Windows API (SdspLdapDriver)**
LDAP Domäne	Eindeutige Bezeichnung der Domäne in der Form: `<DN Bestandteil 1> (<Server aus Verbindungsparametern>)` Variable: `$IdentDomain$`

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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

Index

L

M

V

Z