



One Identity Manager 8.1.1

Administrationshandbuch für die Anbindung Unix-basierter Zielsysteme

Copyright 2019 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

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

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

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

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

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

Patente

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

Marken

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

Legende

-  **WARNUNG:** Das Symbol **WARNUNG** weist auf mögliche Personen- oder Sachschäden oder Schaden mit Todesfolge hin.
-  **VORSICHT:** Das Symbol **VORSICHT** weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.
-  **WICHTIG, HINWEIS, TIPP, MOBIL, or VIDEO:** Ein Informationssymbol weist auf Begleitinformationen hin.

Inhalt

Verwalten von Unix-basierten Zielsystemen	7
Architekturüberblick	7
One Identity Manager Benutzer für die Verwaltung eines Unix-basierten Zielsystems ..	8
Einrichten der Synchronisation mit einem Unix-basierten Zielsystem	11
Benutzer und Berechtigungen für die Synchronisation mit einem Unix-basierten Zielsystem	12
Einrichten des Synchronisationsservers	13
Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Unix Hosts	17
Benötigte Informationen für die Erstellung eine Synchronisationsprojektes	17
Erstellen eines initialen Synchronisationsprojektes	20
Synchronisationsergebnisse anzeigen	24
Aufbewahrungszeit der Protokolle konfigurieren	25
Anpassen einer Synchronisationskonfiguration	25
Synchronisation in den Unix Host konfigurieren	27
Synchronisation verschiedener Unix Hosts konfigurieren	28
Schema aktualisieren	28
Nachbehandlung ausstehender Objekte	30
Provisionierung von Mitgliedschaften konfigurieren	32
Beschleunigung der Provisionierung und Einzelobjektsynchronisation	33
Unterstützung bei der Analyse von Synchronisationsproblemen	34
Deaktivieren der Synchronisation	35
Basisdaten für Unix-basierte Zielsysteme	36
Einrichten von Kontendefinitionen	38
Erstellen einer Kontendefinition	38
Stammdaten einer Kontendefinition	39
Erstellen der Automatisierungsgrade	41
Erstellen einer Abbildungsvorschrift für IT Betriebsdaten	44
Erfassen der IT Betriebsdaten	45
IT Betriebsdaten ändern	47
Zuweisen der Kontendefinition an Personen	48

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen	50
Kontendefinition an Geschäftsrollen zuweisen	50
Kontendefinition an alle Personen zuweisen	51
Kontendefinition direkt an Personen zuweisen	52
Kontendefinition an Systemrollen zuweisen	52
Kontendefinition in den IT Shop aufnehmen	53
Zuweisen der Kontendefinition an ein Zielsystem	55
Löschen einer Kontendefinition	55
Kennwortrichtlinien für Unix Benutzerkonten	58
Vordefinierte Kennwortrichtlinien	58
Anwenden einer Kennwortrichtlinie	59
Bearbeiten von Kennwortrichtlinien	61
Allgemeine Stammdaten einer Kennwortrichtlinie	62
Richtlinieneinstellungen	62
Zeichenklassen für Kennwörter	64
Kundenspezifische Skripte für Kennwortanforderungen	65
Skript zum Prüfen eines Kennwortes	65
Skript zum Generieren eines Kennwortes	66
Ausschlussliste für Kennwörter	68
Prüfen eines Kennwortes	68
Generieren eines Kennwortes testen	68
Initiales Kennwort für neue Unix Benutzerkonten	69
E-Mail-Benachrichtigungen über Anmeldeinformationen	70
Zielsystemverantwortliche	71
Bearbeiten eines Servers	73
Stammdaten eines Jobservers	74
Serverfunktionen eines Jobservers	77
Unix Host	79
Allgemeine Stammdaten eines Unix Hosts	79
Festlegen der Kategorien für die Vererbung von Berechtigungen	81
Synchronisationsprojekt bearbeiten	82
Überblick über den Unix Host	82
Anzeigen der Unix Login-Shells	83
Unix Benutzerkonten	84

Benutzerkonten mit Personen verbinden	84
Unterstützte Typen von Benutzerkonten	85
Standardbenutzerkonten	87
Administrative Benutzerkonten	88
Administrative Benutzerkonten für eine Person bereitstellen	89
Administrative Benutzerkonten für mehrere Personen bereitstellen	90
Privilegierte Benutzerkonten	91
Erfassen der Stammdaten für Unix Benutzerkonten	92
Allgemeine Stammdaten eines Unix Benutzerkontos	94
Stammdaten eines Benutzerkontos für AIX Systeme	97
Grenzwerte eines Benutzerkontos	97
Kennwortdaten eines Benutzerkontos	99
Sicherheitsrelevante Stammdaten eines Benutzerkontos	100
Stammdaten zum verschlüsselnden Dateisystem eines Benutzerkontos	102
Zusätzliche Aufgaben für die Verwaltung von Unix Benutzerkonten	103
Überblick über das Unix Benutzerkonto	103
Ändern des Automatisierungsgrades an einem Unix Benutzerkonto	103
Unix Gruppen direkt an ein Unix Benutzerkonto zuweisen	104
Zusatzeigenschaften an ein Unix Benutzerkonto zuweisen	104
Automatische Zuordnung von Personen zu Unix Benutzerkonten	105
Bearbeiten der Suchkriterien für die automatische Personenzuordnung	107
Deaktivieren von Benutzerkonten für AIX Systeme	110
Löschen und Wiederherstellen von Unix Benutzerkonten	112
Unix Gruppen	113
Erfassen der Stammdaten für Unix Gruppen	113
Allgemeine Stammdaten einer Unix Gruppe	114
Unix Gruppe an Unix Benutzerkonten zuweisen	115
Unix Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen	115
Unix Gruppe an Geschäftsrollen zuweisen	116
Unix Benutzerkonten direkt an eine Unix Gruppe zuweisen	118
Unix Gruppe in Systemrollen aufnehmen	118
Unix Gruppe in den IT Shop aufnehmen	119
Unix Gruppe aus einem IT Shop Regal entfernen	120
Unix Gruppe aus allen IT Shop Regalen entfernen	120
Zusätzliche Aufgaben für die Verwaltung von Unix Gruppen	121

Überblick über die Unix Gruppe	121
Unix Gruppe in Unix Gruppen aufnehmen	121
Wirksamkeit von Gruppenmitgliedschaften	122
Vererbung von Unix Gruppen anhand von Kategorien	124
Zusatzeigenschaften an eine Unix Gruppe zuweisen	127
Löschen von Unix Gruppen	127
Berichte über Unix Objekte	128
Übersicht aller Zuweisungen	129
Anhang: Konfigurationsparameter für die Verwaltung einer Unix- Umgebung	131
Anhang: Standardprojektvorlage für Unix-basierte Zielsysteme	134
Über uns	135
Kontaktieren Sie uns	135
Technische Supportressourcen	135
Index	136

Verwalten von Unix-basierten Zielsystemen

Der One Identity Manager bietet eine vereinfachte Administration der Benutzerkonten einer Unix-basierten Umgebung. Der One Identity Manager konzentriert sich auf die Einrichtung und Bearbeitung von Benutzerkonten und die Versorgung mit den benötigten Berechtigungen. Um die Benutzer mit den benötigten Berechtigungen auszustatten, werden Gruppen im One Identity Manager abgebildet. Damit ist es möglich, die Identity und Access Governance Prozesse wie Attestierung, Identity Audit, Management von Benutzerkonten und Systemberechtigungen, IT Shop oder Berichtsabonnements für Unix-basierte Zielsysteme zu nutzen.

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

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

Der One Identity Manager unterstützt die gängigsten Unix- und Linux Derivate. Detaillierte Informationen finden Sie in den Spezifikationen für [One Identity Authentication Services](#).

Architekturüberblick

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

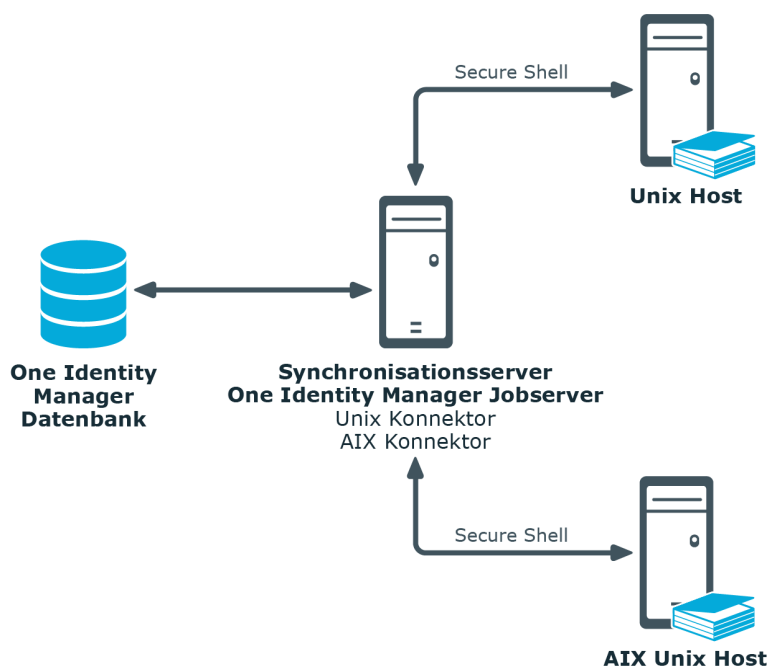
- Unix Host
Unix Host, der das Verzeichnis hält. Dieser Host ist ein ausgewählter produktiver Host mit guter Netzwerkanbindung zum Synchronisationsserver. Der

Synchronisationsserver verbindet sich gegen diesen Host, um auf die Unix Objekte zuzugreifen.

- Synchronisationsserver

Synchronisationsserver für den Abgleich zwischen der One Identity Manager-Datenbank und dem Unix-basierten Zielsystem. Auf diesem Server ist der One Identity Manager Service mit der Maschinenrolle "Unix" installiert. Die Maschinenrolle "Unix" enthält den Unix Konnektor und den AIX Konnektor. Der Unix Konnektor wird für die Synchronisation und Provisionierung der Objekte des Unix-basierten Zielsystems eingesetzt. Der AIX Konnektor wird für die Synchronisation und Provisionierung der Objekte eines IBM AIX Systems eingesetzt. Die Konnektoren kommunizieren direkt mit den Unix Host.

Abbildung 1: Architektur für die Synchronisation



One Identity Manager Benutzer für die Verwaltung eines Unix-basierten Zielsystems

In die Einrichtung und Verwaltung eines Unix-basierten Zielsystems sind folgende Benutzer eingebunden.

Tabelle 1: Benutzer

Benutzer	Aufgaben
Zielsystemadministratoren	<p>Die Zielsystemadministratoren müssen der Anwendungsrolle Zielsysteme Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Administrieren die Anwendungsrollen für die einzelnen Zielsystemtypen.• Legen die Zielsystemverantwortlichen fest.• Richten bei Bedarf weitere Anwendungsrollen für Zielsystemverantwortliche ein.• Legen fest, welche Anwendungsrollen für Zielsystemverantwortliche sich ausschließen.• Berechtigen weitere Personen als Zielsystemadministratoren.• Übernehmen keine administrativen Aufgaben innerhalb der Zielsysteme.
Zielsystemverantwortliche	<p>Die Zielsystemverantwortlichen müssen der Anwendungsrolle Zielsysteme Unix oder einer untergeordneten Anwendungsrolle zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none">• Übernehmen die administrativen Aufgaben für das Zielsystem.• Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen.• Bearbeiten Kennwortrichtlinien für das Zielsystem.• Bereiten Gruppen zur Aufnahme in den IT Shop vor.• Können Personen anlegen, die eine andere Identität haben als den Identitätstyp Primäre Identität.• Konfigurieren im Synchronization Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.• Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.• Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Benutzer	Aufgaben
One Identity Manager Administratoren	<ul style="list-style-type: none"> • Erstellen bei Bedarf im Designer kundenspezifische Rechtegruppen für Anwendungsrollen für die rollenbasierte Anmeldung an den Administrationswerkzeugen. • Erstellen bei Bedarf im Designer Systembenutzer und Rechtegruppen für die nicht-rollenbasierte Anmeldung an den Administrationswerkzeugen. • Aktivieren oder deaktivieren im Designer bei Bedarf zusätzliche Konfigurationsparameter. • Erstellen im Designer bei Bedarf unternehmensspezifische Prozesse. • Erstellen und konfigurieren bei Bedarf Zeitpläne. • Erstellen und konfigurieren bei Bedarf Kennwortrichtlinien.
Administratoren für den IT Shop	<p>Die Administratoren müssen der Anwendungsrolle Request & Fulfillment IT Shop Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Weisen an IT Shop-Strukturen zu.
Administratoren für Organisationen	<p>Die Administratoren müssen der Anwendungsrolle Identity Management Organisationen Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Weisen an Abteilungen, Kostenstellen und Standorte zu.
Administratoren für Geschäftsrollen	<p>Die Administratoren müssen der Anwendungsrolle Identity Management Geschäftsrollen Administratoren zugewiesen sein.</p> <p>Benutzer mit dieser Anwendungsrolle:</p> <ul style="list-style-type: none"> • Weisen an Geschäftsrollen zu.

Einrichten der Synchronisation mit einem Unix-basierten Zielsystem

Der One Identity Manager unterstützt die gängigsten Unix- und Linux Derivate. Detaillierte Informationen finden Sie in den Spezifikationen für [One Identity Authentication Services](#).

Um die Objekte eines Unix-basierten Zielsystems initial in die One Identity Manager-Datenbank einzulesen

1. Stellen Sie im Unix-basierten Zielsystem ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Die One Identity Manager Bestandteile für die Verwaltung von Unix-basierten Zielsystemen sind verfügbar, wenn der Konfigurationsparameter "TargetSystem\Unix" aktiviert ist.
 - Prüfen Sie im Designer, ob der Konfigurationsparameter aktiviert ist. Anderenfalls aktivieren Sie den Konfigurationsparameter und kompilieren Sie die Datenbank.
 - Mit der Installation des Moduls werden weitere Konfigurationsparameter installiert. Prüfen Sie die Konfigurationsparameter und passen Sie die Konfigurationsparameter gegebenenfalls an das gewünschte Verhalten an.
3. Installieren und konfigurieren Sie einen Synchronisationsserver und geben Sie den Server im One Identity Manager als Jobserver bekannt.
4. Erstellen Sie mit dem Synchronization Editor ein Synchronisationsprojekt.

Verwandte Themen

- [Benutzer und Berechtigungen für die Synchronisation mit einem Unix-basierten Zielsystem](#) auf Seite 12
- [Einrichten des Synchronisationsservers](#) auf Seite 13
- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Unix Hosts](#) auf Seite 17
- [Deaktivieren der Synchronisation](#) auf Seite 35
- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 25

- [Anhang: Konfigurationsparameter für die Verwaltung einer Unix-Umgebung](#) auf Seite 131
- [Anhang: Standardprojektvorlage für Unix-basierte Zielsysteme](#) auf Seite 134

Benutzer und Berechtigungen für die Synchronisation mit einem Unix-basierten Zielsystem

Bei der Synchronisation des One Identity Manager mit einem Unix-basierten Zielsystem spielen folgende Benutzer eine Rolle.

Tabelle 2: Benutzer für die Synchronisation

Benutzer	Berechtigungen
Benutzer für den Zugriff auf den Unix Host	<p>Für eine vollständige Synchronisation von Objekten eines Unix-basierten Zielsystems mit der ausgelieferten One Identity Manager Standardkonfiguration werden folgende Berechtigungen benötigt:</p> <ul style="list-style-type: none"> • Berechtigung zum Aufbau einer Secure Shell (SSH) Verbindung zum Host. • Administrative Berechtigungen zum Ausführen von Schreiboperationen auf den Unix Objekten.
Benutzerkonto des One Identity Manager Service	<p>Das Benutzerkonto für den One Identity Manager Service benötigt die Rechte, um die Operationen auf Dateiebene durchzuführen (Rechtevergabe, Verzeichnisse und Dateien anlegen und bearbeiten).</p> <ul style="list-style-type: none"> • Das Benutzerkonto muss der Gruppe "Domänen-Benutzer" (Domain Users) angehören. • Das Benutzerkonto benötigt das erweiterte Benutzerrecht "Anmelden als Dienst" (Log on as a service). • Das Benutzerkonto benötigt Rechte für den internen Webservice. <p>i HINWEIS: Muss der One Identity Manager Service unter dem Benutzerkonto des Network Service (NT Authority\NetworkService) laufen, so können Sie die Rechte für den internen Webservice über folgenden Kommandozeilenaufruf vergeben:</p> <pre>netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"</pre>

Benutzer	Berechtigungen
	<p>Für die automatische Aktualisierung des One Identity Manager Services benötigt das Benutzerkonto Vollzugriff auf das One Identity Manager-Installationsverzeichnis.</p> <p>In der Standardinstallation wird der One Identity Manager installiert unter:</p> <ul style="list-style-type: none"> • %ProgramFiles(x86)%\One Identity (auf 32-Bit Betriebssystemen) • %ProgramFiles%\One Identity (auf 64-Bit Betriebssystemen)
Benutzer für den Zugriff auf die One Identity Manager-Datenbank	Um die Synchronisation über einen Anwendungsserver auszuführen, wird der Standard-Systembenutzer Synchronization bereitgestellt.

Einrichten des Synchronisationsservers

Für die Einrichtung der Synchronisation mit einem Unix-basierten Zielsystem muss ein Server zur Verfügung gestellt werden, auf dem die nachfolgend genannte Software installiert ist:

- Windows Betriebssystem

Unterstützt werden die Versionen:

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

HINWEIS: Beachten Sie die Empfehlungen des Zielsystemherstellers.

- One Identity Manager Service, Unix Konnektor
 - Installieren Sie die One Identity Manager Komponenten mit dem Installationsassistenten.
 1. Wählen Sie die Option **Installationsmodule mit vorhandener Datenbank auswählen.**
 2. Wählen Sie die Maschinenrolle **Server | Jobserver | Unix.**

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

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

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

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

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

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

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

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

1. Starten Sie das Programm Server Installer auf Ihrer administrativen Arbeitsstation.
2. Auf der Seite **Datenbankverbindung** geben Sie die gültigen Verbindungsdaten zur One Identity Manager-Datenbank ein.
3. Auf der Seite **Servereigenschaften** legen Sie fest, auf welchem Server der One Identity Manager Service installiert werden soll.
 - a. Wählen Sie in der Auswahlliste **Server** einen Jobserver aus.
- ODER -
Um einen neuen Jobserver zu erstellen, klicken Sie **Hinzufügen**.
 - b. Bearbeiten Sie folgende Informationen für den Jobserver.

Tabelle 3: Eigenschaften eines Jobserver

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

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

- Auf der Seite **Maschinenrollen** wählen Sie **Unix**.
- Auf der Seite **Serverfunktionen** wählen Sie mindestens eine der folgenden Serverfunktionen:
 - **Unix Konnektor**
 - **AIX Konnektor**
- Auf der Seite **Dienstkonfiguration** prüfen Sie die Konfiguration des One Identity Manager Service.

HINWEIS: Die initiale Konfiguration des Dienstes ist bereits vordefiniert. Sollte eine erweiterte Konfiguration erforderlich sein, können Sie diese auch zu einem späteren Zeitpunkt mit dem Designer durchführen. Ausführliche Informationen zur Konfiguration des Dienstes finden Sie im *One Identity Manager Konfigurationshandbuch*.
- Zur Konfiguration der Remote-Installation, klicken Sie **Weiter**.
- Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
- Auf der Seite **Installationsquelle festlegen** wählen Sie das Verzeichnis mit den Installationsdateien.
- Auf der Seite **Datenbankschlüsseldatei auswählen** wählen die Datei mit dem privaten Schlüssel.

HINWEIS: Diese Seite wird nur angezeigt, wenn die Datenbank verschlüsselt ist.
- Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den

Dienst.

Tabelle 4: Installationsinformationen

Eingabe	Beschreibung
Computer	Server, auf dem der Dienst installiert und gestartet wird. Um einen Server auszuwählen <ul style="list-style-type: none">• Erfassen Sie den Servernamen. - ODER -• Wählen Sie einen Eintrag in der Liste.
Dienstkonto	Angaben zum Benutzerkonto des One Identity Manager Service. Um ein Benutzerkonto für den One Identity Manager Service zu erfassen <ul style="list-style-type: none">• Aktivieren Sie die Option Lokales Systemkonto. Damit wird der One Identity Manager Service unter dem Konto NT AUTHORITY\SYSTEM gestartet. - ODER -• Erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung.
Installationskonto	Angaben zum administrativen Benutzerkonto für die Installation des Dienstes. Um ein administratives Benutzerkonto für die Installation zu erfassen <ul style="list-style-type: none">• Aktivieren Sie die Option Erweitert.• Aktivieren Sie die Option Angemeldeter Benutzer. Es wird das Benutzerkonto des aktuell angemeldeten Benutzers verwendet. - ODER -• Geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.

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

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

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

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

Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Unix Hosts

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

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

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

Detaillierte Informationen zum Thema

- [Benötigte Informationen für die Erstellung eines Synchronisationsprojektes](#) auf Seite 17
- [Erstellen eines initialen Synchronisationsprojektes](#) auf Seite 20
- [Anhang: Standardprojektvorlage für Unix-basierte Zielsysteme](#) auf Seite 134

Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

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

Tabelle 5: Benötigte Informationen für die Erstellung eines Synchronisationsprojektes

Angaben	Erläuterungen
Servername oder IP Adresse des Hosts	Vollständiger Name oder IP-Adresse des Hosts, gegen den sich der Synchronisationsserver verbindet, um auf die Unix Objekte zuzugreifen.
Kommunikationsport auf dem Host	Kommunikationsport auf dem Host zum Aufbau einer Secure Shell (SSH) Verbindung. Standardport ist TCP-Port 22.
Benutzerkonto und	Benutzerkonto und Kennwort zur Anmeldung am Host. Dieses

Angaben	Erläuterungen
Kennwort zur Anmeldung am Host	Benutzerkonto wird für den Zugriff auf den Host per SSH verwendet. Das Benutzerkonto benötigt die Berechtigung zum Aufbau einer SSH-Verbindung.
Methode, Benutzername und Kennwort zur Rechteerhöhung	<p>Für die Ausführung von Kommandos ist der Wechsel in den administrativen Kontext erforderlich. Stellen Sie ein Benutzerkonto mit ausreichenden administrativen Berechtigungen bereit. Mit diesem Benutzerkonto werden Schreiboperationen auf den Unix Objekten ausgeführt.</p> <p>Verfügbare Methoden sind:</p> <ul style="list-style-type: none"> • Default <p>Der Benutzer zur Anmeldung am Host besitzt bereits administrative Berechtigungen.</p> • Sudo <p>Der Benutzer zur Anmeldung am Host kann die administrativen Aufgaben mit den Berechtigungen eines anderen Benutzers , beispielsweise "root", ausführen. Die Konfiguration erfolgt über die sudoer-Datei auf dem Host.</p> • su <p>Diese Methode verwendet das su Kommando zum Kontextwechsel. Es wird ein weiterer Benutzer mit administrativen Berechtigungen benötigt.</p>
Synchronisationsserver für das Unix-basierte Zielsystem	<p>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.</p> <p>Auf dem Synchronisationsserver muss der One Identity Manager Service mit dem Unix Konnektor installiert sein.</p> <p>Der Synchronisationsserver muss im One Identity Manager als Jobserver bekannt sein. Verwenden Sie beim Einrichten des Jobserver die folgenden Eigenschaften.</p>

Angaben

Erläuterungen

Tabelle 6: Zusätzliche Eigenschaften für den Jobserver

Eigenschaft	Wert
Serverfunktion	Unix Konnektor AIX Konnektor
Maschinenrolle	Server/Jobserver/Unix

Verbindungsdaten zur One Identity Manager-Datenbank

- Datenbankserver
- Datenbank
- SQL Server Anmeldung und Kennwort
- Angabe, ob integrierte Windows-Authentifizierung verwendet wird. Die Verwendung dieser Authentifizierung wird nicht empfohlen. Sollten Sie dieses Verfahren dennoch einsetzen, stellen Sie sicher, dass Ihre Umgebung Windows-Authentifizierung 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 Remoteverbindungservers:

- One Identity Manager Service ist gestartet
- RemoteConnectPlugin ist installiert
- Unix Konnektor oder AIX Konnektor ist installiert

Der Remoteverbindungsserver muss im One Identity Manager als Jobserver bekannt sein. Es wird der Name des Jobservers benötigt.

- TIPP:** Der Remoteverbindungsserver benötigt dieselbe Konfiguration (bezüglich der installierten Software sowie der Berechtigungen des Benutzerkontos) wie der Synchronisationsserver. Nutzen Sie den Synchronisationsserver gleichzeitig als Remoteverbindungsserver, indem Sie lediglich das RemoteConnectPlugin zusätzlich installieren.

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

Verwandte Themen

- [Benutzer und Berechtigungen für die Synchronisation mit einem Unix-basierten Zielsystem](#) auf Seite 12
- [Einrichten des Synchronisationservers](#) auf Seite 13

Erstellen eines initialen Synchronisationsprojektes

- HINWEIS:** Der folgende Ablauf beschreibt die Einrichtung eines Synchronisationsprojektes, wenn der Synchronization Editor
- im Standardmodus ausgeführt wird und
 - aus dem Launchpad gestartet wird.

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

Um ein initiales Synchronisationsprojekt für ein Unix-basiertes Zielsystem einzurichten

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

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

2. Wählen Sie den Eintrag **Zielsystemtyp Unix** und klicken Sie **Starten**.
Der Projektassistent des Synchronization Editors wird gestartet.

3. Auf der Seite **Systemzugriff** legen Sie fest, wie der One Identity Manager auf das Zielsystem zugreifen kann.
 - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, möglich, nehmen Sie keine Einstellungen vor.
 - Ist der Zugriff von der Arbeitsstation, auf der Sie den Synchronization Editor gestartet haben, nicht möglich, können Sie eine Remoteverbindung herstellen.
Aktivieren Sie die Option **Verbindung über einen Remoteverbindungsserver herstellen** und wählen Sie unter **Jobserver** den Server, über den die Verbindung hergestellt werden soll.
4. Auf der Seite **Allgemeine Verbindungseinstellungen** erfassen Sie Verbindungsinformationen zum Unix-Host.
 - a. Geben Sie im Eingabefeld **Server oder IP** den Servernamen oder die IP-Adresse des Host ein.
 - b. Geben Sie im Eingabefeld **Port** den Kommunikationsport für den Aufbau der SSH-Verbindung an. Standard-Kommunikationsport ist der TCP-Port 22.
 - c. Erfassen Sie das Benutzerkonto und das Kennwort zur SSH-Anmeldung am Host.
 - d. Klicken Sie **Test**, um die Verbindung zu testen. Es wird versucht eine Verbindung zum Host aufzubauen.
5. Klicken Sie im Bereich **Verbindung prüfen** auf **Test**, um die Verbindung zum Host zu testen.
6. Auf der Seite **Wechsel in den administrativen Kontext** wählen Sie die Methode, die verwendet werden soll, um administrative Berechtigungen zu erhalten.
 - Wählen Sie die Methode "Default", wenn der Benutzer zur Anmeldung am Host bereits administrative Berechtigungen besitzt.
 - Wählen Sie die Methode "Sudo", wenn der am Host angemeldete Benutzer administrative Aufgaben als administrativer Benutzer ausführen kann. Erfassen die im Eingabefeld **Benutzername** den alternativen Benutzer, beispielsweise "root".
 - Wählen Sie die Methode "Su", wenn administrative Aufgaben mit einem anderen Benutzer ausgeführt werden sollen. Erfassen Sie in den Eingabefeldern **Benutzername** und **Kennwort** die Anmeldeinformationen des Benutzers. Standardbenutzer ist "root".
7. 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.
 - ① **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.
8. Der Assistent lädt das Zielsystemschemata. Abhängig von der Art des

Zielsystemzugriffs und der Größe des Zielsystems kann dieser Vorgang einige Minuten dauern.


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

Tabelle 7: Zielsystemzugriff festlegen

Option	Bedeutung
Das Zielsystem soll nur eingelesen werden.	<p>Angabe, ob nur ein Synchronisationsworkflow zum initialen Einlesen des Zielsystems in die One Identity Manager-Datenbank eingerichtet werden soll.</p> <p>Der Synchronisationsworkflow zeigt folgende Besonderheiten:</p> <ul style="list-style-type: none"> • 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.	<p>Angabe, ob zusätzlich zum Synchronisationsworkflow zum initialen Einlesen des Zielsystems ein Provisionierungsworkflow eingerichtet werden soll.</p> <p>Der Provisionierungsworkflow zeigt folgende Besonderheiten:</p> <ul style="list-style-type: none"> • 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.

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

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

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

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

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

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

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

Das Synchronisationsprojekt wird erstellt, gespeichert und sofort aktiviert.

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

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

Um den Inhalt des Synchronisationsprotokolls zu konfigurieren

- Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
- Um das Synchronisationsprotokoll für die Zielsystemverbindung zu konfigurieren, wählen Sie die Kategorie **Konfiguration | Zielsystem**.
- Um das Synchronisationsprotokoll für die Datenbankverbindung zu konfigurieren, wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.
- Wählen Sie den Bereich **Allgemein** und klicken Sie **Konfigurieren**.
- Wählen Sie den Bereich **Synchronisationsprotokoll** und aktivieren Sie **Synchronisationsprotokoll erstellen**.
- 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.

- Klicken Sie **OK**.

Um regelmäßige Synchronisationen auszuführen

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

Um die initiale Synchronisation manuell zu starten

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
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**.

HINWEIS:

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

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

Um die Benutzerkonten über Kontendefinitionen zu verwalten

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

Verwandte Themen

- [Synchronisationsergebnisse anzeigen](#) auf Seite 24
- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 25
- [Einrichten von Kontendefinitionen](#) auf Seite 38
- [Automatische Zuordnung von Personen zu Unix Benutzerkonten](#) auf Seite 105

Synchronisationsergebnisse anzeigen

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

Um das Protokoll einer Synchronisation anzuzeigen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht ►.
In der Navigationsansicht werden die Protokolle aller abgeschlossenen Synchronisationsläufe angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.
Die Auswertung der Synchronisation wird als Bericht angezeigt. Sie können diesen Bericht speichern.

Um das Protokoll einer Provisionierung anzuzeigen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Protokolle**.
3. Klicken Sie in der Symbolleiste der Navigationsansicht ⚡.
In der Navigationsansicht werden die Protokolle aller abgeschlossenen Provisionierungsprozesse angezeigt.
4. Wählen Sie per Maus-Doppelklick das Protokoll, das angezeigt werden soll.
Die Auswertung der Provisionierung wird als Bericht angezeigt. Sie können diesen Bericht speichern.

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

Aufbewahrungszeit der Protokolle konfigurieren

Synchronisationsprotokolle werden für einen festgelegten Zeitraum aufbewahrt.

Um den Aufbewahrungszeitraum für Synchronisationsprotokolle anzupassen

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

Anpassen einer Synchronisationskonfiguration

Mit dem Synchronization Editor haben Sie ein Synchronisationsprojekt für die initiale Synchronisation eines Unix Hosts eingerichtet. Mit diesem Synchronisationsprojekt können Sie Unix Objekte in die One Identity Manager-Datenbank einlesen. Wenn Sie

Benutzerkonten und ihre Berechtigungen mit dem One Identity Manager verwalten, werden Änderungen in das Unix-basierte Zielsystem provisioniert.

Um die Datenbank und das Unix-basierte Zielsystem regelmäßig abzugleichen und Änderungen zu synchronisieren, passen Sie die Synchronisationskonfiguration an.

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

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

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

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

Detaillierte Informationen zum Thema

- [Synchronisation in den Unix Host konfigurieren](#) auf Seite 27
- [Synchronisation verschiedener Unix Hosts konfigurieren](#) auf Seite 28
- [Schema aktualisieren](#) auf Seite 28

Synchronisation in den Unix Host konfigurieren

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

Um eine Synchronisationskonfiguration für die Synchronisation in den Unix Host zu erstellen

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Prüfen Sie, ob die bestehenden Mappings für die Synchronisation in genutzt werden können. Erstellen Sie bei Bedarf neue Mappings.
3. Erstellen Sie mit dem Workflowassistenten einen neuen Workflow.
Es wird ein Workflow mit der Synchronisationsrichtung **In das Zielsystem** angelegt.
4. Erstellen Sie eine neue Startkonfiguration. Nutzen Sie dabei den neu angelegten Workflow.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Detaillierte Informationen zum Thema

- [Synchronisation verschiedener Unix Hosts konfigurieren](#) auf Seite 28

Synchronisation verschiedener Unix Hosts konfigurieren

Voraussetzungen

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

Um ein Synchronisationsprojekt für die Synchronisation eines weiteren Hosts anzupassen

1. Stellen Sie im weiteren Host ein Benutzerkonto für die Synchronisation mit ausreichenden Berechtigungen bereit.
2. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
3. Erstellen Sie für den weiteren Host ein neues Basisobjekt. Verwenden Sie den Assistenten zur Anlage eines Basisobjektes.
 - Wählen Sie im Assistenten den Unix oder AIX Konnektor und geben Sie die Verbindungsparameter bekannt. Die Verbindungsparameter werden in einem spezialisierten Variablenset gespeichert.
Es wird eine Startkonfiguration erstellt, die das neu angelegte Variablenset verwendet.
4. Passen Sie bei Bedarf weitere Komponenten der Synchronisationskonfiguration an.
5. Speichern Sie die Änderungen.
6. Führen Sie eine Konsistenzprüfung durch.

Verwandte Themen

- [Synchronisation in den Unix Host konfigurieren](#) auf Seite 27

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

Um das Schema einer Systemverbindung zu aktualisieren

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Konfiguration | Zielsystem**.
- ODER -
Wählen Sie die Kategorie **Konfiguration | One Identity Manager Verbindung**.
3. Wählen Sie die Ansicht **Allgemein** und klicken Sie **Schema aktualisieren**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
Die Schemadaten werden neu geladen.

Um ein Mapping zu bearbeiten

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Kategorie **Mappings**.
3. Wählen Sie in der Navigationsansicht das Mapping.
Der Mappingeditor wird geöffnet. Ausführliche Informationen zum Bearbeiten von Mappings finden Sie im *One Identity Manager Referenzhandbuch für die Zielsystemsynchronisation*.

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

Nachbehandlung ausstehender Objekte

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

Ausstehende Objekte

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

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

Führen Sie dafür einen Zielsystemabgleich durch.

Um ausstehende Objekte nachzubearbeiten

1. Wählen Sie im Manager die Kategorie **Unix | Zielsystemabgleich: Unix**.

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

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

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




- Das Synchronisationsprotokoll wurde bereits gelöscht.
- ODER -
- Im Zielsystem wurde eine Zuweisung aus einer Mitgliederliste gelöscht.
Bei der Synchronisation wird das Basisobjekt der Zuordnung aktualisiert. Dafür erscheint ein Eintrag im Synchronisationsprotokoll. Der Eintrag in der Zuordnungstabelle wird als ausstehend markiert, es gibt jedoch keinen Eintrag im Synchronisationsprotokoll.
- Im Zielsystem wurde ein Objekt gelöscht, das eine Mitgliederliste enthält.
Bei der Synchronisation werden das Objekt und alle zugehörigen Einträge in Zuordnungstabellen als ausstehend markiert. Ein Eintrag im Synchronisationsprotokoll erscheint jedoch nur für das gelöschte Objekt.

TIPP:

Um die Objekteigenschaften eines ausstehenden Objekts anzuzeigen

- a. Wählen Sie auf dem Formular für den Zielsystemabgleich das Objekt.
 - b. Öffnen Sie das Kontextmenü und klicken Sie **Objekt anzeigen**.
3. Wählen Sie die Objekte, die Sie nachbearbeiten möchten. Mehrfachauswahl ist möglich.
 4. Klicken Sie in der Formularelementeiste eins der folgenden Symbole, um die jeweilige Methode auszuführen.

Tabelle 8: Methoden zur Behandlung ausstehender Objekte

Symbol	Methode	Beschreibung
	Löschen	Das Objekt wird sofort in der One Identity Manager-Datenbank gelöscht. Eine Löschverzögerung wird nicht berücksichtigt. Die Markierung Ausstehend wird für das Objekt entfernt. Indirekte Mitgliedschaften können nicht gelöscht werden.
	Publizieren	Das Objekt wird im Zielsystem eingefügt. Die Markierung Ausstehend wird für das Objekt entfernt. Die Methode löst das Ereignis HandleOutstanding aus. Dadurch wird ein zielsystemspezifischer Prozess ausgeführt, der den Provisionierungsprozess für das Objekt anstößt. Voraussetzungen: <ul style="list-style-type: none">• Das Publizieren ist für die Tabelle, die das Objekt enthält, zugelassen.• Der Zielsystemkonnektor kann schreibend auf das Zielsystem zugreifen.
	Zurücksetzen	Die Markierung Ausstehend wird für das Objekt entfernt.

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

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

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

Um die Massenverarbeitung zu deaktivieren

- Deaktivieren Sie in der Formularelementeiste .

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

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

Provisionierung von Mitgliedschaften konfigurieren

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

- Mitgliedschaften werden im Zielsystem in Form einer Liste als Eigenschaft eines Objekts gespeichert.
- 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 **Unix | Basisdaten zur Konfiguration | Zielsystemtypen**.
2. Wählen Sie in der Ergebnisliste den Zielsystemtyp **Unix**.
3. Wählen Sie die Aufgabe **Konfigurieren der Tabellen zum Publizieren**.
4. Wählen Sie die Zuordnungstabellen, für die Sie die Einzelprovisionierung ermöglichen möchten. Mehrfachauswahl ist möglich.
 - Die Option kann nur für Zuordnungstabellen aktiviert werden, deren Basistabelle eine Spalte XDateSubItem oder CCC_XDateSubItem hat.
 - Zuordnungstabellen, die im Mapping in einer virtuellen Schemaeigenschaft zusammengefasst sind, müssen identisch markiert werden.
5. Klicken Sie **Änderungen zusammenführen**.
6. Speichern Sie die Änderungen.

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

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

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

Beschleunigung der Provisionierung und Einzelobjektsynchronisation

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

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

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

Um die Lastverteilung zu konfigurieren

1. Konfigurieren Sie die Server und geben Sie diese im One Identity Manager als Jobserver bekannt.

- Weisen Sie diesen Jobservern die Serverfunktion **Unix Konnektor** zu.

Alle Jobserver müssen auf den gleichen Unix Host zugreifen können, wie der Synchronisationsserver für das jeweilige Basisobjekt.

2. Weisen Sie im Synchronization Editor an das Basisobjekt eine kundendefinierte Serverfunktion zu.

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

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

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

3. Weisen Sie diese Serverfunktion im Manager an alle Jobserver zu, welche die Prozesse zur Provisionierung und Einzelobjektsynchronisation für das Basisobjekt verarbeiten sollen.

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

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

Um den Synchronisationsserver ohne Lastverteilung zu nutzen

- Entfernen Sie im Synchronization Editor die Serverfunktion vom Basisobjekt.

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

Detaillierte Informationen zum Thema

- [Bearbeiten eines Servers](#) auf Seite 73

Unterstützung bei der Analyse von Synchronisationsproblemen

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

- Ergebnisse der Konsistenzprüfung
- Einstellungen zur Revisionsfilterung

- Verwendeter Scope
- Analyse des Synchronisationspuffers
- Zugriffszeiten auf die Objekte in der One Identity Manager-Datenbank und im Zielsystem

Um den Synchronisationsanalysebericht zu erstellen

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

Die Generierung des Berichts nimmt einige Zeit in Anspruch. Er wird in einem separaten Fenster angezeigt.

3. Drucken Sie den Bericht oder Speichern Sie ihn in einem der verschiedenen Ausgabeformate.

Deaktivieren der Synchronisation

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

Um regelmäßige Synchronisationen zu verhindern

1. Öffnen Sie das Synchronisationsprojekt im Synchronization Editor.
2. Wählen Sie die Startkonfiguration und deaktivieren Sie den hinterlegten Zeitplan.
Synchronisationen können nun nur noch manuell gestartet werden.

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

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

Um das Synchronisationsprojekt zu deaktivieren

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

Detaillierte Informationen zum Thema

- [Erstellen eines Synchronisationsprojektes für die initiale Synchronisation eines Unix Hosts](#) auf Seite 17

Basisdaten für Unix-basierte Zielsysteme

Für die Verwaltung eines Unix-basierten Zielsystems im One Identity Manager sind folgende Basisdaten relevant.

- Konfigurationsparameter

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

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

Weitere Informationen finden Sie unter [Anhang: Konfigurationsparameter für die Verwaltung einer Unix-Umgebung](#) auf Seite 131.

- Kontendefinitionen

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

Weitere Informationen finden Sie unter [Einrichten von Kontendefinitionen](#) auf Seite 38.

- Kennwortrichtlinien

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

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

Weitere Informationen finden Sie unter [Kennwortrichtlinien für Unix Benutzerkonten](#) auf Seite 58.

- Initiales Kennwort für neue Benutzerkonten

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

Weitere Informationen finden Sie unter [Initiales Kennwort für neue Unix Benutzerkonten](#) auf Seite 69.

- E-Mail-Benachrichtigungen über die Anmeldeinformationen

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

Weitere Informationen finden Sie unter [E-Mail-Benachrichtigungen über Anmeldeinformationen](#) auf Seite 70.

- Zielsystemtypen

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

Weitere Informationen finden Sie unter [Nachbehandlung ausstehender Objekte](#) auf Seite 30.

- Zielsystemverantwortliche

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

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

Weitere Informationen finden Sie unter [Zielsystemverantwortliche](#) auf Seite 71.

- Server

Für die Verarbeitung der Unix-spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehört beispielsweise der Synchronisationsserver.

Weitere Informationen finden Sie unter [Bearbeiten eines Servers](#) auf Seite 73.

Einrichten von Kontendefinitionen

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

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


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

Für den Einsatz einer Kontendefinition sind die folgenden Schritte erforderlich:

- [Erstellen einer Kontendefinition](#)
- [Erstellen der Automatisierungsgrade](#)
- [Erstellen einer Abbildungsvorschrift für IT Betriebsdaten](#)
- [Erfassen der IT Betriebsdaten](#)
- [Zuweisen der Kontendefinition an Personen](#)
- [Zuweisen der Kontendefinition an ein Zielsystem](#)

Erstellen einer Kontendefinition

Um eine Kontendefinition zu erstellen

1. Wählen Sie im Manager die Kategorie **Unix | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
-ODER-
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten der Kontendefinition.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- [Stammdaten einer Kontendefinition](#) auf Seite 39

Stammdaten einer Kontendefinition

Für eine Kontendefinition erfassen Sie die folgenden Stammdaten.

Tabelle 9: Stammdaten einer Kontendefinition

Eigenschaft	Beschreibung
Kontendefinition	Bezeichnung der Kontendefinition.
Benutzerkontentabelle	Tabelle im One Identity Manager Schema, welche die Benutzerkonten abbildet.
Zielsystem	Zielsystem für das die Kontendefinition gelten soll.
Vorausgesetzte Kontendefinition	Vorausgesetzte Kontendefinition. Definieren Sie Abhängigkeiten zwischen Kontendefinitionen. Wenn die Kontendefinition bestellt oder zugeordnet wird, wird die vorausgesetzte Kontendefinition automatisch mitbestellt oder zugeordnet. Für einen Unix Host lassen Sie die Angabe leer.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
Automatisierungsgrad (initial)	Standardautomatisierungsgrad, der bei Neuanlage von Benutzerkonten standardmäßig verwendet werden soll.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Kontendefinition an Personen. Erfassen Sie einen Wert zwischen 0 und 1. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter QER CalculateRiskIndex aktiviert ist. Ausführliche Informationen finden Sie im <i>One Identity Manager Administrationshandbuch für Risikobewertungen</i> .
Leistungsposition	Leistungsposition, über welche die Kontendefinition im IT Shop bestellt wird. Weisen Sie eine vorhandene Leistungsposition zu oder legen Sie eine neue Leistungsposition an.
IT Shop	Angabe, ob die Kontendefinition über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von ihren Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Die kann weiterhin direkt an Personen und Rollen außerhalb des IT Shop zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Kontendefinition ausschließlich über den IT Shop bestellbar ist. Die Kontendefinition kann über das Web Portal von den Mitarbeitern bestellt werden und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Kontendefinition an Rollen außerhalb des IT Shop ist nicht zulässig.

Eigenschaft	Beschreibung
Automatische Zuweisung zu Personen	<p>Angabe, ob die Kontendefinition automatisch an alle internen Personen zugewiesen werden soll. Beim Speichern wird die Kontendefinition an jede Person zugewiesen, die nicht als extern markiert ist. Sobald eine Person neu angelegt wird, erhält sie ebenfalls automatisch diese Kontendefinition.</p> <p>! WICHTIG: Aktivieren Sie diese Option nur, wenn sichergestellt ist, dass alle aktuell in der Datenbank vorhandenen internen Personen sowie alle zukünftig neu hinzuzufügenden internen Personen ein Benutzerkonto in diesem Zielsystem erhalten sollen!</p> <p>Um die automatische Zuweisung der Kontendefinition an alle Personen zu entfernen, deaktivieren Sie die Option. Ab diesem Zeitpunkt wird die Kontendefinition nicht neu an Personen zugewiesen. Bestehende Zuweisungen der Kontendefinition bleiben jedoch erhalten.</p>
Kontendefinition bei dauerhafter Deaktivierung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an dauerhaft deaktivierte Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei zeitweiliger Deaktivierung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an zeitweilig deaktivierte Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei verzögertem Löschen beibehalten	<p>Angabe zur Zuweisung der Kontendefinition bei verzögertem Löschen von Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>
Kontendefinition bei Sicherheitsgefährdung beibehalten	<p>Angabe zur Zuweisung der Kontendefinition an sicherheitsgefährdende Personen.</p> <p>Option aktiviert: Die Zuweisung der Kontendefinition bleibt wirksam. Das Benutzerkonto bleibt erhalten.</p> <p>Option nicht aktiviert: Die Zuweisung der Kontendefinition ist nicht wirksam. Das zugehörige Benutzerkonto wird gelöscht.</p>

Eigenschaft	Beschreibung
Ressourcentyp	Ressourcentyp zur Gruppierung von Kontendefinitionen.
Freies Feld 01- Freies Feld 10	Zusätzliche unternehmensspezifische Informationen. Die Anzeigenamen, Formate und Bildungsregeln für die Eingabefelder können Sie mit dem Designer an Ihre Anforderungen anpassen.

Erstellen der Automatisierungsgrade

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

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

Der One Identity Manager liefert eine Standardkonfiguration für die Automatisierungsgrade:

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

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

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

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


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

Um Automatisierungsgrade an eine Kontendefinition zuzuweisen

1. Wählen Sie im Manager die Kategorie **Unix | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Automatisierungsgrade zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Automatisierungsgrade zu.
- ODER -
Entfernen Sie im Bereich **Zuordnungen entfernen** die Automatisierungsgrade.
5. Speichern Sie die Änderungen.

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

Um einen Automatisierungsgrad zu bearbeiten

1. Wählen Sie die Kategorie **Unix | Basisdaten zur Konfiguration | Kontendefinitionen | Automatisierungsgrade**.
2. Wählen Sie in der Ergebnisliste einen Automatisierungsgrad aus. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
-ODER-
Klicken Sie in der Ergebnisliste .
3. Bearbeiten Sie die Stammdaten des Automatisierungsgrades.
4. Speichern Sie die Änderungen.

Verwandte Themen

- [Stammdaten eines Automatisierungsgrades](#) auf Seite 42

Stammdaten eines Automatisierungsgrades

Für einen Automatisierungsgrad erfassen Sie die folgenden Stammdaten.

Tabelle 10: Stammdaten eines Automatisierungsgrades

Eigenschaft	Beschreibung
Automatisierungsgrad	Bezeichnung des Automatisierungsgrades.
Beschreibung	Freitextfeld für zusätzliche Erläuterungen.
IT Betriebsdaten überschreibend	Angabe, ob Daten an Benutzerkonten, die sich aus den IT Betriebsdaten bilden, automatisch aktualisiert werden. Zulässige Werte sind: <ul style="list-style-type: none">• Niemals: Die Daten werden nicht aktualisiert.• Immer: Die Daten werden immer aktualisiert.• Nur initial: Die Daten werden nur initial ermittelt.
Gruppen bei zeitweiliger Deaktivierung beibehalten	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei zeitweiliger Deaktivierung sperren	Angabe, ob die Benutzerkonten zeitweilig deaktivierter Personen gesperrt werden sollen.
Gruppen bei dauerhafter Deaktivierung beibehalten	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei dauerhafter Deaktivierung sperren	Angabe, ob die Benutzerkonten dauerhaft deaktivierter Personen gesperrt werden sollen.
Gruppen bei verzögertem Löschen beibehalten	Angabe, ob die Benutzerkonten zum Löschen markierter Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei verzögertem Löschen sperren	Angabe, ob die Benutzerkonten zum Löschen markierter Personen gesperrt werden sollen.
Gruppen bei Sicherheitsgefährdung beibehalten	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen ihre Gruppenmitgliedschaften behalten sollen.
Benutzerkonten bei Sicherheitsgefährdung sperren	Angabe, ob die Benutzerkonten von sicherheitsgefährdenden Personen gesperrt werden sollen.
Gruppen bei deaktiviertem Benutzerkonto beibehalten	Angabe, ob deaktivierte Benutzerkonten ihre Gruppenmitgliedschaften behalten sollen.

Erstellen einer Abbildungsvorschrift für IT Betriebsdaten

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

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

- Login-Shell
- Gruppen erbbar
- Identität
- Privilegiertes Benutzerkonto

Um eine Abbildungsvorschrift für die IT Betriebsdaten zu erstellen

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

Tabelle 11: Abbildungsvorschrift für IT Betriebsdaten

Eigenschaft	Beschreibung
Spalte	Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird. In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript <code>TSB_ITDataFromOrg</code> verwenden. Ausführliche Informationen dazu finden Sie im <i>One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul</i> .
Quelle	Angabe, welche Rolle verwendet wird, um die Eigenschaften für das Benutzerkonto zu ermitteln. Zur Auswahl stehen: <ul style="list-style-type: none">• Primäre Abteilung• Primärer Standort• Primäre Kostenstelle• Primäre Geschäftsrolle <p>HINWEIS: Verwenden Sie die primäre Geschäftsrolle nur, wenn das Geschäftsrollenmodul vorhanden ist.</p>

Eigenschaft	Beschreibung
	<ul style="list-style-type: none"> keine Angabe <p>Wenn Sie keine Rolle auswählen, müssen Sie einen Standardwert festlegen und die Option Immer Standardwert verwenden setzen.</p>
Standardwert	Standardwert der Eigenschaft für das Benutzerkonto einer Person, wenn der Wert nicht dynamisch aus den IT Betriebsdaten einer Rolle ermittelt werden kann.
Immer Standardwert verwenden	Angabe, ob die Eigenschaft des Benutzerkontos immer mit dem Standardwert besetzt wird. Es erfolgt keine dynamische Ermittlung der IT Betriebsdaten aus einer Rolle.
Benachrichtigung bei Verwendung des Standards	Angabe, ob bei Verwendung des Standardwertes eine E-Mail Benachrichtigung an ein definiertes Postfach versendet wird. Es wird die Mailvorlage Person - Erstellung neues Benutzerkontos mit Standardwerten verwendet. Um die Mailvorlage zu ändern, passen Sie den Konfigurationsparameter TargetSystem Unix Accounts MailTemplateDefaultValues an.

4. Speichern Sie die Änderungen.

Verwandte Themen

- [Erfassen der IT Betriebsdaten](#) auf Seite 45

Erfassen der IT Betriebsdaten

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

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

Beispiel

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

Erstellen Sie eine Kontendefinition A für die Standardbenutzerkonten des Hosts A und eine Kontendefinition B für die administrativen Benutzerkonten des Hosts 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 den Host A fest. Diese IT Betriebsdaten werden für die Standardbenutzerkonten verwendet. Zusätzlich legen Sie für die Abteilung A die wirksamen IT Betriebsdaten für die Kontendefinition B fest. Diese IT Betriebsdaten werden für administrative Benutzerkonten verwendet.

Um IT Betriebsdaten festzulegen

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

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

Tabelle 12: IT Betriebsdaten

Eigenschaft	Beschreibung
Wirksam für	<p>Anwendungsbereich der IT Betriebsdaten. Die IT Betriebsdaten können für ein Zielsystem oder für eine definierte Kontendefinition verwendet werden.</p> <p>Um den Anwendungsbereich festzulegen</p> <ol style="list-style-type: none">Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.Wählen Sie unter Tabelle die Tabelle, die das Zielsystem abbildet oder für eine Kontendefinition die Tabelle TSBAccountDef.Wählen Sie unter Wirksam für das konkrete Zielsystem oder die konkrete Kontendefinition.Klicken Sie OK.
Spalte	<p>Eigenschaft des Benutzerkontos, für die der Wert gesetzt wird.</p> <p>In der Auswahlliste werden die Spalten angeboten, die in ihrer Bildungsregel das Skript TSB_ITDataFromOrg verwenden. Ausführliche Informationen dazu finden Sie im <i>One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul</i>.</p>
Wert	<p>Konkreter Wert, welcher der Eigenschaft des Benutzerkontos zugewiesen werden soll.</p>

4. Speichern Sie die Änderungen.

Verwandte Themen

- [Erstellen einer Abbildungsvorschrift für IT Betriebsdaten](#) auf Seite 44

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, Kostenstelle, Geschäftsrolle oder eines Standorts wurden geändert.
- ODER -
- Die Standardwerte in der IT Betriebsdaten Abbildungsvorschrift für eine Kontendefinition wurden geändert.

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

Um die Bildungsregeln auszuführen

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

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

Alter Aktueller Wert der Objekteigenschaft.
Wert:

Neuer Wert, den die Objekteigenschaft durch die Änderung an den
Wert: IT Betriebsdaten annehmen würde.

Auswahl: Angabe, ob die Änderung für das Benutzerkonto übernommen werden soll.

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

Für alle markierten Benutzerkonten und Eigenschaften werden die Bildungsregeln ausgeführt.

Zuweisen der Kontendefinition an Personen

Kontendefinitionen werden an die Personen des Unternehmens zugewiesen.

Das Standardverfahren für die Zuweisung von Kontendefinitionen an Personen ist die indirekte Zuweisung. Die Kontendefinitionen werden an die Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen zugewiesen. Die Personen werden gemäß ihrer Funktion im Unternehmen in diese Abteilungen, Kostenstellen, Standorte oder Geschäftsrollen

eingeordnet und erhalten so ihre Kontendefinitionen. Um auf Sonderanforderungen zu reagieren, können einzelne Kontendefinitionen direkt an Personen zugewiesen werden.

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

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

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

Voraussetzungen für die indirekte Zuweisung von Kontendefinitionen an Personen

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

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


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

Detaillierte Informationen zum Thema

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 50
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 50
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 51
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 52
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 52
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 53

Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Unix | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
 2. Wählen Sie in der Ergebnisliste die Kontendefinition.
 3. Wählen Sie die Aufgabe **Organisationen zuweisen**.
 4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Organisationen zu.
 - Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
 - Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
 - Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.
- TIPP:** Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Organisationen entfernen.
- Um eine Zuweisung zu entfernen**
- Wählen Sie die Organisation und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 50
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 51
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 52
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 52
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 53

Kontendefinition an Geschäftsrollen zuweisen

Installierte Module: Geschäftsrollenmodul

Um Kontendefinitionen in eine hierarchische Rolle aufzunehmen

1. Wählen Sie im Manager die Kategorie **Unix | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
2. Wählen Sie in der Ergebnisliste eine Kontendefinition.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Geschäftsrolle und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 50
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 51
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 52
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 52
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 53

Kontendefinition an alle Personen zuweisen

Um eine Kontendefinition an alle Personen zuzuweisen

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

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

5. Speichern Sie die Änderungen.

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

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

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 50
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 50
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 52
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 52
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 53

Kontendefinition direkt an Personen zuweisen

Um eine Kontendefinition direkt an Personen zuzuweisen

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Person und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 50
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 50
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 51
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 52
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 53

Kontendefinition an Systemrollen zuweisen

Installierte Module: Systemrollenmodul

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

Um Kontendefinitionen in eine Systemrolle aufzunehmen

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Systemrolle und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Verwandte Themen

- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 50
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 50
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 51
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 52
- [Kontendefinition in den IT Shop aufnehmen](#) auf Seite 53

Kontendefinition in den IT Shop aufnehmen

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

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

TIPP: Im Web Portal werden alle bestellbaren Produkte nach Servicekategorien zusammengestellt. Damit die Kontendefinition im Web Portal leichter gefunden werden kann, weisen Sie der Leistungsposition eine Servicekategorie zu.

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

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

Um eine Kontendefinition in den IT Shop aufzunehmen

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

Um eine Kontendefinition aus einzelnen Regalen des IT Shops zu entfernen

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

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

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

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

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

Verwandte Themen

- [Stammdaten einer Kontendefinition](#) auf Seite 39
- [Kontendefinition an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 50
- [Kontendefinition an Geschäftsrollen zuweisen](#) auf Seite 50
- [Kontendefinition an alle Personen zuweisen](#) auf Seite 51
- [Kontendefinition direkt an Personen zuweisen](#) auf Seite 52
- [Kontendefinition an Systemrollen zuweisen](#) auf Seite 52

Zuweisen der Kontendefinition an ein Zielsystem

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

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

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

Um die Kontendefinition an ein Zielsystem zuzuweisen

1. Wählen Sie im Manager in der Kategorie **Unix | Hosts** den Host.
2. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie in der Auswahlliste **Kontendefinition (initial)** die Kontendefinition für die Benutzerkonten.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- [Automatische Zuordnung von Personen zu Unix Benutzerkonten](#) auf Seite 105

Löschen einer Kontendefinition


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

Um eine Kontendefinition zu löschen

1. Entfernen Sie die automatische Zuweisung der Kontendefinition an alle Personen.
 - a. Wählen Sie im Manager die Kategorie **Unix | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
 - b. Wählen Sie in der Ergebnisliste die Kontendefinition.
 - c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
 - d. Deaktivieren Sie auf dem Tabreiter **Allgemein** die Option **Automatische Zuweisung zu Personen**.
 - e. Speichern Sie die Änderungen.
2. Entfernen Sie die direkte Zuordnung der Kontendefinition zu Personen.
 - a. Wählen Sie im Manager die Kategorie **Unix | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
 - b. Wählen Sie in der Ergebnisliste die Kontendefinition.
 - c. Wählen Sie die Aufgabe **An Personen zuweisen**.
 - d. Entfernen Sie im Bereich **Zuordnungen entfernen** die Personen.
 - e. Speichern Sie die Änderungen.
3. Entfernen Sie die Zuordnung der Kontendefinition zu Abteilungen, Kostenstellen und Standorten.
 - a. Wählen Sie im Manager die Kategorie **Unix | 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 **Unix | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
 - b. Wählen Sie in der Ergebnisliste die Kontendefinition.
 - c. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
Entfernen Sie im Bereich **Zuordnungen entfernen** die Geschäftsrollen.
 - d. Speichern Sie die Änderungen.
5. Wenn die Kontendefinition über den IT Shop bestellt wurde, muss sie abbestellt und aus allen IT Shop Regalen entfernt werden.

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

Um eine Kontendefinition aus allen Regalen des IT Shops zu entfernen

- a. Wählen Sie im Manager die Kategorie **Unix | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen** (bei nicht-rollenbasierter Anmeldung).
- ODER -
Wählen Sie im Manager die Kategorie **Berechtigungen | Kontendefinitionen** (bei rollenbasierter Anmeldung).
 - b. Wählen Sie in der Ergebnisliste die Kontendefinition.
 - c. Wählen Sie die Aufgabe **Entfernen aus allen Regalen (IT Shop)**.
 - d. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
 - e. Klicken Sie **OK**.
Die Kontendefinition wird durch den One Identity Manager Service aus allen Regalen entfernt. Dabei werden sämtliche Bestellungen und Zuweisungsbestellungen mit dieser Kontendefinition abbestellt.
6. Entfernen Sie die Zuordnung der Kontendefinition als vorausgesetzte Kontendefinition einer anderen Kontendefinition. Solange die Kontendefinition Voraussetzung einer anderen Kontendefinition ist, kann sie nicht gelöscht werden. Prüfen Sie alle Kontendefinitionen.
- a. Wählen Sie im Manager die Kategorie **Unix | 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 **Unix | Hosts** den Host.
 - 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 **Unix | Basisdaten zur Konfiguration | Kontendefinitionen | Kontendefinitionen**.
 - b. Wählen Sie in der Ergebnisliste die Kontendefinition.
 - c. Klicken Sie , um die Kontendefinition zu löschen.

Kennwortrichtlinien für Unix Benutzerkonten

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

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

Detaillierte Informationen zum Thema

- [Vordefinierte Kennwortrichtlinien](#) auf Seite 58
- [Anwenden einer Kennwortrichtlinie](#) auf Seite 59
- [Bearbeiten von Kennwortrichtlinien](#) auf Seite 61
- [Kundenspezifische Skripte für Kennwortanforderungen](#) auf Seite 65
- [Ausschlussliste für Kennwörter](#) auf Seite 68
- [Prüfen eines Kennwortes](#) auf Seite 68
- [Generieren eines Kennwortes testen](#) auf Seite 68

Vordefinierte Kennwortrichtlinien

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

Kennwortrichtlinie für die Anmeldung am One Identity Manager

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

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

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

Kennwortrichtlinie für die Bildung des zentralen Kennwortes von Personen

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

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

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

Kennwortrichtlinien für Benutzerkonten

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

- ❗ **WICHTIG:** Wenn Sie nicht mit zielsystemspezifischen Kennwortrichtlinien arbeiten, wirkt die Standardrichtlinie **One Identity Manager Kennwortrichtlinie**. Stellen Sie in diesem Fall sicher, dass die Standardrichtlinie nicht gegen die Anforderungen der Zielsysteme verstößt.
- ❗ **HINWEIS:** Bei der Aktualisierung von One Identity Manager Version 7.x auf One Identity Manager Version 8.1.1 werden die Einstellung der Konfigurationsparameter zur Bildung von Kennwörtern auf die zielsystemspezifischen Kennwortrichtlinien umgesetzt.

Für Unix-basierte Zielsysteme ist die Kennwortrichtlinie **Unix Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Unix Benutzerkonten (`UNIXAccount.UserPassword`) eines Unix Hosts anwenden.

Wenn die Kennwortanforderungen der Hosts unterschiedlich sind, wird empfohlen, je Host eine eigene Kennwortrichtlinie einzurichten.

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

Anwenden einer Kennwortrichtlinie

Für Unix-basierte Zielsysteme ist die Kennwortrichtlinie **Unix Kennwortrichtlinie** vordefiniert. Diese Kennwortrichtlinie können Sie auf die Kennwörter der Unix Benutzerkonten (`UNIXAccount.UserPassword`) eines Unix Hosts anwenden.

Wenn die Kennwortanforderungen der Hosts unterschiedlich sind, wird empfohlen, je Host 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 Hosts des Benutzerkontos
4. Kennwortrichtlinie **One Identity Manager Kennwortrichtlinie** (Standardrichtlinie)

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

Um eine Kennwortrichtlinie neu zuzuweisen

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

Tabelle 13: Zuweisen einer Kennwortrichtlinie

Eigenschaft	Beschreibung
Anwenden auf	Anwendungsbereich der Kennwortrichtlinie. Um den Anwendungsbereich festzulegen <ol style="list-style-type: none">a. Klicken Sie auf die Schaltfläche → neben dem Eingabefeld.b. Wählen Sie unter Tabelle eine der folgenden Referenzen:<ul style="list-style-type: none">• 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.

Eigenschaft	Beschreibung
	<p>c. Wählen Sie unter Anwenden auf die Tabelle, die die Basisobjekte enthält.</p> <ul style="list-style-type: none"> • 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. <p>d. Klicken Sie OK.</p>
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 **Unix | Basisdaten zur Konfiguration | Kennwortrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Objekte zuweisen**.
4. Wählen Sie im Bereich **Zuweisungen** die Zuweisung, die Sie ändern möchten.
5. Wählen Sie in der Auswahlliste **Kennwortrichtlinie** die neu anzuwendende Kennwortrichtlinie.
6. Speichern Sie die Änderungen.

Bearbeiten von Kennwortrichtlinien

Um eine Kennwortrichtlinie zu bearbeiten

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

-ODER-

Klicken Sie in der Ergebnisliste .

3. Bearbeiten Sie die Stammdaten der Kennwortrichtlinie.
4. Speichern Sie die Änderungen.




Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten einer Kennwortrichtlinie](#) auf Seite 62
- [Richtlinieneinstellungen](#) auf Seite 62
- [Zeichenklassen für Kennwörter](#) auf Seite 64
- [Kundenspezifische Skripte für Kennwortanforderungen](#) auf Seite 65

Allgemeine Stammdaten einer Kennwortrichtlinie

Für eine Kennwortrichtlinie erfassen Sie folgende allgemeine Stammdaten.

Tabelle 14: Stammdaten einer Kennwortrichtlinie

Eigenschaft	Bedeutung
Anzeigename	Bezeichnung der Kennwortrichtlinie. Übersetzen Sie den eingegebenen Text über die Schaltfläche  .
Beschreibung	Freitextfeld für zusätzliche Erläuterungen. Übersetzen Sie den eingegebenen Text über die Schaltfläche  .
Fehlermeldung	Kundenspezifische Fehlermeldung, die ausgegeben wird, wenn die Richtlinie nicht erfüllt wird. Übersetzen Sie den eingegebenen Text über die Schaltfläche  .
Eigentümer (Anwendungsrolle)	Anwendungsrolle, deren Mitglieder die Kennwortrichtlinie konfigurieren können.
Standardrichtlinie	Kennzeichnung als Standardrichtlinie für Kennwörter.

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

Richtlinieneinstellungen

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

Tabelle 15: Richtlinieneinstellungen

Eigenschaft	Bedeutung
Initiales Kennwort	Initiales Kennwort für neu erzeugte Benutzerkonten. Wird beim Erstellen eines Benutzerkontos kein Kennwort angegeben oder kein Zufallskennwort generiert, dann wird das initiale Kennwort benutzt.
Kennwortbestätigung	Kennwortwiederholung.
Min. Länge	Minimale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben muss.
Max. Länge	Maximale Länge des Kennwortes. Geben Sie die Anzahl von Zeichen an, die ein Kennwort haben kann.
Max. Fehlanmeldungen	<p>Anzahl der maximalen Fehlanmeldungen. Legen Sie die Anzahl der ungültigen Kennworteingaben fest. Wird nur berücksichtigt, bei Anmeldung am One Identity Manager.</p> <p>Die Angabe wird nur berücksichtigt, wenn die Anmeldung am One Identity Manager mit einem Systembenutzer- oder Personen-basierten Authentifizierungsmodul erfolgt. Hat ein Benutzer die Anzahl der maximalen Fehlanmeldungen erreicht, kann sich die Person oder der Systembenutzer nicht mehr am One Identity Manager anmelden.</p> <p>Kennwörter gesperrter Personen und Systembenutzer können im Kennworrücksetzungsportal zurückgesetzt werden. Ausführliche Informationen finden Sie im <i>One Identity Manager Anwenderhandbuch für das Web Portal</i>.</p>
Max. Tage gültig	Maximales Alter des Kennwortes. Geben Sie die Zeitspanne an, in der ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird.
Kennwortchronik	Anzahl der zu speichernden Kennwörter. Wird beispielsweise der Wert 5 eingegeben, werden die letzten fünf Kennwörter des Benutzers gespeichert.
Min. Kennwortstärke	Angabe, wie sicher ein Kennwort sein muss. Je höher die Kennwortstärke, desto sicherer ist das Kennwort. Mit dem Wert 0 wird die Kennwortstärke nicht geprüft. Die Werte 1 , 2 , 3 und 4 geben die erforderliche Komplexität des Kennwortes an. Dabei stellt der Wert 1 die geringsten Anforderungen an die Komplexität eines Kennwortes. Der Wert 4 fordert die höchste Komplexität.
Namensbestandteile unzulässig	Angabe, ob Namensbestandteile im Kennwort zulässig oder unzulässig sind. Ist die Option aktiviert, sind Namensbestandteile in Kennwörtern nicht zulässig. Es werden die Werte der Spalten berücksichtigt, für welche die

Eigenschaft	Bedeutung
	Option Enthält Namensbestandteile für die Kennwortprüfung aktiviert ist. Die Option passen Sie im Designer an der Spaltendefinition an. Ausführliche Informationen finden Sie im <i>One Identity Manager Konfigurationshandbuch</i> .

Zeichenklassen für Kennwörter

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

Tabelle 16: Zeichenklassen für Kennwörter

Eigenschaft	Bedeutung
Min. Anzahl Buchstaben	Angabe, wie viele alphabetische Zeichen ein Kennwort mindestens enthalten muss.
Min. Anzahl Kleinbuchstaben	Angabe, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Großbuchstaben	Angabe, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.
Min. Anzahl Ziffern	Angabe, wie viele Ziffern ein Kennwort mindestens enthalten muss.
Min. Anzahl Sonderzeichen	Angabe, wie viele Sonderzeichen ein Kennwort mindestens enthalten muss.
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.
Kleinbuchstaben nicht erlaubt	Angabe, ob das Kennwort Kleinbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Großbuchstaben nicht erlaubt	Angabe, ob das Kennwort Großbuchstaben enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.

Eigenschaft	Bedeutung
Ziffern nicht erlaubt	Angabe, ob das Kennwort Ziffern enthalten darf. Die Einstellung wird nur beim Generieren von Kennwörtern berücksichtigt.
Sonderzeichen nicht erlaubt	Angabe, ob das Kennwort Sonderzeichen enthalten darf. 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 65
- [Skript zum Generieren eines Kennwortes](#) auf Seite 66

Skript zum Prüfen eines Kennwortes

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

Syntax für Prüfskripte

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

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Kennwort, das zu prüfen ist

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

Beispiel für ein Skript zum Prüfen eines Kennwortes

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

```

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

```

Um ein kundenspezifisches Skript zum Prüfen eines Kennwortes zu verwenden

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

Skript zum Generieren eines Kennwortes

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

Syntax für Generierungsskripte

```

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

```

Mit Parametern:

policy = Kennwortrichtlinienobjekt

spwd = Generiertes Kennwort

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

Beispiel für ein Skript zum Generieren eines Kennwortes

Das Skript ersetzt die unzulässigen Zeichen ? und ! in Zufallskennwörtern.

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

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

```
End Sub
```

Um ein kundenspezifisches Skript zum Generieren eines Kennwortes zu verwenden

1. Erstellen Sie im Designer in der Kategorie **Skriptbibliothek** Ihr Skript.
2. Bearbeiten Sie die Kennwortrichtlinie.
 - a. Wählen Sie im Manager die Kategorie **Unix | 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 65

Ausschlussliste für Kennwörter

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

HINWEIS: Die Ausschlussliste ist global für alle Kennwortrichtlinien gültig.

Um einen Begriff in die Ausschlussliste aufzunehmen

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

Prüfen eines Kennwortes

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

Um zu prüfen, ob ein Kennwort der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **Unix | Basisdaten zur Konfiguration | Kennwortrichtlinien**.
2. Wählen Sie in der Ergebnisliste die Kennwortrichtlinie.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Wählen Sie den Tabreiter **Test**.
5. Wählen Sie in der Auswahlliste **Basisobjekt für den Test** die Tabelle und das Objekt für die Prüfung.
6. Geben Sie im Eingabefeld **Kennwort überprüfen** das Kennwort ein.
Neben dem Eingabefeld wird angezeigt, ob das Kennwort gültig ist.

Generieren eines Kennwortes testen

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

Um ein Kennwort zu generieren, das der Kennwortrichtlinie entspricht

1. Wählen Sie im Manager die Kategorie **Unix | 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 Unix Benutzerkonten

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

- Erstellen Sie Benutzerkonten manuell und tragen Sie in den Stammdaten der Benutzerkonten ein Kennwort ein.
- Vergeben Sie beim Erstellen von Benutzerkonten ein zufällig generiertes initiales Kennwort.
 - Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | Unix | Accounts | InitialRandomPassword**.
 - Verwenden Sie zielsystemspezifische Kennwortrichtlinien und definieren Sie in den Kennwortrichtlinien die Zeichenklassen, die das Kennwort enthalten muss.
 - Legen Sie fest, an welche Person das initiale Kennwort per E-Mail versendet wird.
- Verwenden Sie das zentrale Kennwort der Person. Das zentrale Kennwort der zugeordneten Person wird auf das Kennwort des Benutzerkontos abgebildet. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Verwandte Themen

- [Kennwortrichtlinien für Unix Benutzerkonten](#) auf Seite 58
- [E-Mail-Benachrichtigungen über Anmeldeinformationen](#) auf Seite 70

E-Mail-Benachrichtigungen über Anmeldeinformationen

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

Um Benachrichtigungen zu nutzen, sind folgende Voraussetzungen zu erfüllen:

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

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

Um die initialen Anmeldeinformationen per E-Mail zu versenden

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

Es wird standardmäßig eine Benachrichtigung mit der Mailvorlage **Person - Erstellung neues Benutzerkonto** versendet. Die Benachrichtigung enthält den Namen des Benutzerkontos.

4. Aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | Unix | Accounts | InitialRandomPassword | SendTo | MailTemplatePassword**.

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

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

Zielsystemverantwortliche

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

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

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

Inbetriebnahme der Anwendungsrollen für Zielsystemverantwortliche

1. Der One Identity Manager Administrator legt Personen als Zielsystemadministratoren fest.
2. Die Zielsystemadministratoren nehmen die Personen in die Standardanwendungsrolle für die Zielsystemverantwortlichen auf.
Zielsystemverantwortliche der Standardanwendungsrolle sind berechtigt alle Unix Hosts im One Identity Manager zu bearbeiten.
3. Zielsystemverantwortliche können innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche berechtigen und bei Bedarf weitere untergeordnete Anwendungsrollen erstellen und einzelnen Unix Hosts zuweisen.

Tabelle 17: Standardanwendungsrolle für Zielsystemverantwortliche

Benutzer	Aufgaben
Zielsystemverantwortliche	Die Zielsystemverantwortlichen müssen der Anwendungsrolle Zielsysteme Unix oder einer untergeordneten Anwendungsrolle zugewiesen sein. Benutzer mit dieser Anwendungsrolle: <ul style="list-style-type: none">• Übernehmen die administrativen Aufgaben für das Zielsystem.

Benutzer

Aufgaben

- Erzeugen, ändern oder löschen die Zielsystemobjekte, wie beispielsweise Benutzerkonten oder Gruppen.
- Bearbeiten Kennwortrichtlinien für das Zielsystem.
- Bereiten Gruppen zur Aufnahme in den IT Shop vor.
- Können Personen anlegen, die eine andere Identität haben als den Identitätstyp **Primäre Identität**.
- Konfigurieren im Synchronisation Editor die Synchronisation und definieren das Mapping für den Abgleich von Zielsystem und One Identity Manager.
- Bearbeiten Zielsystemtypen sowie die ausstehenden Objekte einer Synchronisation.
- Berechtigen innerhalb ihres Verantwortungsbereiches weitere Personen als Zielsystemverantwortliche und erstellen bei Bedarf weitere untergeordnete Anwendungsrollen.

Um initial Personen als Zielsystemadministrator festzulegen

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


Um initial Personen in die Standardanwendungsrolle für Zielsystemverantwortliche aufzunehmen

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

Um als Zielsystemverantwortlicher weitere Personen als Zielsystemverantwortliche zu berechtigen

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

Um Zielsystemverantwortliche für einzelne Hosts festzulegen

1. Melden Sie sich als Zielsystemverantwortlicher am Manager an.
2. Wählen Sie die Kategorie **Unix | Hosts**.
3. Wählen Sie in der Ergebnisliste den Host.
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 | Unix** zu.
 - b. Klicken Sie **Ok**, um die neue Anwendungsrolle zu übernehmen.
6. Speichern Sie die Änderungen.
7. Weisen Sie der Anwendungsrolle die Personen zu, die berechtigt sind, den Host im One Identity Manager zu bearbeiten.

Verwandte Themen

- [One Identity Manager Benutzer für die Verwaltung eines Unix-basierten Zielsystems](#) auf Seite 8
- [Allgemeine Stammdaten eines Unix Hosts](#) auf Seite 79

Bearbeiten eines Servers

Für die Verarbeitung der Unix spezifischen Prozesse im One Identity Manager müssen die Server mit ihren Serverfunktionen bekannt sein. Dazu gehört beispielsweise der Synchronisationsserver.

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

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

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

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

Um einen Jobserver und seine Funktionen zu bearbeiten

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

Detaillierte Informationen zum Thema

- [Stammdaten eines Jobservers](#) auf Seite 74
- [Serverfunktionen eines Jobservers](#) auf Seite 77

Stammdaten eines Jobservers

- HINWEIS:** Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** zur Verfügung.
- HINWEIS:** Abhängig von den installierten Modulen können weitere Eigenschaften verfügbar sein.

Tabelle 18: Eigenschaften eines Jobservers

Eigenschaft	Bedeutung
Server	Bezeichnung des Jobservers.
Vollständiger Servername	Vollständiger Servername gemäß DNS Syntax. Beispiel: <Name des Servers>.<Vollqualifizierter Domänenname>
Zielsystem	Zielsystem des Computerkontos.
Sprachkultur	Sprache des Servers.
Server ist Cluster	Angabe, ob der Server einen Cluster abbildet.

Eigenschaft	Bedeutung
Server gehört zu Cluster	Cluster, zu dem der Server gehört. HINWEIS: Die Eigenschaften Server ist Cluster und Server gehört zu Cluster schließen einander aus.
IP-Adresse (IPv6)	Internet Protokoll Version 6 (IPv6)-Adresse des Servers.
IP-Adresse (IPv4)	Internet Protokoll Version 4 (IPv4)-Adresse des Servers.
Kopierverfahren (Quellserver)	Zulässige Kopierverfahren, die genutzt werden können, wenn dieser Server Quelle einer Kopieraktion ist. Derzeit werden nur Kopierverfahren über die Programme Robocopy und rsync unterstützt. Wird kein Verfahren angegeben, ermittelt der One Identity Manager Service zur Laufzeit das Betriebssystem des Servers, auf dem die Kopieraktion ausgeführt wird. Die Replikation erfolgt dann zwischen Servern mit einem Windows Betriebssystem mit dem Programm Robocopy und zwischen Servern mit einem Linux Betriebssystem mit dem Programm rsync. Unterscheiden sich die Betriebssysteme des Quellserver 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.
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. Jeder One Identity Manager Service innerhalb des gesamten Netzwerkes muss eine eindeutige Queue-Bezeichnung erhalten. Mit exakt dieser Queue-Bezeichnung werden die Prozessschritte an der Jobqueue angefordert. Die Queue-Bezeichnung wird in die Konfigurationsdatei des One Identity Manager Service eingetragen.

Eigenschaft	Bedeutung
Serverbetriebssystem	Betriebssystem des Servers. Diese Angabe wird für die Pfadauslösung bei der Replikation von Softwareprofilen benötigt. Zulässig sind die Werte Win32 , Windows , Linux und Unix . Ist die Angabe leer, wird Win32 angenommen.
Angaben zum Dienstkonto	Benutzerkonteninformationen des One Identity Manager Service. Für die Replikation zwischen nicht vertrauenden Systemen (beispielsweise non-trusted Domänen, Linux-Server) müssen für die Server die Benutzerkonteninformationen des One Identity Manager Service in der Datenbank bekanntgegeben werden. Dazu sind das Dienstkonto, die Domäne des Dienstkontos und das Kennwort des Dienstkontos für die Server entsprechend einzutragen.
One Identity Manager Service installiert	Angabe, ob auf diesem Server ein One Identity Manager Service installiert und aktiv ist. Die Option wird durch die Prozedur QBM_PJobQueueLoad aktiviert, sobald die Queue das erste Mal angefragt wird. Die Option wird nicht automatisch entfernt. Für Server, deren Queue nicht mehr aktiv ist, können Sie diese Option im Bedarfsfall manuell zurücksetzen.
Stopp One Identity Manager Service	Angabe, ob der One Identity Manager Service gestoppt ist. Wenn diese Option für den Jobserver gesetzt ist, wird der One Identity Manager Service keine Aufträge mehr verarbeiten. Den Dienst können Sie mit entsprechenden administrativen Rechten im Programm Job Queue Info stoppen und starten. Ausführliche Informationen finden Sie im <i>One Identity Manager Handbuch zur Prozessüberwachung und Fehlersuche</i> .
Kein automatisches Softwareupdate	Angabe, ob der Server von der automatischen Softwareaktualisierung auszuschließen ist. HINWEIS: Server, für welche die Option aktiviert ist, müssen Sie manuell aktualisieren.
Softwareupdate läuft	Angabe, ob gerade eine Softwareaktualisierung ausgeführt wird.
Serverfunktion	Funktion des Servers in der One Identity Manager-Umgebung. Abhängig von der Serverfunktion wird die Verarbeitung der One Identity Manager-Prozesse ausgeführt.

Verwandte Themen

- [Serverfunktionen eines Jobservers](#) auf Seite 77

Serverfunktionen eines Jobserver

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

- HINWEIS:** Alle Bearbeitungsmöglichkeiten stehen Ihnen auch im Designer in der Kategorie **Basisdaten | Installationen | Jobserver** zur Verfügung.
- HINWEIS:** Abhängig von den installierten Modulen können weitere Serverfunktionen verfügbar sein.

Tabelle 19: Zulässige Serverfunktionen

Serverfunktion	Anmerkungen
CSV Konnektor	Server, auf dem der CSV Konnektor für die Synchronisation installiert ist.
Domänen-Controller	Active Directory Domänen-Controller. Server, die nicht als Domänen-Controller gekennzeichnet sind, werden als Memberserver betrachtet.
Druckserver	Server, der als Druckserver arbeitet.
Generischer Server	Server für die generische Synchronisation mit einem kundendefinierten Zielsystem.
Homeserver	Server zur Anlage von Homeverzeichnissen für Benutzerkonten.
Aktualisierungsserver	<p>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.</p> <p>Bei der initialen Schemainstallation wird der Server, auf dem die One Identity Manager-Datenbank installiert ist, mit dieser Serverfunktion gekennzeichnet.</p>
SQL Ausführungsserver	Der Server kann SQL Aufträge ausführen. Für eine Lastverteilung der SQL Prozesse können mehrere SQL Ausführungsserver eingerichtet werden. Das System verteilt die erzeugten SQL Prozesse über alle Jobserver mit dieser Serverfunktion.
CSV Skriptserver	Der Server kann CSV-Dateien per Prozesskomponente ScriptComponent verarbeiten.
Nativer Datenbankkonnektor	Der Server kann sich mit einer ADO.Net Datenbank verbinden.

Serverfunktion	Anmerkungen
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.
Profilservers	Server für die Einrichtung von Profilverzeichnissen für Benutzerkonten.
SAM Synchronisationsserver	Server für die Synchronisation mit einem SMB-basierten Zielsystem aus.
SMTP Host	Server, auf dem durch den One Identity Manager Service E-Mail Benachrichtigungen verschickt werden. Voraussetzung zum Versenden von Mails durch den One Identity Manager Service ist ein konfigurierter SMTP Host.
Standard Berichtserver	Server, auf dem die Berichte generiert werden.
Windows PowerShell Konnektor	Der Server kann Windows PowerShell Version 3.0 oder neuer ausführen.
Unix Konnektor	Der Server kann sich zu einem Unix System über SSH verbinden.
AIX Konnektor	Der Server kann sich zu einem AIX System über SSH verbinden.

Verwandte Themen

- [Stammdaten eines Jobservers](#) auf Seite 74

Unix Host

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

- HINWEIS:** Nach der initialen Synchronisation des Hosts sollten Sie die primäre Gruppe eintragen, die als Standard bei der Einrichtung der Benutzerkonten verwendet wird.

Um die Stammdaten eines Unix Hosts zu bearbeiten

1. Wählen Sie die Kategorie **Unix | Hosts**.
2. Wählen Sie in der Ergebnisliste den Host.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Bearbeiten Sie die Stammdaten für einen Host.
5. Speichern Sie die Änderungen.

Verwandte Themen



- [Allgemeine Stammdaten eines Unix Hosts](#) auf Seite 79

Allgemeine Stammdaten eines Unix Hosts

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

Tabelle 20: Allgemeine Stammdaten eines Hosts

Eigenschaft	Beschreibung
Hostname	Name des Hosts.
Primäre Gruppe	Primäre Gruppe für Benutzerkonten. Diese Gruppe wird als primäre Gruppe beim Erzeugen eines Benutzerkontos

Eigenschaft	Beschreibung
Gerät	<p>verwendet.</p> <p>Gerät, mit dem der Computer verbunden ist. Legen Sie über die Schaltfläche  neben der Auswahlliste ein neues Gerät an.</p>
AIX System	<p>Angabe, ob es sich beim Host um ein IBM AIX System handelt. Für Benutzerkonten auf IBM AIX Systemen werden zusätzliche Eigenschaften angeboten.</p>
Kontendefinition (initial)	<p>Initiale Kontendefinition zur Erzeugung von Benutzerkonten. Diese Kontendefinition wird verwendet, wenn für diesen Host die automatische Zuordnung von Personen zu Benutzerkonten genutzt wird und dabei bereits verwaltete Benutzerkonten (Zustand Linked configured) entstehen sollen. Es wird der Standardautomatisierungsgrad der Kontendefinition angewendet.</p> <p>Ist keine Kontendefinition angegeben, werden die Benutzerkonten nur mit der Person verbunden (Zustand Linked). Dies ist beispielsweise bei der initialen Synchronisation der Fall.</p>
Zielsystemverantwortliche	<p>Anwendungsrolle, in der die Zielsystemverantwortlichen des Hosts festgelegt sind. Die Zielsystemverantwortlichen bearbeiten nur die Objekte des Hosts, dem sie zugeordnet sind. Jedem Host können somit andere Zielsystemverantwortliche zugeordnet werden.</p> <p>Wählen Sie die One Identity Manager Anwendungsrolle aus, deren Mitglieder verantwortlich für die Administration dieses Hosts sind. Über die Schaltfläche  neben dem Eingabefeld können Sie eine neue Anwendungsrolle erstellen.</p>
Synchronisiert durch	<p>Art der Synchronisation, über welche die Daten zwischen dem Host und dem One Identity Manager synchronisiert werden. Sobald Objekte für diesen Host im One Identity Manager vorhanden sind, kann die Art der Synchronisation nicht mehr geändert werden.</p> <p>Beim Erstellen eines Hosts mit dem Synchronization Editor wird One Identity Manager verwendet.</p>


Eigenschaft	Beschreibung									
	Tabelle 21: Zulässige Werte									
	<table border="1"> <thead> <tr> <th>Wert</th> <th>Synchronisation durch</th> <th>Provisionierung durch</th> </tr> </thead> <tbody> <tr> <td>One Identity Manager</td> <td>Unix Konnektor</td> <td>Unix Konnektor</td> </tr> <tr> <td>Keine Synchronisation</td> <td>keine</td> <td>keine</td> </tr> </tbody> </table>	Wert	Synchronisation durch	Provisionierung durch	One Identity Manager	Unix Konnektor	Unix Konnektor	Keine Synchronisation	keine	keine
Wert	Synchronisation durch	Provisionierung durch								
One Identity Manager	Unix Konnektor	Unix Konnektor								
Keine Synchronisation	keine	keine								
	<p>HINWEIS: Wenn Sie Keine Synchronisation festlegen, definieren Sie unternehmensspezifische Prozesse, um Daten zwischen dem One Identity Manager und dem Zielsystem auszutauschen.</p>									
Betriebssystembeschreibung	Beschreibung des Betriebssystems.									
Distribution	Installierte Distribution des Betriebssystems.									
Distributionsversion	Version der installierten Distribution.									
Kernelversion	Aktuelle Kernelversion.									
Betriebssystemtyp	Typ des Betriebssystems, zum Beispiel Linux, AIX, UNIX.									

Festlegen der Kategorien für die Vererbung von Berechtigungen

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 31**.

Um Kategorien zu definieren

1. Wählen Sie im Manager in der Kategorie **Unix | Hosts** den Host.
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 Unix Gruppen anhand von Kategorien](#) auf Seite 124

Synchronisationsprojekt bearbeiten

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

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

Um ein bestehendes Synchronisationsprojekt im Synchronization Editor zu öffnen

1. Wählen Sie die Kategorie **Unix | Hosts**.
2. Wählen Sie in der Ergebnisliste den Host. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
3. Wählen Sie die Aufgabe **Synchronisationsprojekt bearbeiten....**

Verwandte Themen

- [Anpassen einer Synchronisationskonfiguration](#) auf Seite 25

Überblick über den Unix Host

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

Um einen Überblick über einen Host zu erhalten

1. Wählen Sie die Kategorie **Unix | Hosts**.
2. Wählen Sie in der Ergebnisliste den Host.
3. Wählen Sie die Aufgabe **Überblick über den Unix Host**.

Anzeigen der Unix Login-Shells

Die Informationen zu den Login-Shells eines Hosts werden in die One Identity Manager eingelesen und können nicht bearbeitet werden. Login-Shells können Sie bei der Einrichtung der Benutzerkonten verwenden.

Um Verwendung der Login-Shells anzuzeigen

1. Wählen Sie die Kategorie **Unix | Hosts | <Hostname> | Login-Shells**.
2. Wählen Sie in der Ergebnisliste die Login-Shell.
3. Wählen Sie die Aufgabe **Überblick über die Unix Login-Shell**.

Verwandte Themen

- [Erstellen einer Abbildungsvorschrift für IT Betriebsdaten](#) auf Seite 44
- [Allgemeine Stammdaten eines Unix Benutzerkontos](#) auf Seite 94

Unix Benutzerkonten

Mit dem One Identity Manager verwalten Sie die lokalen Benutzerkonten eines Unix-basierten Zielsystems. Über die Mitgliedschaft in Gruppen erhalten die Benutzerkonten die nötigen Rechte zum Zugriff auf die Ressourcen.

Detaillierte Informationen zum Thema

- [Benutzerkonten mit Personen verbinden](#) auf Seite 84
- [Unterstützte Typen von Benutzerkonten](#) auf Seite 85
- [Erfassen der Stammdaten für Unix Benutzerkonten](#) auf Seite 92
- [Automatische Zuordnung von Personen zu Unix Benutzerkonten](#) auf Seite 105

Benutzerkonten mit Personen verbinden

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

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

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

Wenn Sie Benutzerkonten über Kontendefinitionen verwalten, können Sie das Verhalten von Benutzerkonten beim Deaktivieren oder Löschen von Personen festlegen.

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

Verwandte Themen

- [Erfassen der Stammdaten für Unix Benutzerkonten](#) auf Seite 92
- [Einrichten von Kontendefinitionen](#) auf Seite 38
- [Automatische Zuordnung von Personen zu Unix Benutzerkonten](#) auf Seite 105
- Ausführliche Informationen zur Behandlung und Administration von Personen und Benutzerkonten finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Unterstützte Typen von Benutzerkonten

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

Zur Abbildung der verschiedenen Benutzerkontentypen werden die folgenden Eigenschaften verwendet.

- Identität

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

Tabelle 22: Identitäten von Benutzerkonten

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

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

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

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

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

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

- Privilegiertes Benutzerkonto

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

Detaillierte Informationen zum Thema

- [Standardbenutzerkonten](#) auf Seite 87
- [Administrative Benutzerkonten](#) auf Seite 88
- [Administrative Benutzerkonten für eine Person bereitstellen](#) auf Seite 89
- [Administrative Benutzerkonten für mehrere Personen bereitstellen](#) auf Seite 90
- [Privilegierte Benutzerkonten](#) auf Seite 91

Standardbenutzerkonten

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

Um Standardbenutzerkonten über Kontendefinitionen zu erstellen

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

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

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

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

- Verwenden Sie in der Abbildungsvorschrift für die Spalte IdentityType den Standardwert **Primary** und aktivieren Sie die Option **Immer Standardwert verwenden**.
4. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem. Wählen Sie unter **Wirksam für** das konkrete Zielsystem.
Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.
 5. Weisen Sie die Kontendefinition an die Personen zu.
Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

Verwandte Themen

- [Einrichten von Kontendefinitionen](#) auf Seite 38

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 Person bereitstellen](#) auf Seite 89
- [Administrative Benutzerkonten für mehrere Personen bereitstellen](#) auf Seite 90


Administrative Benutzerkonten für eine Person bereitstellen

Voraussetzungen

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

Um ein administratives Benutzerkonto für eine Person bereitzustellen

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

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

Verwandte Themen

- [Administrative Benutzerkonten für mehrere Personen bereitstellen](#) auf Seite 90
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Administrative Benutzerkonten für mehrere Personen bereitstellen


Voraussetzung

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

Um ein administratives Benutzerkonto für mehrere Personen bereitzustellen

1. Kennzeichnen Sie das Benutzerkonto als Gruppenidentität.
 - a. Wählen Sie im Manager die Kategorie **Unix | Benutzerkonten**.
 - b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
 - c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
 - d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Identität** den Wert **Gruppenidentität**.

2. Verbinden Sie das Benutzerkonto mit einer Dummy-Person.
 - a. Wählen Sie im Manager die Kategorie **Unix | Benutzerkonten**.
 - b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
 - c. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
 - d. Auf dem Tabreiter **Allgemein** wählen Sie in der Auswahlliste **Person** die Dummy-Person.

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

3. Weisen Sie dem Benutzerkonto die Personen zu, die dieses administrative Benutzerkonto nutzen sollen.
 - a. Wählen Sie im Manager die Kategorie **Unix | Benutzerkonten**.
 - b. Wählen Sie in der Ergebnisliste das Benutzerkonto.
 - c. Wählen Sie die Aufgabe **Personen mit Nutzungsberechtigungen zuzuweisen**.
 - d. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Personen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Person und doppelklicken Sie .

Verwandte Themen

- [Administrative Benutzerkonten für eine Person bereitstellen](#) auf Seite 89
- Ausführliche Informationen zur Abbildung von Identitäten von Personen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.

Privilegierte Benutzerkonten

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

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

Um privilegierte Benutzerkonten über Kontendefinitionen zu erstellen

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

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

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

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

- Zusätzlich können Sie eine Abbildungsvorschrift für die Spalte `IdentityType` festlegen. Die Spalte besitzt verschiedene zulässige Werte, die privilegierte Benutzerkonten repräsentieren.
 - Um zu verhindern, dass privilegierte Benutzerkonten die Berechtigungen des Standardbenutzers erben, definieren Sie eine Abbildungsvorschrift für die Spalte `IsGroupAccount` mit dem Standardwert **0** und aktivieren Sie die Option **Immer Standardwert verwenden**.
5. Erfassen Sie die wirksamen IT Betriebsdaten für das Zielsystem.
- Legen Sie an den Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen fest, welche IT Betriebsdaten bei der Einrichtung eines Benutzerkontos wirksam werden sollen.
6. Weisen Sie die Kontendefinition direkt an die Personen zu, die mit privilegierten Benutzerkonten arbeiten sollen.
- Durch die Zuweisung der Kontendefinition an eine Person wird über die integrierten Vererbungsmechanismen und anschließende Prozessverarbeitung ein neues Benutzerkonto erzeugt.

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

- Um ein Präfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | Unix | Accounts | PrivilegedAccount | AccountName_Prefix**.
- Um ein Postfix für den Anmeldenamen zu verwenden, aktivieren Sie im Designer den Konfigurationsparameter **TargetSystem | Unix | Accounts | PrivilegedAccount | AccountName_Postfix**.

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

Verwandte Themen


- [Einrichten von Kontendefinitionen](#) auf Seite 38

Erfassen der Stammdaten für Unix Benutzerkonten

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

- ① **HINWEIS:** Um Benutzerkonten für die Personen eines Unternehmens einzurichten, wird der Einsatz von Kontendefinitionen empfohlen. Einige der nachfolgend beschriebenen Stammdaten werden dabei über Bildungsregeln aus den Personenstammdaten gebildet.
- ① **HINWEIS:** Sollen Personen ihre Benutzerkonten über Kontendefinitionen erhalten, müssen die Personen ein zentrales Benutzerkonto besitzen und über die Zuordnung zu einer primären Abteilung, einem primären Standort oder einer primären Kostenstelle ihre IT Betriebsdaten erhalten.

Um ein Benutzerkonto zu erstellen

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

Um die Stammdaten eines Benutzerkontos zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Unix | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Bearbeiten Sie die Stammdaten des Benutzerkontos.
4. Speichern Sie die Änderungen.

Um ein Benutzerkonto für eine Person manuell zuzuweisen oder zu erstellen

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

Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten eines Unix Benutzerkontos](#) auf Seite 94
- [Stammdaten eines Benutzerkontos für AIX Systeme](#) auf Seite 97



Verwandte Themen

- [Einrichten von Kontendefinitionen](#) auf Seite 38
- [Unterstützte Typen von Benutzerkonten](#) auf Seite 85
- [Benutzerkonten mit Personen verbinden](#) auf Seite 84

Allgemeine Stammdaten eines Unix Benutzerkontos

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

Tabelle 23: Allgemeine Stammdaten eines Benutzerkontos

Eigenschaft	Beschreibung
Host	Host des Benutzerkontos.
Person	<p>Person, die das Benutzerkonto verwendet. Wurde das Benutzerkonto über eine Kontendefinition erzeugt, ist die Person bereits eingetragen. Wenn Sie das Benutzerkonto manuell erstellen, können Sie die Person aus der Auswahlliste wählen. Wenn Sie die automatische Personenzuordnung nutzen, wird beim Speichern des Benutzerkontos eine zugehörige Person gesucht und in das Benutzerkonto übernommen.</p> <p>Für ein Benutzerkonto mit einer Identität vom Typ Organisatorische Identität, Persönliche Administratoridentität, Zusatzidentität, Gruppenidentität oder Dienstidentität können Sie eine neue Person erstellen. Klicken Sie dafür  neben dem Eingabefeld und erfassen Sie die erforderlichen Personenstammdaten. Die Pflichteingaben sind abhängig vom gewählten Identitätstyp.</p>
Kontendefinition	<p>Kontendefinition, über die das Benutzerkonto erstellt wurde.</p> <p>Die Kontendefinition wird benutzt, um die Stammdaten des Benutzerkontos automatisch zu befüllen und um einen Automatisierungsgrad für das Benutzerkonto festzulegen. Der One Identity Manager ermittelt die IT Betriebsdaten der zugeordneten Person und trägt sie in die entsprechenden Eingabefelder des Benutzerkontos ein.</p> <p> HINWEIS: Die Kontendefinition darf nach dem Speichern des Benutzerkontos nicht geändert werden.</p>
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.
Login-Shell	Shell die ausgeführt wird, wenn ein Benutzer sich mittels Terminal-basierter Anmeldung am Unix anmeldet.
Benutzername	Name des Benutzerkontos zur Anmeldung an einem Unix Host. Haben Sie eine Kontendefinition zugeordnet, wird dieses

Eigenschaft	Beschreibung
	Eingabefeld abhängig vom Automatisierungsgrad automatisch mit dem zentralen Benutzerkonto der Person ausgefüllt.
Benutzer-ID	Benutzer-ID des Benutzerkontos im Unix Host.
Kennwort	<p>Kennwort für das Benutzerkonto. Das zentrale Kennwort der zugeordneten Person kann auf das Kennwort des Benutzerkontos abgebildet werden. Ausführliche Informationen zum zentralen Kennwort einer Person finden Sie im <i>One Identity Manager Administrationshandbuch für das Identity Management Basismodul</i>.</p> <p>Wenn Sie ein initiales Kennwort für Benutzerkonten verwenden, wird dieses automatisch bei Erstellen eines Benutzerkontos eingetragen.</p> <p>i 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.</p>
Kennwortbestätigung	Kennwortwiederholung.
Primäre Gruppe ID	ID der primären Gruppe des Benutzerkontos.
Primäre Gruppe	<p>Bezeichnung der primären Gruppe des Benutzerkontos. Diese Angabe bestimmt den Gruppenbesitz von Dateien, die vom Benutzer erstellt werden.</p> <p>Die primäre Gruppe eines Benutzerkontos wird folgendermaßen gebildet:</p> <ul style="list-style-type: none"> • Wenn am Host eine primäre Gruppe eingetragen ist, wird diese Gruppe als primäre Gruppe beim Erzeugen eines Benutzerkontos verwendet. • Wenn Sie am Host keine primäre Gruppe eintragen, wird beim Erzeugen eines neuen Benutzerkontos ein neue Gruppe mit dem Anzeigenamen des Benutzerkontos erzeugt und als primäre Gruppe zugewiesen.
Homeverzeichnis	Kompletter Pfad zum Homeverzeichnis des Benutzers, zum Beispiel /home/user001.
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 <i>One Identity Manager Administrationshandbuch für Risikobewertungen</i> .
Kategorie	Kategorien für die Vererbung von Gruppen an das Benutzerkonto.

Eigenschaft	Beschreibung
Kommentar (GECOS)	<p>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.</p> <p>Freitextfeld für zusätzliche Erläuterungen. Zusätzliche Informationen über das Benutzerkonto, die im GECOS in /etc/password gefunden werden. Haben Sie eine Kontendefinition zugeordnet, wird dieses Eingabefeld abhängig vom Automatisierungsgrad automatisch mit dem internen Namen der Person ausgefüllt.</p>
Identität	<p>Typ der Identität des Benutzerkontos. Zulässige Werte sind:</p> <ul style="list-style-type: none"> • Primäre Identität: Standardbenutzerkonto einer Person. • Organisatorische Identität: Sekundäres Benutzerkonto, welches für unterschiedliche Rollen in der Organisation verwendet wird, beispielsweise bei Teilverträgen mit anderen Unternehmensbereichen. • Persönliche Administratoridentität: Benutzerkonto mit administrativen Berechtigungen, welches von einer Person genutzt wird. • Zusatzidentität: Benutzerkonto, das beispielsweise zu Trainingszwecken genutzt wird. • Gruppenidentität: Benutzerkonto mit administrativen Berechtigungen, welches von mehreren Personen genutzt wird. Weisen Sie alle Personen zu, die das Benutzerkonto nutzen. • Dienstidentität: Dienstkonto.
Gruppen erbbbar	<p>Angabe, ob das Benutzerkonto Gruppen über die Person erben darf. Ist die Option aktiviert, werden Gruppen über hierarchische Rollen oder IT Shop Bestellungen an das Benutzerkonto vererbt.</p> <ul style="list-style-type: none"> • Wenn Sie eine Person mit Benutzerkonto beispielsweise in eine Abteilung aufnehmen und Sie dieser Abteilung Gruppen zugewiesen haben, dann erbt das Benutzerkonto diese Gruppen. • Wenn eine Person eine Gruppenmitgliedschaft im IT Shop bestellt hat und diese Bestellung genehmigt und zugewiesen ist, dann erbt das Benutzerkonto der Person diese Gruppe nur, wenn die Option aktiviert ist.
Privilegiertes Benutzerkonto	<p>Angabe, ob es sich um ein privilegiertes Benutzerkonto handelt.</p>

Verwandte Themen

- [Einrichten von Kontendefinitionen auf Seite 38](#)
- [Kennwortrichtlinien für Unix Benutzerkonten auf Seite 58](#)
- [Initiales Kennwort für neue Unix Benutzerkonten auf Seite 69](#)
- [Vererbung von Unix Gruppen anhand von Kategorien auf Seite 124](#)
- [Unterstützte Typen von Benutzerkonten auf Seite 85](#)
- [Allgemeine Stammdaten eines Unix Hosts auf Seite 79](#)
- [Deaktivieren von Benutzerkonten für AIX Systeme auf Seite 110](#)

Stammdaten eines Benutzerkontos für AIX Systeme

Für Benutzerkonten in einem IBM AIX System können Sie zusätzliche Stammdaten, wie Grenzwerte, Kennwortdaten, Sicherheitsinformationen oder Informationen zum verschlüsselnden Dateisystem erfassen. Diese Daten werden angezeigt, wenn der Host mit der Option **AIX System** gekennzeichnet ist.

Detaillierte Informationen zum Thema

- [Grenzwerte eines Benutzerkontos auf Seite 97](#)
- [Kennwortdaten eines Benutzerkontos auf Seite 99](#)
- [Sicherheitsrelevante Stammdaten eines Benutzerkontos auf Seite 100](#)
- [Stammdaten zum verschlüsselnden Dateisystem eines Benutzerkontos auf Seite 102](#)
- [Allgemeine Stammdaten eines Unix Hosts](#)

Grenzwerte eines Benutzerkontos

Auf dem Tabreiter **Grenzen** erfassen Sie folgende Grenzwerte für die Ressourcen der Prozesse eines Benutzers in einem AIX System. Diese Daten werden in `/etc/security/limits` abgebildet.

Tabelle 24: Grenzwerte für ein Benutzerkonto in einem AIX System

Eigenschaft	Beschreibung
Speicherabbild (weich)	Weiche Beschränkung für die größte Speicherabbilddatei, die ein Benutzerprozess erstellen kann. (Parameter <code>core</code>).
Speicherabbild (hart)	Absolute Obergrenze für die größte Speicherabbilddatei, die ein Benutzerprozess erstellen kann. (Parameter <code>core_hard</code>).

Eigenschaft	Beschreibung
CPU Zeit (weich)	Weiche Beschränkung für die Zeit (in Sekunden), die ein Benutzerprozess verwenden darf. (Parameter <code>cpu</code>).
CPU Zeit (hart)	Maximale Zeit (in Sekunden), die ein Benutzerprozess verwenden darf. (Parameter <code>cpu_hard</code>).
Datengröße (weich)	Weiche Beschränkung für größte Prozessdatensegment für einen Benutzerprozess. (Parameter <code>data</code>).
Datengröße (hart)	Größte Prozessdatensegment für einen Benutzerprozess. (Parameter <code>data_hard</code>).
Dateigröße (weich)	Weiche Beschränkung für die größte Datei, die ein Benutzerprozess erstellen oder erweitern darf. (Parameter <code>fsize</code>).
Dateigröße (hart)	Absolute Obergrenze für die größte Datei, die ein Benutzerprozess erstellen oder erweitern darf. (Parameter <code>fsize_hard</code>).
Speichergröße (weich)	Weiche Beschränkung für die maximale Menge an physischem Speicher, die ein Benutzerprozess belegen darf. (Parameter <code>rss</code>).
Speichergröße (hart)	Maximale Menge an physischem Speicher, die ein Benutzerprozess belegen darf. (Parameter <code>rss_hard</code>).
Stack-Größe (weich)	Weiche Beschränkung für das größte Prozess-Stack-Segment für einen Benutzerprozess. (Parameter <code>stack</code>).
Stack-Größe (hart)	Größte Prozess-Stack-Segment für einen Benutzerprozess. (Parameter <code>stack_hard</code>).
Datei-Deskriptor (weich)	Weiche Beschränkung für die Anzahl der Datei-Deskriptoren, die ein Benutzerprozess gleichzeitig geöffnet haben darf. (Parameter <code>nofiles</code>).
Datei-Deskriptor (hart)	Absolute Obergrenze für die Anzahl der Datei-Deskriptoren, die ein Benutzerprozess gleichzeitig geöffnet haben darf. (Parameter <code>nofiles_hard</code>).
Threads (weich)	Weiche Beschränkung für die Anzahl der Threads eines Prozesses. (Parameter <code>threads</code>).
Threads (hart)	Absolute Obergrenze für die Anzahl der Threads eines Prozesses. (Parameter <code>threads_hard</code>).
Prozesse (weich)	Weiche Beschränkung für die Anzahl der Prozess pro Benutzer. (Parameter <code>nproc</code>).
Prozesse (hart)	Absolute Obergrenze für die Anzahl der Prozess pro Benutzer. (Parameter <code>nproc_hard</code>).

Kennwortdaten eines Benutzerkontos

Auf dem Tabreiter **Kennwort** erfassen Sie folgende zusätzliche Informationen für ein Benutzerkonto in einem AIX System. Diese Daten werden in `/etc/security/user` abgebildet.

Tabelle 25: Kennwortdaten für ein Benutzerkonto in einem AIX System

Eigenschaft	Beschreibung
<code>minlen</code>	Minimale Anzahl von Zeichen die ein Kennwort haben muss. (Parameter <code>minlen</code>).
<code>maxrepeats</code>	Maximale Anzahl, die ein Zeichen in einem neuen Kennwort wiederholt werden darf. Der Standardwert 8 gibt an, dass keine maximale Anzahl festgelegt ist. (Parameter <code>maxrepeats</code>).
<code>mindiff</code>	Definiert, wie viele Zeichen sich zwischen neuem und altem Kennwort unterscheiden müssen. (Parameter <code>mindiff</code>).
<code>minalpha</code>	Definiert, wie viele alphabetische Zeichen ein neues Kennwort mindestens enthalten muss. (Parameter <code>minalpha</code>).
<code>minloweralpha</code>	Angabe, wie viele Kleinbuchstaben ein neues Kennwort mindestens enthalten muss. (Parameter <code>minloweralpha</code>).
<code>minupperalpha</code>	Angabe, wie viele Großbuchstaben ein neues Kennwort mindestens enthalten muss. (Parameter <code>minupperalpha</code>).
<code>mindigit</code>	Angabe, wie viele Ziffern ein neues Kennwort mindestens enthalten muss. (Parameter <code>mindigit</code>).
<code>minspecialchar</code>	Angabe, wie viele Sonderzeichen ein neues Kennwort mindestens enthalten muss. (Parameter <code>minspecialchar</code>).
<code>minother</code>	Definiert, wie viele nicht-alphabetische Zeichen ein neues Kennwort mindestens enthalten muss. (Parameter <code>minother</code>).
<code>dictionlist</code>	Wörterbuchdateien, die nicht erlaubte Kennwörter enthalten. (Parameter <code>dictionlist</code>).
<code>histexpire</code>	Länge der Kennworthistorie in Wochen. (Parameter <code>histexpire</code>).
<code>histsize</code>	Anzahl der eindeutigen neuen Kennwörter, bevor ein altes Kennwort erneut verwendet werden kann. (Parameter <code>histsize</code>).
<code>minage</code>	Anzahl der Wochen, die ein Kennwort benutzt werden muss, bevor der Benutzer das Kennwort ändern darf. (Parameter <code>minage</code>).
<code>maxage</code>	Anzahl der Wochen, die ein Kennwort verwendet werden kann, bevor ein neues Kennwort erwartet wird. (Parameter <code>maxage</code>).
<code>maxexpired</code>	Maximaler Zeitraum (in Wochen) nach dem Ablauf des maximalen Kennwortalters, in der ein Benutzer ein abgelaufenes Kennwort ändern kann. (Parameter <code>maxexpired</code>).

Eigenschaft	Beschreibung
pwdchecks	Methoden zur Kennwortbeschränkung, die auf neue Kennwörter angewendet werden. Der Wert enthält eine kommagetrennte Liste von Methodennamen. (Parameter pwdchecks).
pwdwarntime	Anzahl der Tage, bevor das System eine Warnung erzeugt, dass eine Kennwortänderung erforderlich ist. (Parameter pwdwarntime).

Sicherheitsrelevante Stammdaten eines Benutzerkontos

Auf dem Tabreiter **Sicherheit** erfassen Sie folgende zusätzliche Informationen für ein Benutzerkonto in einem AIX System. Diese Daten werden in `/etc/security/user` abgebildet.

Tabelle 26: Zusätzliche sicherheitsrelevante Informationen für ein Benutzerkonto in einem AIX System

Eigenschaft	Beschreibung
account_locked	Angabe, ob das Benutzerkonto gesperrt ist. (Parameter account_locked).
admin	Angabe, ob es sich um ein administratives Benutzerkonto handelt. (Parameter admin).
admgroups	Gruppen, die ein Benutzer verwaltet. (Parameter admgroups).
auditclasses	Audit-Klassen des Benutzerkontos. (Parameter auditclasses).
auth1	Zusätzlich benötigte Methoden für die Authentifizierung des Benutzers. (Parameter auth1).
auth2	Zusätzliche optionale Methoden für die Authentifizierung des Benutzers. (Parameter auth2).
core_compress	Angabe, ob die Komprimierung der Speicherabbilddatei aktiviert ist. (Parameter core_compress).
core_path	Angabe, ob die Spezifikation des Pfades der Speicherabbilddatei aktiviert ist. (Parameter core_path). Ist die Option aktiviert, wird die Speicherabbilddatei im angegebenen Verzeichnis abgelegt. Anderenfalls wird die Datei im Arbeitsverzeichnis des Benutzers abgelegt.
core_naming	Namenskonventionen für die Speicherabbilddatei. Wenn die Option aktiviert ist, wird die Speicherabbilddatei mit einer Prozess ID, einer Zeit und einem Datumstempel versehen. (Parameter core_naming).
daemon	Angabe, ob ein Benutzer ein Programm unter Verwendung des Cron-Daemon oder des src (system resource controller) Daemon ausführen kann. (Parameter daemon).

Eigenschaft	Beschreibung
dce_export	Angabe, ob die DCE Registrierung die lokalen Benutzerinformationen mit den DCE Benutzerinformationen während einer DCE Exportoperation überschreiben darf. (Parameter dce_export).
expires	Ablaufdatum des Benutzerkontos. (Parameter expires).
login	Angabe, ob sich ein Benutzer mit dem login Kommando am System anmelden kann. (Parameter login).
logintimes	Zeiten, Tage oder beides, zu denen dem Benutzer der Zugriff auf das System erlaubt ist. (Parameter logintimes).
loginretries	Anzahl der ungültigen Anmeldeversuche, die nach der letzten gültigen Anmeldung erlaubt sind, bevor das System den Benutzer sperrt. (Parameter loginretries). Null oder ein negativer Wert legen fest, dass keine Beschränkung vorhanden ist.
projects	Liste von Projekten, denen ein Benutzerprozess zugewiesen sein kann. Der Wert enthält eine kommagetrennte Liste von Projektnamen. (Parameter projects).
registry	Definiert die Authentifizierungsregistrierung, in der der Benutzer administriert wird. (Parameter registry).
rlogin	Angabe, ob der Zugriff von einem Remote-Standort mit dem telnet oder rlogin Kommando erlaubt ist. (Parameter rlogin).
su	Angabe, ob ein Benutzer mit dem su Kommando auf einen anderen Benutzer wechseln kann. (Parameter su).
sugroups	Gruppen, die das su Kommando zum Wechseln auf definierte Benutzer verwenden können. (Parameter sugroups).
SYSTEM	Authentifizierungsmechanismus des Systems für den Benutzer. (Parameter SYSTEM).
tpath	Status des vertrauenswürdigen Pfades eines Benutzers. (Parameter tpath).
ttys	Enthält die Terminals, auf die ein Benutzer Zugriff hat. (Parameter ttys).
umask	Bestimmt die Dateiberechtigungen. (Parameter umask). Der Standardwert ist 022.

Verwandte Themen

- [Deaktivieren von Benutzerkonten für AIX Systeme](#) auf Seite 110

Stammdaten zum verschlüsselnden Dateisystem eines Benutzerkontos

Auf dem Tabreiter **Verschlüsselndes Dateisystem** erfassen Sie folgende zusätzliche Informationen zur Nutzung des verschlüsselnden Dateisystems (EFS) für ein Benutzerkonto in einem AIX System. Diese Daten werden in `/etc/security/user` abgebildet.

Tabelle 27: Stammdaten eines Benutzerkontos für das verschlüsselnde Dateisystem

Eigenschaft	Beschreibung
<code>efs_adminks_access</code>	Ablageort des Schlüsselspeichers für den <code>efs_admin</code> (Parameter <code>efs_adminks_access</code>). Zulässige Werte: <ul style="list-style-type: none">fileldap
<code>efs_allowksmodechangebyuser</code>	Angabe, ob ein Benutzer den Modus ändern darf. (Parameter <code>efs_allowksmodechangebyuser</code>).
<code>efs_file_algo</code>	Algorithmus der zur Generierung des Dateischutzschlüssels verwendet wird. (Parameter <code>efs_file_algo</code>). Zulässige Werte: <ul style="list-style-type: none">AES_128_CBCAES_192_CBCAES_256_CBC
<code>efs_initialks_mode</code>	Initialer Modus des Schlüsselspeichers des Benutzers. (Parameter <code>efs_initialks_mode</code>). Zulässige Werte: <ul style="list-style-type: none">guardadmin
<code>efs_keystore_access</code>	Ablageort des benutzerspezifischen Schlüsselspeichers. (Parameter <code>efs_keystore_access</code>). Zulässige Werte: <ul style="list-style-type: none">nonefile
<code>efs_keystore_algo</code>	Algorithmus der zur Generierung des privaten Schlüssels der Benutzer verwendet wird, wenn der Schlüsselspeicher erstellt wird. (Parameter <code>efs_keystore_algo</code>). Zulässige Werte: <ul style="list-style-type: none">RSA_1024RSA_2048RSA_4096

Zusätzliche Aufgaben für die Verwaltung von Unix Benutzerkonten

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

Überblick über das Unix Benutzerkonto

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

Um einen Überblick über ein Benutzerkonto zu erhalten

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

Ändern des Automatisierungsgrades an einem Unix Benutzerkonto

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

Um den Automatisierungsgrad für ein Benutzerkonto zu ändern

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

Verwandte Themen

- [Erfassen der Stammdaten für Unix Benutzerkonten](#) auf Seite 92

Unix Gruppen direkt an ein Unix Benutzerkonto zuweisen

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

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

Um Gruppen direkt an ein Benutzerkonto zuzuweisen

1. Wählen Sie im Manager die Kategorie **Unix | 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

- [Unix Gruppe an Unix Benutzerkonten zuweisen](#) auf Seite 115

Zusatzeigenschaften an ein Unix Benutzerkonto zuweisen

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

Um Zusatzeigenschaften für ein Benutzerkonto festzulegen

1. Wählen Sie im Manager die Kategorie **Unix | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Zusatzeigenschaften zuweisen**.

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

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Zusatzeigenschaft und doppelklicken Sie .

5. Speichern Sie die Änderungen.

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

Automatische Zuordnung von Personen zu Unix Benutzerkonten

Tabelle 28: Konfigurationsparameter für die automatische Personenzuordnung

Konfigurationsparameter	Bedeutung
TargetSystem\Unix\PersonAutoFullsync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem\Unix\PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\Unix\PersonExcludeList	Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe () getrennten Liste, die als reguläres Suchmuster verarbeitet wird. Beispiel: ROOT
TargetSystem\Unix\PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.

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

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

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

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

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

Beispiel:

ROOT

- Legen Sie über den Konfigurationsparameter "TargetSystem\Unix\PersonAutoDisabledAccounts" fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
- Weisen Sie dem Host eine Kontendefinition zu. Stellen Sie sicher, dass der Automatisierungsgrad, der verwendet werden soll, als Standardautomatisierungsgrad eingetragen ist.
- Definieren Sie die Suchkriterien für die Personenzuordnung im Host.

HINWEIS:

Für die Synchronisation gilt:

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

Außerhalb der Synchronisation gilt:

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

HINWEIS:

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

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

Um die Benutzerkonten über Kontendefinitionen zu verwalten

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

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

Verwandte Themen

- [Erstellen einer Kontendefinition](#) auf Seite 38
- [Zuweisen der Kontendefinition an ein Zielsystem](#) auf Seite 55
- [Bearbeiten der Suchkriterien für die automatische Personenzuordnung](#) auf Seite 107

Bearbeiten der Suchkriterien für die automatische Personenzuordnung

Die Kriterien für die Personenzuordnung werden am Host definiert. Dabei legen Sie fest, welche Eigenschaften eines Benutzerkontos mit welchen Eigenschaften einer Person

übereinstimmen müssen, damit die Person dem Benutzerkonto zugeordnet werden kann. Die Suchkriterien können Sie durch Formatdefinitionen weiter einschränken. Das zusammengestellte Suchkriterium wird in XML-Notation in die Spalte **Suchkriterien für die automatische Personenzuordnung** (AccountToPersonMatchingRule) der Tabelle UNXHost geschrieben.

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

- HINWEIS:** Bei der Zuordnung der Personen zu Benutzerkonten anhand der Suchkriterien erhalten die Benutzerkonten den Standardautomatisierungsgrad der Kontendefinition, die am Zielsystem des Benutzerkontos eingetragen ist. Abhängig davon, wie das Verhalten des verwendeten Automatisierungsgrades definiert ist, können Eigenschaften der Benutzerkonten angepasst werden.

Für administrative Benutzerkonten wird empfohlen, die Zuordnung nicht anhand der Suchkriterien vorzunehmen. Ordnen Sie Personen zu administrativen Benutzerkonten über die Aufgabe **Stammdaten bearbeiten** am jeweiligen Benutzerkonto zu.
- HINWEIS:** Der One Identity Manager liefert ein Standardmapping für die Personenzuordnung. Führen Sie die folgenden Schritte nur aus, wenn Sie das Standardmapping unternehmensspezifisch anpassen möchten.

Um Kriterien für die Personenzuordnung festzulegen

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

Tabelle 29: Standardsuchkriterien für Benutzerkonten und Kontakte

Anwenden auf	Spalte an Person	Spalte am Benutzerkonto
Unix Benutzerkonten	Zentrales Benutzerkonto (CentralAccount)	Benutzername (AccountName)

5. Speichern Sie die Änderungen.

Direkte Zuordnung von Personen an Benutzerkonten anhand einer Vorschlagsliste

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

Tabelle 30: Ansichten zur manuellen Zuordnung

Ansicht	Beschreibung
Vorgeschlagene Zuordnungen	Die Ansicht listet alle Benutzerkonten auf, denen der One Identity Manager eine Person zuordnen kann. Dazu werden die Personen angezeigt, die durch die Suchkriterien ermittelt und zugeordnet werden können.
Zugeordnete Benutzerkonten	Die Ansicht listet alle Benutzerkonten auf, denen eine Person zugeordnet ist.
Ohne Personenzuordnung	Die Ansicht listet alle Benutzerkonten auf, denen keine Person zugeordnet ist und für die über die Suchkriterien keine passende Person ermittelt werden kann.

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

Um die Suchkriterien auf die Benutzerkonten anzuwenden

- Klicken Sie **Neu laden**.

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

Um Personen direkt über die Vorschlagsliste zuzuordnen

1. Klicken Sie **Vorgeschlagene Zuordnungen**.

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

Den ausgewählten Benutzerkonten werden die per Suchkriterium ermittelten Personen zugeordnet.

– ODER –

2. Klicken Sie **Ohne Personenzuordnung**.

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

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

Um Zuordnungen zu entfernen

1. Klicken Sie **Zugeordnete Benutzerkonten**.
 - a. Klicken Sie **Auswahl** für alle Benutzerkonten, deren Personenzuordnung entfernt werden soll. Mehrfachauswahl ist möglich.
 - b. Klicken Sie **Ausgewählte entfernen**.
 - c. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Von den ausgewählten Benutzerkonten werden die zugeordneten Personen entfernt.

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

Verwandte Themen

- [Automatische Zuordnung von Personen zu Unix Benutzerkonten](#) auf Seite 105

Deaktivieren von Benutzerkonten für AIX Systeme

HINWEIS: Das nachfolgend beschriebene Verhalten gilt nur für Benutzerkonten in einem AIX System.

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

Szenario:

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

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

Szenario:

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

Benutzerkonten, die mit Personen verbunden sind, jedoch nicht über Kontendefinitionen verwaltet werden, werden deaktiviert, wenn die Person dauerhaft oder zeitweilig

deaktiviert wird. Das Verhalten ist abhängig vom Konfigurationsparameter **QER | Person | TemporaryDeactivation**.

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

Um das Benutzerkonto bei deaktiviertem Konfigurationsparameter zu deaktivieren

1. Wählen Sie im Manager die Kategorie **Unix | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Sicherheit** die Option **account_locked**.
5. Speichern Sie die Änderungen.

Szenario:

- Benutzerkonten sind nicht mit Personen verbunden.

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

1. Wählen Sie im Manager die Kategorie **Unix | Benutzerkonten**.
2. Wählen Sie in der Ergebnisliste das Benutzerkonto.
3. Wählen Sie die Aufgabe **Stammdaten bearbeiten**.
4. Aktivieren Sie auf dem Tabreiter **Sicherheit** die Option **account_locked**.
5. Speichern Sie die Änderungen.

Verwandte Themen

- [Einrichten von Kontendefinitionen](#) auf Seite 38
- [Erstellen der Automatisierungsgrade](#) auf Seite 41
- [Löschen und Wiederherstellen von Unix Benutzerkonten](#) auf Seite 112
- Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Löschen und Wiederherstellen von Unix Benutzerkonten

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

Um ein Benutzerkonto zu löschen

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

Um ein Benutzerkonto wiederherzustellen

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

Konfigurieren der Löschverzögerung

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

Verwandte Themen

- [Deaktivieren von Benutzerkonten für AIX Systeme](#) auf Seite 110
- Ausführliche Informationen zum Deaktivieren und Löschen von Personen und Benutzerkonten finden Sie im One Identity Manager Administrationshandbuch für das Zielsystem-Basismodul.

Unix Gruppen

Im Unix Host können Benutzerkonten in Gruppen zusammengefasst werden, mit denen der Zugriff auf Ressourcen geregelt werden kann. Lokale Gruppen werden durch die Synchronisation in den One Identity Manager eingelesen. Sie 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 oder den IT Shop zuweisen.

Detaillierte Informationen zum Thema

- [Erfassen der Stammdaten für Unix Gruppen](#) auf Seite 113
- [Unix Gruppe an Unix Benutzerkonten zuweisen](#) auf Seite 115

Erfassen der Stammdaten für Unix Gruppen

Um die Stammdaten einer Gruppe zu bearbeiten

1. Wählen Sie im Manager die Kategorie **Unix | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe und führen Sie die Aufgabe **Stammdaten bearbeiten** aus.
3. Auf dem Stammdatenformular bearbeiten Sie die Stammdaten der Gruppe.
4. Speichern Sie die Änderungen.

Detaillierte Informationen zum Thema

- [Allgemeine Stammdaten einer Unix Gruppe](#) auf Seite 114

Allgemeine Stammdaten einer Unix Gruppe

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

Tabelle 31: Allgemeine Stammdaten

Eigenschaft	Beschreibung
Name der Gruppe	Bezeichnung der Gruppe.
Gruppen-ID	ID der Gruppe.
Host	Host der Gruppe.
IT Shop	Angabe, ob die Gruppe über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Die Gruppe kann weiterhin direkt an Benutzerkonten und hierarchische Rollen zugewiesen werden.
Verwendung nur im IT Shop	Angabe, ob die Gruppe ausschließlich über den IT Shop bestellbar ist. Ist die Option aktiviert, kann die Gruppe über das Web Portal von Ihren Mitarbeitern bestellt und über definierte Genehmigungsverfahren zugeteilt werden. Eine direkte Zuweisung der Gruppe an hierarchische Rollen oder Benutzerkonten ist nicht zulässig.
Leistungsposition	Angabe einer Leistungsposition, um die Gruppe über den IT Shop zu bestellen.
Risikoindex	Wert zur Bewertung des Risikos von Zuweisungen der Gruppe an Benutzerkonten. Stellen Sie einen Wert zwischen 0 und 1 ein. Das Eingabefeld ist nur sichtbar, wenn der Konfigurationsparameter QER CalculateRiskIndex aktiviert ist. Ausführliche Informationen zur Risikobewertung finden Sie im One Identity Manager Administrationshandbuch für Risikobewertungen.
Kategorie	Kategorien für die Vererbung von Gruppen. Gruppen können selektiv an Benutzerkonten vererbt werden. Dazu werden die Gruppen und die Benutzerkonten in Kategorien eingeteilt. Wählen Sie aus der Auswahlliste eine oder mehrere Kategorien.

Verwandte Themen

- [Vererbung von Unix Gruppen anhand von Kategorien](#) auf Seite 124
- Ausführliche Informationen zur Vorbereitung der Gruppen für die Bestellung über den IT Shop finden Sie im One Identity Manager Administrationshandbuch für IT Shop.

Unix Gruppe an Unix Benutzerkonten zuweisen

Gruppen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Bei der indirekten Zuweisung werden Personen und Gruppen in hierarchische Rollen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen eingeordnet. Aus der Position innerhalb der Hierarchie und der Vererbungsrichtung werden die Gruppen berechnet, die einer Person zugewiesen sind.

Wenn Sie eine Person in Rollen aufnehmen und die Person ein Benutzerkonto besitzt, dann wird dieses Benutzerkonto in die Gruppen aufgenommen. Voraussetzungen für die indirekte Zuweisung an die Benutzerkonten von Personen sind

- Für die Rollenklassen (Abteilung, Kostenstelle, Standort oder Geschäftsrollen) ist die Zuweisung von Personen und Gruppen erlaubt.
- Die Benutzerkonten sind mit der Option **Gruppen erbbar** gekennzeichnet.

Des Weiteren können Gruppen über IT Shop-Bestellungen an Personen zugewiesen werden. Damit Gruppen über IT Shop-Bestellungen zugewiesen werden können, werden Personen als Kunden in einen Shop aufgenommen. Alle Gruppen, die als Produkte diesem Shop zugewiesen sind, können von den Kunden bestellt werden. Bestellte Gruppen werden nach erfolgreicher Genehmigung den Personen zugewiesen.

Detaillierte Informationen zum Thema

- [Unix Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 115
- [Unix Gruppe an Geschäftsrollen zuweisen](#) auf Seite 116
- [Unix Benutzerkonten direkt an eine Unix Gruppe zuweisen](#) auf Seite 118
- [Unix Gruppe in Systemrollen aufnehmen](#) auf Seite 118
- [Unix Gruppe in den IT Shop aufnehmen](#) auf Seite 119

Unix Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen

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

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

1. Wählen Sie im Manager die Kategorie **Unix | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Organisationen zuweisen**.

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

- Weisen Sie auf dem Tabreiter **Abteilungen** die Abteilungen zu.
- Weisen Sie auf dem Tabreiter **Standorte** die Standorte zu.
- Weisen Sie auf dem Tabreiter **Kostenstellen** die Kostenstellen zu.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Organisation und doppelklicken Sie .

5. Speichern Sie die Änderungen.

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

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

- ODER -

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

- ODER -

Wählen Sie im Manager die Kategorie **Organisationen | Standorte**.

2. Wählen Sie in der Ergebnisliste die Abteilung, die Kostenstelle oder den Standort.

3. Wählen Sie die Aufgabe **Unix 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


- [Unix Gruppe an Geschäftsrollen zuweisen](#) auf Seite 116
- [Unix Benutzerkonten direkt an eine Unix Gruppe zuweisen](#) auf Seite 118
- [Unix Gruppe in Systemrollen aufnehmen](#) auf Seite 118
- [Unix Gruppe in den IT Shop aufnehmen](#) auf Seite 119

Unix Gruppe an Geschäftsrollen zuweisen


Installierte Module: Geschäftsrollenmodul

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

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

1. Wählen Sie im Manager die Kategorie **Unix | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **Geschäftsrollen zuweisen**.
4. Weisen Sie im Bereich **Zuordnungen hinzufügen** die Geschäftsrollen zu.
 - 1 **TIPP:** Im Bereich **Zuordnungen entfernen** können Sie die Zuweisung von Geschäftsrollen entfernen.
Um eine Zuweisung zu entfernen
 - Wählen Sie die Geschäftsrolle und doppelklicken Sie .
5. Speichern Sie die Änderungen.

Um Gruppen an eine Geschäftsrolle zuzuweisen (bei rollenbasierter Anmeldung)

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

- [Unix Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 115
- [Unix Benutzerkonten direkt an eine Unix Gruppe zuweisen](#) auf Seite 118
- [Unix Gruppe in Systemrollen aufnehmen](#) auf Seite 118
- [Unix Gruppe in den IT Shop aufnehmen](#) auf Seite 119

Unix Benutzerkonten direkt an eine Unix Gruppe zuweisen

Gruppen können direkt oder indirekt an Benutzerkonten zugewiesen werden. Die indirekte Zuweisung erfolgt über die Einordnung der Person und der Gruppen in Unternehmensstrukturen, wie Abteilungen, Kostenstellen, Standorten oder Geschäftsrollen. Besitzt die Person ein Benutzerkonto in einem Unix-basierten Zielsystem, werden die Gruppen der Rollen an dieses Benutzerkonto vererbt.


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

Um eine Gruppe direkt an Benutzerkonten zuzuweisen

1. Wählen Sie im Manager die Kategorie **Unix | 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

- [Unix Gruppen direkt an ein Unix Benutzerkonto zuweisen](#) auf Seite 104
- [Unix Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 115
- [Unix Gruppe an Geschäftsrollen zuweisen](#) auf Seite 116
- [Unix Gruppe in Systemrollen aufnehmen](#) auf Seite 118
- [Unix Gruppe in den IT Shop aufnehmen](#) auf Seite 119

Unix Gruppe in Systemrollen aufnehmen

Installierte Module: Systemrollenmodul

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


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

Um eine Gruppe an Systemrollen zuzuweisen

1. Wählen Sie im Manager die Kategorie **Unix | 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

- [Unix Gruppe an Abteilungen, Kostenstellen und Standorte zuweisen](#) auf Seite 115
- [Unix Gruppe an Geschäftsrollen zuweisen](#) auf Seite 116
- [Unix Benutzerkonten direkt an eine Unix Gruppe zuweisen](#) auf Seite 118
- [Unix Gruppe in den IT Shop aufnehmen](#) auf Seite 119

Unix Gruppe in den IT Shop aufnehmen

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

- Die Gruppe muss mit der Option **IT Shop** gekennzeichnet sein.
 - Der Gruppe muss eine Leistungsposition zugeordnet sein.
 - Soll die Gruppe nur über IT Shop-Bestellungen an Personen zugewiesen werden können, muss die Gruppe zusätzlich mit der Option **Verwendung nur im IT Shop** gekennzeichnet sein. Eine direkte Zuweisung an hierarchische Rollen ist dann nicht mehr zulässig.
- HINWEIS:** Bei rollenbasierter Anmeldung können die IT Shop Administratoren Gruppen an IT Shop Regale zuweisen. Zielsystemadministratoren sind nicht berechtigt Gruppen in den IT Shop aufzunehmen.

Um eine Gruppe in den IT Shop aufzunehmen

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

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

Verwandte Themen

- [Allgemeine Stammdaten einer Unix Gruppe](#) auf Seite 114
- [Unix Gruppe aus einem IT Shop Regal entfernen](#) auf Seite 120
- [Unix Gruppe aus allen IT Shop Regalen entfernen](#) auf Seite 120

Unix Gruppe aus einem IT Shop Regal entfernen

Um eine Gruppe aus einzelnen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Unix | Gruppen** (bei nicht-rollebasierter Anmeldung).
- ODER -
Wählen Sie die Kategorie **Berechtigungen | Unix Gruppen** (bei rollebasierter Anmeldung).
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Wählen Sie die Aufgabe **In IT Shop aufnehmen**.
4. Entfernen Sie im Bereich **Zuordnungen entfernen** die Gruppe aus den IT Shop Regalen.
5. Speichern Sie die Änderungen.

Unix Gruppe aus allen IT Shop Regalen entfernen

Um eine Gruppe aus allen Regalen des IT Shops zu entfernen

1. Wählen Sie die Kategorie **Unix | Gruppen** (bei nicht-rollebasierter Anmeldung).
- ODER -

Wählen Sie die Kategorie **Berechtigungen | Unix 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.

Zusätzliche Aufgaben für die Verwaltung von Unix Gruppen

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

Überblick über die Unix Gruppe

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

Um einen Überblick über eine Gruppe zu erhalten

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

Unix Gruppe in Unix Gruppen aufnehmen

Mit dieser Aufgabe nehmen Sie eine Gruppe in andere Gruppen auf.

Um Gruppen direkt an eine Gruppe zuzuweisen

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

ausgewählten Gruppe untergeordnet sind.

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

Um eine Zuweisung zu entfernen

- Wählen Sie die Gruppe und doppelklicken Sie .

5. Speichern Sie die Änderungen.

Wirksamkeit von Gruppenmitgliedschaften

Tabelle 32: Konfigurationsparameter für die bedingte Vererbung

Konfigurationsparameter	Wirkung bei Aktivierung
QER Structures Inherite GroupExclusion	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Wirksamkeit von Gruppenmitgliedschaften. Ist der Parameter aktiviert, können aufgrund von Ausschlussdefinitionen die Gruppenmitgliedschaften reduziert werden. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.

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

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

HINWEIS:

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

Die Wirksamkeit der Zuweisungen wird in den Tabellen UNXAccountInUNXGroup und BaseTreeHasUNXGroup über die Spalte XIsInEffect abgebildet.

Beispiel für die Wirksamkeit von Gruppenmitgliedschaften

- In einem Host 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 diesem Host. Sie gehört primär der Abteilung "Marketing" an. Sekundär sind ihr die Geschäftsrolle "Kontrollgruppe" und die Abteilung "Finanzen" zugewiesen. Ohne Ausschlussdefinition erhält das Benutzerkonto alle Berechtigungen der Gruppen A, B und C.

Durch geeignete Maßnahmen soll verhindert werden, dass eine Person sowohl Bestellungen auslösen als auch Rechnungen zur Zahlung anweisen kann. Das heißt, die Gruppen A und B schließen sich aus. Eine Person, die Rechnungen prüft, darf ebenfalls keine Rechnungen zur Zahlung anweisen. Das heißt, die Gruppen B und C schließen sich aus.

Tabelle 33: Festlegen der ausgeschlossenen Gruppen (Tabelle UNXGroupExclusion)

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

Tabelle 34: Wirksame Zuweisungen

Person	Mitglied in Rolle	Wirksame Gruppe
Ben King	Marketing	Gruppe A
Jan Bloggs	Marketing, Finanzen	Gruppe B
Clara Harris	Marketing, Finanzen, Kontrollgruppe	Gruppe C
Jenny Basset	Marketing, Kontrollgruppe	Gruppe A, Gruppe C

Für Clara Harris ist nur die Zuweisung der Gruppe C wirksam und wird ins Zielsystem publiziert. Verlässt Clara Harris die Geschäftsrolle "Kontrollgruppe" zu einem späteren Zeitpunkt, wird die Gruppe B ebenfalls wirksam.

Für Jenny Basset sind die Gruppen A und C wirksam, da zwischen beiden Gruppen kein Ausschluss definiert wurde. Das heißt, die Person ist berechtigt Bestellungen

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

Tabelle 35: Ausgeschlossene Gruppen und wirksame Zuweisungen

Person	Mitglied in Rolle	Zugewiesene Gruppe	Ausgeschlossene Gruppe	Wirksame Gruppe
Jenny Basset	Marketing	Gruppe A		Gruppe C
	Kontrollgruppe	Gruppe C	Gruppe B Gruppe A	

Voraussetzungen

- Der Konfigurationsparameter **QER | Structures | Inherit | GroupExclusion** ist aktiviert.
- Sich ausschließende Gruppen gehören zum selben Host.

Um Gruppen auszuschließen

1. Wählen Sie im Manager die Kategorie **Unix | 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 Unix 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 31**.

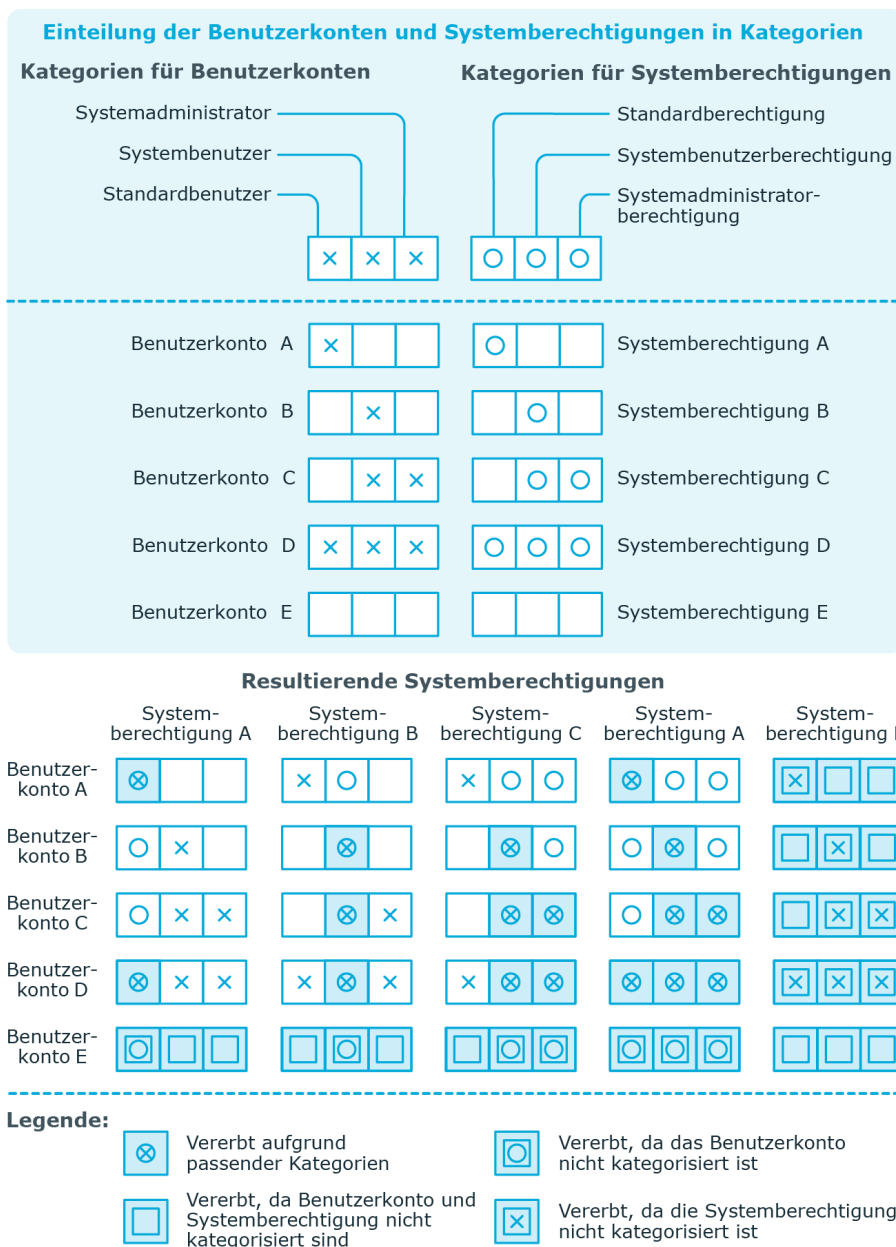
Jedes Benutzerkonto kann einer oder mehreren Kategorien zugeordnet werden. Jede Gruppe kann ebenfalls einer oder mehreren Kategorien zugeteilt werden. Stimmt mindestens eine der Kategoriepositionen zwischen Benutzerkonto und zugewiesener Gruppe überein, wird die Gruppe an das Benutzerkonto vererbt. Ist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

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

Tabelle 36: Beispiele für Kategorien

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

Abbildung 2: Beispiel für die Vererbung über Kategorien



Um die Vererbung über Kategorien zu nutzen

- Definieren Sie am Host die Kategorien.
- Weisen Sie die Kategorien den Benutzerkonten über ihre Stammdaten zu.
- Weisen Sie die Kategorien den Gruppen über ihre Stammdaten zu.

Verwandte Themen

- [Festlegen der Kategorien für die Vererbung von Berechtigungen](#) auf Seite 81
- [Allgemeine Stammdaten eines Unix Benutzerkontos](#) auf Seite 94
- [Allgemeine Stammdaten einer Unix Gruppe](#) auf Seite 114

Zusatzeigenschaften an eine Unix Gruppe zuweisen


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

Um Zusatzeigenschaften für eine Gruppe festzulegen

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

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


Um eine Zuweisung zu entfernen

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

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

Löschen von Unix Gruppen

Um eine Gruppe zu löschen

1. Wählen Sie die Kategorie **Unix | Gruppen**.
2. Wählen Sie in der Ergebnisliste die Gruppe.
3. Löschen Sie die Gruppe über die Schaltfläche .
4. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Die Gruppe wird endgültig aus der One Identity Manager-Datenbank und der Unix-Umgebung gelöscht.

Berichte über Unix Objekte

Der One Identity Manager stellt verschiedene Berichte zur Verfügung, in denen Informationen über das ausgewählte Basisobjekt und seine Beziehungen zu anderen Objekten der One Identity Manager-Datenbank aufbereitet sind. Für Unix-basierte Zielsysteme stehen folgende Berichte zur Verfügung.

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

Tabelle 37: Berichte für das Zielsystem

Bericht	Beschreibung
Übersicht aller Zuweisungen	Der Bericht ermittelt alle Rollen, in denen sich Personen befinden, die im ausgewählten Host mindestens ein Benutzerkonto besitzen.
Unverbundene Benutzerkonten anzeigen	Der Bericht zeigt alle Benutzerkonten des Hosts, denen keine Person zugeordnet ist. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung.
Personen mit mehreren Benutzerkonten anzeigen	Der Bericht zeigt alle Personen, die mehrere Benutzerkonten im Host besitzen. Der Bericht enthält eine Risikoeinschätzung.
Ungenutzte Benutzerkonten anzeigen	Der Bericht enthält alle Benutzerkonten des Hosts, die in den letzten Monaten nicht verwendet wurden. Der Bericht enthält die Gruppenmitgliedschaften und die Risikoeinschätzung.
Abweichende Systemberechtigungen anzeigen	Der Bericht enthält alle Gruppen des Hosts, die aus manuellen Operationen im Zielsystem resultieren und nicht aus der Provisionierung über den One Identity Manager.
Benutzerkonten mit einer überdurchschnittlichen Anzahl an Systemberechtigungen	Der Bericht enthält alle Benutzerkonten des Hosts, die eine überdurchschnittliche Anzahl an Gruppenmitgliedschaften besitzen.

Bericht	Beschreibung
anzeigen	
Unix Benutzerkonten- und Gruppenverteilung	Der Bericht enthält eine Zusammenfassung zur Benutzerkonten- und Gruppenverteilung aller Hosts. Den Bericht finden Sie in der Kategorie Mein One Identity Manager .
Datenqualität der Unix Benutzerkonten	Der Bericht enthält verschiedenen Auswertungen zur Datenqualität der Benutzerkonten aller Hosts. Den Bericht finden Sie in der Kategorie Mein One Identity Manager .


Übersicht aller Zuweisungen

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

Beispiele

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

Um detaillierte Informationen über Zuweisungen anzuzeigen

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

Angezeigt werden alle Rollen der gewählten Rollenklasse. Die Färbung der Steuerelemente zeigt an, in welcher Rolle sich Personen befinden, denen das

ausgewählte Basisobjekt zugewiesen ist. Die Bedeutung der Steuerelemente des Berichts ist in einer separaten Legende erläutert. Die Legende erreichen Sie über das Symbol **i** in der Symbolleiste des Berichtes.

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

Abbildung 3: Symbolleiste des Berichts Übersicht aller Zuweisungen



Tabelle 38: Bedeutung der Symbole in der Symbolleiste des Berichts

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

Anhang: Konfigurationsparameter für die Verwaltung einer Unix-Umgebung

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

Tabelle 39: Konfigurationsparameter

Konfigurationsparameter	Beschreibung
TargetSystem\Unix	Präprozessorrelevanter Konfigurationsparameter zur Steuerung der Modellbestandteile für die Verwaltung Unix-basierter Zielsysteme. Ist der Parameter aktiviert, sind die Bestandteile des Zielsystems verfügbar. Die Änderung des Parameters erfordert eine Kompilierung der Datenbank.
TargetSystem\Unix\Accounts	Der Konfigurationsparameter erlaubt die Konfiguration der Angaben zu Benutzerkonten.
TargetSystem\Unix\Accounts\InitialRandomPassword	Der Konfigurationsparameter legt fest, ob bei Neuanlage von Benutzerkonten ein zufällig generiertes Kennwort vergeben wird. Das Kennwort muss mindestens die Zeichenklassen enthalten, die in der zugewiesenen Kennwortrichtlinie definiert sind.
TargetSystem\Unix\Accounts\InitialRandomPassword\SendTo	Der Konfigurationsparameter enthält die Person, die eine E-Mail mit dem zufällig generierten Kennwort erhalten soll (Verantwortlicher der Kostenstelle/Abteilung/Standort/Rolle, Verantwortlicher der Person oder XUserInserted). Ist kein Empfänger ermittelbar, dann wird an die im Konfigurationsparameter "TargetSystem\Unix\DefaultAddress" hinterlegte

Konfigurationsparameter	Beschreibung
	Adresse versandt.
TargetSystem\Unix\Accounts\ InitialRandomPassword\SendTo\ MailTemplateAccountName	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Anmeldeinformationen zum Benutzerkonto zu versorgen. Es wird die Mailvorlage Person - Erstellung neues Benutzerkonto verwendet.
TargetSystem\Unix\Accounts\ InitialRandomPassword\SendTo\ MailTemplatePassword	Der Konfigurationsparameter enthält den Namen der Mailvorlage, welche versendet wird, um Benutzer mit den Informationen zum initialen Kennwort zu versorgen. Es wird die Mailvorlage Person - Initiales Kennwort für neues Benutzerkonto verwendet.
TargetSystem\Unix\Accounts\ MailTemplateDefaultValues	Der Konfigurationsparameter enthält die Mailvorlage, die zum Senden von Benachrichtigungen genutzt wird, wenn bei der automatischen Erstellung eines Benutzerkontos Standardwerte der IT Betriebsdatenabbildung verwendet werden. Es wird die Mailvorlage Person - Erstellung neues Benutzerkonto mit Standardwerten verwendet.
TargetSystem\Unix\Accounts\ PrivilegedAccount	Der Konfigurationsparameter erlaubt die Konfiguration der Einstellungen für privilegierte Unix Benutzerkonten.
TargetSystem\Unix\Accounts\ PrivilegedAccount\ AccountName_Postfix	Der Konfigurationsparameter enthält das Postfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem\Unix\Accounts\ PrivilegedAccount\ AccountName_Prefix	Der Konfigurationsparameter enthält das Präfix zur Bildung des Anmeldenamens für privilegierte Benutzerkonten.
TargetSystem\Unix\DefaultAddress	Der Konfigurationsparameter enthält die Standard-E-Mail-Adresse des Empfängers für Benachrichtigungen über Aktionen im Zielsystem.
TargetSystem\Unix\ MaxFullsyncDuration	Der Konfigurationsparameter enthält die maximale Laufzeit in Minuten für eine Synchronisation. Während dieser Zeit erfolgt keine Neuberechnung der Gruppenmitgliedschaften durch den DBQueue Prozessor. Bei Überschreitung der festgelegten maximalen Laufzeit werden die Berechnungen von Gruppenmitgliedschaften wieder ausgeführt.

Konfigurationsparameter	Beschreibung
TargetSystem\Unix\ PersonAutoDefault	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die außerhalb der Synchronisation in der Datenbank angelegt werden.
TargetSystem\Unix\ PersonAutoDisabledAccounts	Der Konfigurationsparameter legt fest, ob an deaktivierte Benutzerkonten automatisch Personen zugewiesen werden. Die Benutzerkonten erhalten keine Kontendefinition.
TargetSystem\Unix\ PersonAutoFullSync	Der Konfigurationsparameter legt den Modus für die automatische Personenzuordnung für Benutzerkonten fest, die durch die Synchronisation in der Datenbank angelegt oder aktualisiert werden.
TargetSystem\Unix\ PersonExcludeList	<p>Der Konfigurationsparameter enthält eine Auflistung aller Benutzerkonten, für die keine automatische Personenzuordnung erfolgen soll. Angabe der Namen in einer Pipe () getrennten Liste, die als reguläres Suchmuster verarbeitet wird.</p> <p>Beispiel: ROOT</p>

Anhang: Standardprojektvorlage für Unix-basierte Zielsysteme

Eine Standardprojektvorlage sorgt dafür, dass alle benötigten Informationen im One Identity Manager angelegt werden. Dazu gehören beispielsweise die Mappings, Workflows und das Basisobjekt der Synchronisation. Wenn Sie keine Standardprojektvorlage verwenden, müssen Sie das Basisobjekt der Synchronisation selbst im One Identity Manager bekannt geben.

Verwenden Sie eine Standardprojektvorlage für die initiale Einrichtung des Synchronisationsprojektes. Für kundenspezifische Implementierungen können Sie das Synchronisationsprojekt mit dem Synchronization Editor erweitern.

Die Vorlage verwendet Mappings für die folgenden Schematypen.

Tabelle 40: Abbildung der unix Schematypen auf Tabellen im One Identity Manager Schema

Schematyp im Unix-basierten Zielsystem	Tabelle im One Identity Manager Schema
Group	UNXGroup
Host	UNXHost
LoginShell	UNXLoginShell
User	UNXAccount

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 Geschäftssagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen besuchen Sie <https://www.oneidentity.com/company/contact-us.aspx> oder rufen Sie + 1-800-306-9329 an.

Technische Supportressourcen

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

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

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

A

Anmeldeinformationen 70
Architekturüberblick 7
Ausschlussdefinition 122
Ausstehendes Objekt 30

B

Benachrichtigung 70
Benutzerkonto
 administratives Benutzerkonto 88, 90
 Bildungsregeln ausführen 47
 Identität 85
 Kennwort
 Benachrichtigung 70
 privilegiertes Benutzerkonto 85, 91
 Standardbenutzerkonto 87
 Typ 85
Bildungsregel
 IT Betriebsdaten ändern 47

E

E-Mail-Benachrichtigung 70
Einzelobjektsynchronisation
 beschleunigen 33

I

Identität 85
IT Betriebsdaten
 ändern 47

IT Shop Regal
 Kontendefinitionen zuweisen 53

J

Jobserver
 bearbeiten 13
 Lastverteilung 33

K

Kennwort
 initial 70
Kennwortrichtlinie 58
 Anzeigename 62
 Ausschlussliste 68
 bearbeiten 61
 Fehlanmeldungen 62
 Fehlermeldung 62
 Generierungsskript 65-66
 initiales Kennwort 62
 Kennwort generieren 68
 Kennwort prüfen 68
 Kennwortalter 62
 Kennwortlänge 62
 Kennwortstärke 62
 Kennwortzyklus 62
 Namensbestandteile 62
 Prüfskript 65
 Standardrichtlinie 59, 62
 Vordefinierte 58
 Zeichenklassen 64

- zuweisen 59
- Konfigurationsparameter 131
- Kontendefinition 38
 - an Abteilung zuweisen 50
 - an alle Personen zuweisen 51
 - an Geschäftsrolle zuweisen 50
 - an Kostenstelle zuweisen 50
 - an Person zuweisen 48, 52
 - an Standort zuweisen 50
 - an Systemrollen zuweisen 52
 - an Unix Host zuweisen 55
 - automatisch zuweisen 51
 - Automatisierungsgrad 41
 - erstellen 38
 - in IT Shop aufnehmen 53
 - IT Betriebsdaten 44-45
 - löschen 55

L

- Lastverteilung 33

M

- Mitgliedschaft
 - Änderung provisionieren 32

O

- Objekt
 - ausstehend 30
 - publizieren 30
 - sofort löschen 30
- One Identity Manager
 - Administrator 8
 - Benutzer 8
 - Zielsystemadministrator 8

- Zielsystemverantwortlicher 8, 71

P

- Personenzuordnung
 - automatisch 105
 - entfernen 108
 - manuell 108
 - Suchkriterium 107
 - Tabellenspalte 107
- Projektvorlage 134
- Provisionierung
 - beschleunigen 33
 - Mitgliederliste 32

S

- Schema
 - aktualisieren 28
 - Änderungen 28
 - komprimieren 28
- Synchronisation
 - Basisobjekt
 - erstellen 28
 - Benutzer 12
 - Berechtigungen 12
 - einrichten 11
 - Erweitertes Schema 28
 - konfigurieren 20, 25
 - Scope 25
 - starten 20
 - Synchronisationsprojekt
 - erstellen 17, 20
 - Variable 25
 - Variablenset 28
 - Verbindungsparameter 20, 25, 28

- verhindern 35
 - verschiedene Hosts 28
 - Workflow 20, 27
 - Zielsystemschemata 28
 - Synchronisationsanalysebericht 34
 - Synchronisationskonfiguration
 - anpassen 25, 27-28
 - Synchronisationsprojekt
 - bearbeiten 82
 - deaktivieren 35
 - erstellen 17, 20
 - Projektvorlage 134
 - Synchronisationsprotokoll 24
 - Aufbewahrungszeit 25
 - Synchronisationsrichtung
 - In das Zielsystem 20, 27
 - In den Manager 20
 - Synchronisationsserver
 - installieren 13
 - Jobserver 13
 - konfigurieren 13
 - Synchronisationsworkflow
 - erstellen 20, 27
- U**
- Unix Benutzerkonto
 - administratives Benutzerkonto 88
 - Automatisierungsgrad 94, 103
 - Benutzerkonto UID 94
 - Benutzername 94
 - deaktivieren (AIX System) 110
 - EFS (AIX System) 102
 - einrichten 92
 - Grenzwerte (AIX System) 97
 - Gruppe zuweisen 104, 118
 - Gruppen-ID 94
 - Gruppen erbbar 44
 - Gruppen erben 94
 - Homeverzeichnis 94
 - Host 94
 - Identität 44, 94
 - Kategorie 94, 124
 - Kennwort 94
 - initial 69
 - Kennwortdaten (AIX System) 99
 - Kommentar (Gecos) 94
 - Kontendefinition 55, 94
 - Login-Shell 44, 94
 - löschen 112
 - Person 94
 - Person zuweisen 84, 92, 94, 105
 - primäre Gruppe 79, 94
 - privilegiertes Benutzerkonto 44, 91, 94
 - Risikoindeks 94
 - Sicherheit (AIX System) 100
 - sperrern 112
 - Standardbenutzerkonto 87
 - verschlüsselndes Dateisystem (AIX System) 102
 - wiederherstellen 112
 - Zusatzeigenschaft zuweisen 104
 - Unix Gruppe
 - an Abteilung zuweisen 115
 - an Geschäftsrolle zuweisen 116
 - an Kostenstelle zuweisen 115
 - an Standort zuweisen 115
 - aus IT Shop entfernen 120
 - ausschließen 122
 - bearbeiten 113

- Benutzerkonto zuweisen 104, 115, 118
- Gruppe zuweisen 121
- Gruppen-ID 114
- Host 114
- in IT Shop aufnehmen 119
- in Systemrolle aufnehmen 118
- Kategorie 114, 124
- Leistungsposition 114
- löschen 127
- primäre Gruppe 79, 94
- Risikoindex 114
- wirksam 122
- Zusatzeigenschaft zuweisen 127
- Unix Host 82
 - AIX System 79
 - Anwendungsrollen 8
 - Berichte 128
 - einrichten 79
 - Kategorie 81, 124
 - Kontendefinition 79
 - Kontendefinition (initial) 55
 - Personenzuordnung 107
 - primäre Gruppe 79
 - Synchronisation 79
 - Übersicht aller Zuweisungen 129
 - Zielsystemverantwortlicher 8, 71, 79
- Unix Login-Shell 83

Z

- Zeitplan
 - deaktivieren 35
- Zielsystemabgleich 30